Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan säädettäväksi uusi laki tietoliikennetiedustelusta siviilitiedustelussa sekä muutettavaksi poliisilakia niin, että siihen lisättäisiin uusi 5 a luku, jossa säädettäisiin tiedustelumenetelmistä ja niiden käytöstä siviilitiedustelussa. Lisäksi esityksessä ehdotetaan muutettavaksi lakia poliisin hallinnosta, lakia henkilötietojen käsittelystä poliisitoimessa, rikoslakia, esitutkintalakia, pakkokeinolakia ja lakia oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa. Esitys liittyy samanaikaisesti annettaviin hallituksen esityksiin, joissa ehdotetaan säädettäviksi uusi sotilastiedustelulaki ja uusi laki tiedustelutoiminnan valvonnasta.

Esityksessä ehdotettavan lainsäädännön keskeisin tavoite on kansallisen turvallisuuden parantaminen ja säädöspohjan luominen tiedustelulle. Tavoitteena on parantaa suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuuteen kohdistuvilta kaikkein vakavimmilta uhkilta. Nämä olisivat siviilitiedustelun kohteita, jotka määriteltäisiin tyhjentävästi laissa. Lakiehdotusten valmistelussa perusoikeuksien suojaan puuttuminen on pyritty rajaamaan niin vähäiseksi kuin tiedustelutoiminnan tehokkuudelle ja tuloksellisuudelle asetettavat vaatimukset huomioon ottaen on mahdollista.

Tiedustelumenetelmiä koskevasta sääntelystä perustuisi menetelmällisesti ja määritelmällisesti osin poliisilain 5 luvun salaisiin tiedonhankintakeinoihin. Tiedustelumenetelmiä olisivat lisäksi paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten ja tietojen saanti yksityiseltä yhteisöltä sekä tietoliikennetiedustelu. Tiedustelumenetelmien tarkoituksena olisi tuottaa välttämätöntä tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta ylimmän valtiojohdon päätöksenteon tueksi sekä kansallisen turvallisuuden suojaamiseksi. Tietoliikennetiedustelun erityistavoitteena olisi myös parantaa Suomen kykyä suojautua vakavimpia tietoverkkouhkia vastaan.

Tiedustelumenetelmien päätöksentekoa koskeva sääntely perustuisi myös osin poliisilain 5 lukuun. Tietoliikennetiedustelusta päättäisi tuomioistuin. Tuomioistuin päättäisi myös paikkatiedustelusta silloin, kun se kohdistuu kotirauhan suojaamaan paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty. Ulkomaan tiedustelusta, tiedustelumenetelmien käytöstä ulkomaan tiedustelussa sekä kansainväliseen yhteistyöhön osallistumisesta päättäisi suojelupoliisin päällikkö.

Tiedustelumenetelmillä saatua tietoa voitaisiin tietyin edellytyksin luovuttaa esitutkinta- tai muulle toimivaltaiselle viranomaiselle. Tiedon käyttötarkoitussidonnaisuuden johdosta luovuttamisen edellytykset määriteltäisiin tiukoiksi.

Poliisilain 5 a luvussa säädettäisiin yhteistyöstä sotilastiedusteluviranomaisen ja muiden viranomaisten kanssa sekä salaisen tiedonhankinnan yhteensovittamisesta suojelupoliisin, sotilastiedusteluviranomaisen, keskusrikospoliisin ja muun viranomaisen virkamiesten työturvallisuuden varmistamiseksi.

Poliisilain 5 a luvussa sekä laissa tietoliikennetiedustelusta siviilitiedustelussa säädettäisiin jäljentämiskielloista, kuuntelu- ja katselukielloista sekä tiedustelukiellosta. Eräiden ammattiryhmien viestintä nauttisi korostettua suojaa siviilitiedustelulta. Tiedustelumenetelmien käytöstä tulisi tiettyjen edellytysten täyttyessä ilmoittaa niiden kohteille.

Suojelupoliisin tiedustelullisten toimivaltuuksien lisääntymisen myötä sen esitutkinta- ja pakkokeinotoimivaltuudet ehdotetaan poistettavaksi oikeudenmukaisen oikeudenkäynnin turvaa-

miseksi. Tämä ei estäisi suojelupoliisin mahdollisuutta osallistua esitutkintaviranomaisen suorittamaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa.

Tiedustelullisten toimivaltuuksien ja todennäköisen resurssien lisääntymisen myötä suojelupoliisiin kohdistettavan laillisuusvalvonnan merkitys korostuu. Suojelupoliisin toiminnan valvontaa ehdotetaan tehostettavaksi tässä esityksessä. Suojelupoliisin olisi annettava tieto tiedusteluvaltuutetulle sille myönnetyistä tuomioistuimen päätöksistä ja luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen. Suojelupoliisin olisi myös mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle muita tiedustelumenetelmiä koskevista päätöksistä, siviilitiedustelun suojaamisesta, ilmaisukiellosta ja rikostorjuntaan luovutettavan tiedon siirtämistä koskevista päätöksistä.

Tähän esitykseen liittyvässä esityksessä tiedustelun valvonnasta ehdotetuksi lainsäädännöksi ehdotetaan perustettavaksi riippumaton oikeudellinen valvoja tiedusteluvaltuutettu, joka valvoisi tiedustelutoimintaa reaaliaikaisesti.

Esitys liittyy myös perustuslain 10 §:n tarkistamista koskevaan hallituksen esitykseen. Luottamuksellisen viestin suojaan puuttuvat toimivaltuudet kytkeytyvät ehdotettuun perustuslain muutokseen.

Kaikki tiedustelutoimintaan liittyvät hallituksen esitykset ovat riippuvaisia toisistaan, ja ne tulisi saattaa perustuslakivaliokunnan käsiteltäväksi yhtäaikaisesti.

Lait ehdotetaan tulemaan voimaan mahdollisimman pian sen jälkeen kun ne on hyväksytty ja vahvistettu.

LUONNOS

SISÄLLYS

HALLITUKSEN ESITYS EDUSKUNNALLE SIVIILITIEDUSTELUA KOSKEVAKSI LAINSÄÄDÄNNÖKSI ... 1
ESITYKSEN PÄÄASIALLINEN SISÄLTÖ ... 1
SISÄLLYS ... 3
YLEISPERUSTELUT ... 6
1 JOHDANTO ... 6
2 NYKYTILA ... 8
2.1 Muuttuva turvallisuusympäristö ... 8
2.2 Lainsäädäntö ja käytäntö ... 12
Kansallisen turvallisuuden viranomaiskenttä ... 12
Suojelupoliisin tehtävät ... 14
Suojelupoliisin tiedonhankinta ... 16
Poliisioikeudelliset periaatteet ... 16
Tietoturvauhkien torjunta ... 31
Suojelupoliisin tiedonhankinta ulkomailla ... 33
Suojelupoliisin toiminnan ohjaus ... 34
Suojelupoliisin toiminnan laillisuusvalvonta ... 35
2.3 Kansainvälinen kehitys sekä ulkomaiden lainsäädäntö ... 38
Yleistä ... 38
Norja ... 39
Tanska ... 43
Saksa ... 44
2.4 Kansainvälisten sopimusten ihmisoikeusvelvoitteet ... 50
Yleistä ... 50
KP-sopimus ... 51
Euroopan ihmisoikeussopimus ... 51
2.5 Euroopan unionin perusoikeuskirja ... 64
Euroopan unionin tuomioistuimen ratkaisukäytäntö ... 65
2.6 Nykytilan arviointi ... 68
Yleistä ... 68
Suojelupoliisin tehtävät ... 69
Suojelupoliisin toimivaltuudet ... 70
Suojelupoliisin oikeudellinen valvonta ... 104
Henkilötietojen käsittely ... 105
Esitutkintatoimivaltuudet ... 106
3 ESITYKSEN TAVOITTEET JA KESKEISET EHDOTUKSET ... 108
3.1 Tavoitteet ... 108
3.2 Toteuttamisvaihtoehdot ... 110
Rikostorjuntatoimivaltuuksien käyttöalan laajentaminen ... 110
Tiedonhankintalakityöryhmän ehdotus ... 112
3.3 Keskeiset ehdotukset ... 114
Poliisilaki ... 114
Laki tietoliikennetiedustelusta siviilitiedustelussa ... 121
4 ESITYKSEN VAIKUTUKSET ... 135
4.1 Taloudelliset vaikutukset ... 135
Suojelupoliisi ... 136

LUONNOS

Sisäministeriö ... 139
Muu poliisihallinto ... 140
Oikeushallinto ... 143
Yhteenveto lakiehdotusten taloudellisista vaikutuksista ... 143
4.2 Vaikutukset kansantalouteen ja yrityksiin ... 144
4.3 Vaikutukset viranomaisten toimintaan ... 147
4.4 Yhteiskunnalliset vaikutukset ... 148
Kansalaisten asema yhteiskunnassa ja kansalaisyhteiskunnan toiminta ... 148
Rikostorjunta ja turvallisuus ... 149
Tietoyhteiskuntavaikutukset ... 149
4.5 Siviilitiedustelulainsäädännön hyötyjen ja haittojen arviointia ... 153
Uhkantorjunta ... 153
Rikostorjunta ... 153
Välittömät kustannusvaikutukset ... 154
Kokoavia huomioita ... 154
5 ASIAN VALMISTELU ... 154
5.1 Valmisteluvaiheet ja -aineisto ... 154
5.2 Lausunnot ja niiden huomioon ottaminen ... 157
6 RIIPPUVUUS MUISTA ESITYKSISTÄ ... 159
YKSITYISKOHTAISET PERUSTELUT ... 161
1 LAKIEHDOTUSTEN PERUSTELUT ... 161
1.1 Laki poliisilain muuttamisesta ... 161
1 luku **Yleiset säännökset** ... 161
5 luku **Salaiset tiedonhankintakeinot** ... 162
5 a luku **Siviilitiedustelun tiedustelumenetelmät** ... 165
9 luku **Erinäiset säännökset** ... 228
1.2 Laki tietoliikennetiedustelusta siviilitiedustelussa ... 229
1.3 Laki poliisin hallinnosta annetun lain muuttamisesta ... 258
1.4 Laki henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta ... 259
1.5 Laki esitutkintalain muuttamisesta ... 260
2 luku **Esitutkintaan osalliset** ... 260
1.6 Laki rikoslain muuttamisesta ... 260
12 luku **Maanpetosrikoksista** ... 260
1.7 Laki pakkokeinolain muuttamisesta ... 261
2 luku **Kiinniottaminen, pidättäminen ja vangitseminen** ... 261
10 luku **Salaiset pakkokeinot** ... 261
1.8 Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain muuttamisesta ... 262
2 VOIMAANTULO ... 263
3 SUHDE PERUSTUSLAKIIN JA SÄÄTÄMISJÄRJESTYS ... 264
3.1 Johdanto ... 264
3.2 Toimivaltuussääntely perusoikeussäännösten kannalta ... 264
3.3 Muu sääntely perustuslain kannalta ... 269
3.4 Säätämisjärjestyksen arviointi ... 270
LAKIEHDOTUKSET ... 272
1. Laki poliisilain muuttamisesta ... 272
2. Laki tietoliikennetiedustelusta siviilitiedustelussa ... 302
3. Laki poliisin hallinnosta annetun lain muuttamisesta ... 309
4. Laki henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta ... 310

LUONNOS

5. Laki esitutkintalain muuttamisesta ... 312
6. Laki rikoslain muuttamisesta ... 313
7. Laki pakkokeinolain muuttamisesta ... 314
8. Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain muuttamisesta ... 316
RINNAKKAISTEKSTI ... 318
1. Laki poliisilain muuttamisesta ... 318
3. Laki poliisin hallinnosta annetun lain muuttamisesta ... 366
4. Laki henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta ... 368
5. Laki esitutkintalain muuttamisesta ... 371
7. Laki pakkokeinolain muuttamisesta ... 372
8. Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain muuttamisesta ... 375

LUONNOS

YLEISPERUSTELUT

1 Johdanto

Suomen turvallisuusympäristö on viime vuosina merkittävästi muuttunut ja digitalisoitunut. Sisäiseen ja ulkoiseen turvallisuuteen kohdistuvat uhat limittyvät toisiinsa entistä läheisemmin. Kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä maamme ulkopuolelle. Uhkien kansainvälisestä luonteesta seuraa, että niiden taustalla olevat tahot ovat verkostoituneet eri maiden alueelle. 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. Uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja niiden toiminnan ennakoiminen on vaikeutunut. 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 poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona sotilaallisten voimakeinojen ohella.

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. Siviiliviranomaisten tiedonhankinta perustuu pääosin rikostorjuntatoimivaltuuksiin, julkisiin lähteisiin sekä kansainvälisen ja muun vapaaehtoisen yhteistyön puitteissa saataviin tietoihin.

Sisäministeriön hallinnonalan viranomaisilla, erityisesti suojelupoliisilla, on merkittävä rooli kansalliseen turvallisuuteen kohdistuvien siviililuonteisten uhkien torjunnassa. Suojelupoliisi on valtakunnallinen poliisiyksikkö, jonka tehtävänä on torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa. Suojelupoliisin tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi. Suojelupoliisi suorittaa toimialallaan tehtävänsä mukaista jatkuvaa turvallisuustiedustelua sekä ylläpitää näin syntyvää valtion turvallisuusympäristön kansallista ja kansainvälistä tilannekuvaa sekä raportoi niistä valtiojohdolle ja turvallisuusviranomaisille.

Suojelupoliisin tiedonhankintatoimivaltuudet perustuvat poliisin toimintaa koskeviin yleislakeihin, pääosin poliisilakiin sekä esitutkinta- ja pakkokeinolakiin. Tiedonhankintatoimivaltuuksien käyttö on sidottu rikoksen ennalta estämiseen, paljastamiseen ja selvittämiseen sekä joissain tapauksissa vaaran torjumiseen.

Puolustusministeriön hallinnonalalle kuuluva puolustusvoimat vastaa Suomen sotilaallisesta puolustamisesta. Sotilastiedustelun tehtävät liittyvät sotilasstrategisen tilannekuvan muodostamiseen ja ylläpitämiseen sekä kansainvälisten tehtävien turvallisuuteen. Sotilastiedustelusta ei ole nimenomaisia säännöksiä laissa. Puolustusvoimien sotilasvastatiedustelu vastaa, suojelupoliisille laissa säädettyä toimivaltaa rajoittamatta, sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvan laittoman tiedustelutoiminnan ja sotilaallisen maanpuolustuksen tarkoi-

tusta vaarantavien rikosten estämisestä, mutta ei kuitenkaan niihin liittyvästä rikostutkinnasta, joka kuuluu suojelupoliisin vastuulle.

Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten, erityisesti suojelupoliisin ja puolustusvoimien, tiedonhankintakyvyn parantamiseksi. Tavoitteena oli selvittää lainsäädännön tila turvallisuusviranomaisten tiedonhankintaa koskevan toimivaltuussääntelyn osalta. Tavoitteena oli myös arvioida, kuinka kansallisesta turvallisuudesta erityisesti tietoverkoissa esiintyvien uhkien torjumiseksi voitaisiin huolehtia paremmin.

Työryhmä luovutti mietintönsä puolustusministeriölle 14.1.2015 (Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö). Tiedonhankintalakityöryhmä esitti, että siviili- ja sotilastiedustelulle luodaan säädösperusta. Tätä tarkoitusta varten se ehdotti, että käynnistettäisiin yksi tai useampia lainsäädäntöhankkeita, jotka voitaisiin valmistella toimialakohtaisesti. Tässä yhteydessä tulisi myös harkita esimerkiksi parlamentaarista tai muuta poliittisessa ohjauksessa tapahtuvaa valmistelua.

Tiedonhankintalakityöryhmän mietinnöstä järjestettiin lausuntokierros. Lausunnoista laadittu yhteenveto on julkaistu 30.6.2015. Lausunnonantajat pääsääntöisesti kannattivat tiedustelua koskevan lainsäädännön kehittämistä.

Samanaikaisesti tiedonhankintalakityöryhmän kanssa toimi osin samoja kysymyksiä tarkastellut sisäministeriön asettama suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittänyt työryhmä. Sen 24.9.2014 julkaistussa loppuraportissa (Sisäministeriön julkaisu 28/2014) todetaan, että jos suojelupoliisin tehtäviä ja toimivaltuuksia kehitetään merkittävästi tiedustelullisempaan suuntaan, syntyy tarve ulkoisen laillisuusvalvonnan ja parlamentaarisen valvonnan muotojen uudistamiselle. Kyse voisi olla esimerkiksi uusien tuomioistuinlupien edellyttämisestä ja erityisen parlamentaarisen valvontaelimen perustamisesta. Jos suojelupoliisin toiminnan ulkomaantiedustelullisten elementtien merkitys edelleen kasvaa, tulisi siviilitiedustelun ja sotilastiedustelun tehtävien ja toimivaltuuksien sääntelyn, ohjauksen ja valvonnan kehittämisen olla toisensa huomioon ottavaa. Samoin, jos suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, tulisi oikeudenmukaisen oikeudenkäynnin turvaamiseksi harkita suojelupoliisin esitutkintatehtävien ja -toimivaltuuksien rajoittamista. Suojelupoliisi voisi osallistua edelleenkin tarpeen mukaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa.

Tiedustelulainsäädännön valmistelulla on perusta hallitusohjelmassa. Pääministeri Juha Sipilän hallitusohjelman mukaan kasvavat riskit ja uudet uhat edellyttävät koko yhteiskunnalta uudenlaista valmiutta ja varautumista. Hallitusohjelman mukaisesti tavoitteena on vahvistaa kokonaisturvallisuusajattelua kansallisesti, Euroopan unionissa ja kansainvälisessä yhteistyössä. Tämä koskee erityisesti uusien ja laaja-alaisten uhkien kuten hybridivaikuttamisen, kyberhyökkäysten ja terrorismin torjuntaa. Hallitus esittää ohjelmassa säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle. Lainsäädännön myötä halutaan kyetä vastaamaan aiempaa paremmin turvallisuusympäristön muutoksiin ja Suomea koskeviin uudenlaisiin uhkiin. Samalla painotetaan, että valmistelun yhteydessä kiinnitetään huomiota perus- ja ihmisoikeuksien toteutumiseen.

Sisäministeriö käynnisti siviilitiedustelua koskevan hankkeen, puolustusministeriö sotilastiedustelua koskevan hankkeen ja oikeusministeriö perustuslain mahdollista muuttamista koskevan hankkeen. Kolmen eri työryhmän hankkeita päätettiin valmistella kiinteässä yhteistyössä. Lisäksi todettiin, että liikenne- ja viestintäministeriö tarjoaa asiantuntija-apua työryhmille digitalisaatiokehityksen huomioimisessa. Edelleen sisäministeriö asetti parlamentaarisen seuran-

taryhmän tiedustelulainsäädännön uudistamiseen liittyville hankkeille. Seurantaryhmän tarkoituksena oli toimia linkkinä lainsäädäntöhankkeiden ja eduskunnan välillä, jotta eduskunta olisi jatkuvasti tietoinen hankkeiden etenemisestä.

Sisäministeriön hankkeen tavoitteena oli keskittyä siviilitiedustelua koskevan lainsäädännön valmisteluun. Hankkeen keskeisin tavoite oli kansallisen turvallisuuden parantaminen. Tavoitteena oli parantaa turvallisuusviranomaisten kykyä ennakoida ja estää toimialallaan sellaisia vahingollisia tekoja ja toimenpiteitä, jotka voivat vaarantaa erityisen tärkeitä kansallisia etuja.

Suojelupoliisille ei tällä hetkellä ole säädetty erityisiä toimivaltuuksia valtion turvallisuuteen liittyvän uhkatiedon hankkimiseksi. Suojelupoliisin tärkeimpänä tehtävänä on yhteistyössä erityisesti keskusrikospoliisin kanssa ennalta estää ja paljastaa terrorismiin, laittomaan tiedustelutoimintaan, joukkotuhoaseiden levittämiseen ja ääriliikkeisiin sekä valtion turvallisuutta vaarantavaan järjestäytyneeseen rikollisuuteen kytkeytyviä hankkeita. Hankkeessa harkitaan toimivaltuuksien kehittämistä ulkomaan henkilötiedustelua ja tietojärjestelmätiedustelua sekä rajat ylittävään tietoliikenteeseen kohdistettavaa tiedustelua varten.

Tavoitteena on valmistella siviilitiedustelua koskevat keskeiset säännökset ja näin parantaa suojelupoliisin tiedonhankintaa poliisin tehtäviin liittyvistä vakavista kansainvälisistä uhista siten, että suojelupoliisilla olisi toimivaltuudet ulkomaan henkilötiedusteluun ja tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun. Valmistelu voidaan tarvittaessa toteuttaa myös vaiheittain ottaen huomioon perustuslaista nykyisin johtuvat mahdolliset rajoitukset. Sotilastiedustelun ja samanaikaisesti sisäministeriössä valmisteltavana olevien siviilitiedustelua koskevien säännösten tulisi olla keskenään yhteen sovitettuja.

Oikeusministeriö käynnisti 17.10.2016 hankkeen, jonka tehtävänä oli valmistella lainsäädäntö tiedustelutoiminnan valvonnasta. Työryhmän toimeksiantoa tarkistettiin 9.2.2017 koskemaan siviili- ja sotilastiedusteluviranomaisten tiedustelutoiminnan laillisuusvalvonnan järjestämistä koskevan lainsäädännön valmistelua. Parlamentaarista valvontajärjestelmää koskevan lainsäädännön valmistelu siirtyi eduskunnan pääsihteerin asettaman eduskunnan kanslian sisäisen työryhmän valmisteltavaksi.

Oikeusministeriö asetti 28.9.2015 asiantuntijatyöryhmän selvittämään ja valmistelemaan luottamuksellisen viestin salaisuuden suojaa koskevan perustuslakisääntelyn tarkistamista. Asiantuntijatyöryhmän tehtävänä oli myöhemmin asetettavaa parlamentaarista valmistelua varten selvittää ja valmistella perustuslain tarkistamista siten, että lailla voidaan säätää tarpeellisiksi katsottavien edellytysten täyttyessä kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin suojaan. Oikeusministeriön ehdotus perustuslain tarkistamiseksi valmistui 23.9.2016. Työryhmä ehdotti 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.

2 Nykytila

2.1 Muuttuva turvallisuusympäristö

Sisäisen turvallisuuden strategia hyväksyttiin valtioneuvostossa 5.10.2017. Strategia pohjautuu toukokuussa 2016 eduskunnalle annettuun sisäisen turvallisuuden selontekoon. Strategian

mukaankin Suomen turvallisuusympäristö on kiistatta monimutkaistunut. Uudet haasteet ja tehtävät edellyttävät viranomaisilta asianmukaista suorituskykyä. Turvallisuusviranomaisten ydintoimintojen ja palvelutason on oltava turvattuja. Turvallisuusympäristön muutoksiin on vastattava ajanmukaistamalla turvallisuusviranomaisten tilannekuvaa, toimivaltuuksia sekä parantamalla viranomaisten suorituskykyä. Nyt yhteiskunnan mahdollisuudet reagoida kansalliseen turvallisuuteen kohdistuviin uhkiin ovat merkittävässä epäsuhdassa uhkien toteutumisesta aiheutuvien vahinkojen kanssa.

Uusien uhkien ilmenemismuotoja ovat strategian mukaan esimerkiksi terrorismi sekä hybridi- ja kyberuhkat, jotka voivat olla myös voimapolitiikan välineitä. Tavoitteena on, että sisäministeriön ja valtioneuvoston kokonaistilannekuva sekä siviilitiedustelulla hankittu analysoitu tieto on kaikkien kansallisen turvallisuuden suojaamiseen osallistuvien toimijoiden käytössä oikeaaikaisesti. Tavoitteena on lisäksi parantaa turvallisuusviranomaisten toimintavalmiutta ja suorituskykyä muuttuneen toimintaympäristön vaatimusten mukaisesti kehittämällä toimivaltuuksia, varautumista, toimintamalleja ja voimavaroja. Lisäksi vahvistetaan turvallisuustoimijoiden strategisen turvallisuusviestinnän osaamista ja vähennetään viranomaisten sekä muiden toimijoiden yhteistyöllä tahallisen ja tarkoitusperäisen virheellisen tiedon levittämisen kielteisiä turvallisuusvaikutuksia.

Valtioneuvosto antoi eduskunnalle 19.5.2016 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 puolustusselonteko annettiin eduskunnalle 16.2.2017. Se toteuttaa turvallisuus- ja puolustuspolitiikasta annettua selontekoa. Sisäisen turvallisuuden selonteko, ulko- ja turvallisuuspoliittinen selonteko sekä puolustusselonteko muodostavat kokonaisturvallisuuden keskeisen viitekehyksen. Taustaa tälle työlle antoivat vuoden 2012 turvallisuus- ja puolustuspoliittinen selonteko sekä yhteiskunnan turvallisuusstrategia vuodelta 2010.

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 Venäjän ja lännen suhteiden huononeminen, kansainvälinen terrorismi, kyberuhat ja laajamittainen laiton maahantulo ovat merkittävimmät viimeaikaiset muutokset 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.

LUONNOS

Ulko- ja turvallisuuspolitiikan 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. 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. Edellä mainitut selonteot korostavat, että suomalaisten turvallisuutta ja hyvinvointia on parannettava. Rajat ylittävien uhkien torjuminen ja niihin varautuminen edellyttävät niin siviili- kuin sotilaallisten voimavarojen hyödyntämistä, laajan keinovalikoiman käyttämistä. Omien vahvuuksiensa pohjalta Suomen on pystyttävä ennakoimaan toimintaympäristön muutoksia ja vastaamaan muutosten asettamiin vaatimuksiin. Sisäisen turvallisuuden selonteon mukaan 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.

Valtioneuvoston puolustusselonteko vahvistaa Suomen lähialueiden turvallisuustilanteen heikentymisen sekä toteaa jännitteiden Itämeren alueella ja epävarmuuden laajemminkin yhä edelleen lisääntyneen. Sotilaallisen voiman ohella voidaan käyttää muuta laajaa keinovalikoimaa tavoitteiden saavuttamiseksi.

Edellä mainituissa selonteoissa niin sanottu hybridivaikuttaminen nousee näkyvään asemaan. Hybridivaikuttaminen voidaan määritellä suunnitelmalliseksi toiminnaksi, jossa valtiollinen tai ei-valtiollinen toimija hyödyntää samanaikaisesti erilaisia sotilaallisia keinoja tai esimerkiksi taloudellisia tai teknologiaan perustuvia painostuskeinoja, informaatio-operaatioita ja sosiaalista mediaa pyrkimyksenään hyödyntää kohdevaltion haavoittuvuuksia. Vaikuttaminen voi kohdistua kohdevaltion niin poliittiseen, taloudelliseen, sotilaalliseen kuin infrastruktuurin rakenteisiin. Hybridivaikuttamisessa ei yleensä ole kyse aseellista hyökkäystä valmistelevista toimenpiteistä, vaan sellaisista painostustoimista, jotka tehokkuutensa johdosta tekevät aseellisen hyökkäyksen tarpeettomaksi.

Digitalisoitumisen vaikutus turvallisuusympäristön kehittymiseen

Digitalisoitumisen vaikutusta turvallisuusympäristön kehittymiseen ja kyberturvallisuutta käsitellään muun muassa Suomen kyberturvallisuusstrategiassa (Valtioneuvoston periaatepäätös 24.1.2013) ja puolustusministeriön mietinnössä Suomalaisen tiedustelulainsäädännön suuntaviivoja (tiedonhankintalakityöryhmän mietintö) vuodelta 2015.

Kyberturvallisuusstrategia toteaa Suomen olevan tietoyhteiskuntana riippuvainen tietoverkkojen ja -järjestelmien toiminnasta ja näin ollen myös erittäin haavoittuvainen niihin kohdistuvil-

le 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 vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.

Tiedonhankintatyöryhmän 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 (vakoilu, terroriteot, kaksikäyttötuotteiden maastavienti). Toisaalta tietoverkkoja hyödynnetään varsinaisena tekovälineenä kohdistaa kohteeseen - esimerkiksi Suomen valtioon - tätä vakavasti vahingoittavia tekoja. Kyse voi olla Suomen kyberturvallisuusstrategian tarkoittamista kybervakoiluksi tai kyberterrorismiksi luonnehdittavista teoista.

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. Vakoiluoperaatio on ennakkoon tarkoin suunniteltu ja sillä on täsmällinen operatiivinen tavoite kerätä tietoa esimerkiksi ulko- ja turvallisuuspolitiikkaan, talouteen ja teollisuuteen liittyvistä seikoista. Esimerkkinä tällaisesta vakoiluoperaatioista voidaan mainita ulkoasiainministeriöön kohdistettu, syksyllä 2013 ilmi tullut tapaus. Tiedusteluohjelmien lisäksi voidaan tietojärjestelmiin toimittaa haittaohjelmia, jotka aktivoituvat kriisin alkaessa

Tiedonhankintalakityöryhmän mietinnön mukaan kybervakoilun ja -operaatioiden merkitys kasvaa tulevina vuosina entisestään. Syitä tälle ovat mahdollisuus toteuttaa kybertoimintaympäristössä tekoja alhaisin kustannuksin, suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski. Kaikki Suomen turvallisuusympäristön kehityksen kannalta olennaiset ulkovallat panostavat määrätietoisesti ja mittavasti offensiivisen 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. Terroristisessa tarkoituksessa toteutettujen kyberhyökkäysten uhka Suomea kohtaan arvioidaan tiedonhankintalakityöryhmän mietinnössä yhä rajalliseksi, mutta toisaalta mietintö toteaa, tilanteen voivan muuttua nopeasti kansainvälisessä toimintaympäristössä tapahtuvien kehitysten seurauksena. Terroristiryhmien mahdollisina tekotapoina tulevat kyseeseen kriittisten verkkopalveluiden saatavuutta haittaavat palvelunestohyökkäykset sekä SCADA-valvomojärjestelmän kautta tehdyt tuhotyöt, jotka pahimmillaan aiheuttavat mittavia henkilö- ja omaisuusvahinkoja.

Valtioneuvoston kanslia julkaisi 17.2.2017 riippumattoman tutkimuksen Suomen kyberturvallisuuden tilasta (Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 30/2017). Tutkimuksen mukaan kansallinen kyberturvallisuustapahtumien havainnointikyky on puutteellinen. Siksi tilannetietoisuus on heikko ja edellytykset estää, rajoittaa ja toipua vakavista kyberhyökkäyksistä on rajallinen. Suomalaisen yhteiskunnan kaikkia elintärkeitä toimintoja sekä huoltovarmuuskriittisiä yrityksiä ei ole tällä hetkellä suojattu riittävällä tavalla erilaisia kybe-

ruhkia 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

Kansallisen turvallisuuden viranomaiskenttä

Turvallisuusympäristön muutosten ennakoinnissa ja niihin varautumisessa merkitystä on lukuisten valtion viranomaisten toiminnalla. Vaikka edellä on todettu, että sotilaalliset ja siviiliuhkat yhä läheisemmin kietoutuvat toisiinsa, voidaan niitä koskeva perusjaottelu yhä katsoa tarkoituksenmukaiseksi. Sotilaallisiin uhkiin varautumisesta ja niiden torjunnasta vastaa puolustusvoimat. Puolustusvoimien ja niiden osana sotilastiedustelun tehtäviä ja toimivaltuuksia käsitellään tähän esitykseen liittyvässä puolustusministeriön sotilastiedustelulainsäädäntöä koskevassa esityksessä.

Toimivaltaisten viranomaisten kenttä on monitahoisempi mitä tulee ei-sotilaallisiin uhkiin varautumiseen. Kaikkia niitä viranomaisia, joiden tehtävillä on merkitystä kansallisen turvallisuuden suojaamisen kannalta tai sivuavat sitä, ei ole tarkoituksenmukaista tai edes mahdollista käsitellä tässä.

Poliisi on sisäisen turvallisuuden kannalta keskeisin vastuuviranomainen. Sen tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisihallituksen johtamassa poliisiorganisaatiossa kansalliseen turvallisuuteen kytkeytyviä tehtäviä kuuluu sekä valtakunnallisena yksikkönä toimivalle keskusrikospoliisille että paikallisille poliisilaitoksille.

Keskusrikospoliisi torjuu poliisin hallinnosta annetun lain 9 §:n mukaan kansainvälistä, järjestäytynyttä, ammattimaista, taloudellista ja muuta vakavaa rikollisuutta. Keskusrikospoliisi muun muassa suorittaa pääsääntöisesti terrorismirikosten esitutkinnan. Se tutkii myös muut kansallisen turvallisuuden kannalta merkitykselliset rikokset kuin erikseen suojelupoliisin tutkittaviksi osoitetut maan- ja valtiopetokselliset rikokset. Keskusrikospoliisissa toimii niin sanottu PTR-keskus, jonka puitteissa poliisi, Rajavartiolaitos ja Tulli harjoittavat yhteistä rikostiedustelu- ja analyysitoimintaa. Toiminnan tarkoituksena on ylläpitää rikollisuuden tilannekuvaa, valmistella vakavan rajat ylittävän ja järjestäytyneen rikollisuuden torjuntakohteita, sarjoittaa rikoksia sekä valmistella rikostiedustelumuistioita ja uhka-arvioita. Keskusrikospoliisiin kuuluu myös vuonna 2015 perustettu kyberrikostorjuntakeskus.

Paikallispoliisille kuuluvat rikosten ennalta estämiseen, paljastamiseen, selvittämiseen ja syyteharkintaan saattamiseen ohella yleisen järjestyksen ja turvallisuuden ylläpitäminen. Viimeksi mainittuun tehtävään kuuluu muun muassa väkivaltaista radikalisoitumista ehkäisevän ja siihen varhaisvaiheessa puuttuvan toiminnan yhteensovittaminen paikallistasolla.

Muusta poliisiorganisaatiosta erotettiin 1.1.2016 poliisin valtakunnallisena yksikkönä toimiva suojelupoliisi, jonka toimivaltuuksien kehittämistä tämä esitys keskeisesti koskee. Suojelupoliisin tehtäviä käsitellään tästä syystä jäljempänä tarkemmin.

Kansallisen turvallisuuden ja valtiosuvereenisuuden kannalta merkitystä on Suomen ulkorajojen valvonnalla ja rajaturvallisuudella. Niiden ylläpitämisestä vastaa Rajavartiolaitos, jonka tehtävistä säädetään rajavartiolaissa (578/2005). Rajanylityspaikoilla toimivaltainen viran-

omainen on myös Tulli, joka tullin hallinnosta annetun lain (960/2012) mukaan vastaa muun muassa ulkomaanliikenteen tullivalvonnasta. Sekä Rajavartiolaitos että Tulli huolehtivat omiin tehtäviinsä liittyvien rikosten estämisestä, paljastamisesta ja selvittämisestä.

Maahanmuuttovirasto (Migri) käsittelee ja ratkaisee maahantuloon, maassa oleskeluun, pakolaisuuteen sekä Suomen kansalaisuuteen liittyviä asioita. Ulkomaalaisen maahantulon ja maassaolon edellytysten arvioinnin kannalta merkitystä on sillä, ettei ulkomaalaisen toiminnasta aiheudu vaaraa kansalliselle turvallisuudelle.

Kansallisen turvallisuusympäristön nopeassa muutoksessa ajanaisaisen tilannetiedon merkitys korostuu. Valtioneuvoston kansliassa toimii valtioneuvoston tilannekeskus, joka tuottaa reaaliaikaista turvallisuustapahtumatietoa ja toimivaltaisten viranomaisten tiedoista koottua tilannekuvaa. Tilannekeskus yhdistää eri viranomaisilta ja avoimista lähteistä saadut tiedot ja raportoi niiden pohjalta valtionjohdolle ja eri viranomaisille. Tilannekeskus toimii myös Suomen kansallisena yhteyspisteenä muun muassa Euroopan unionin suuntaan erikseen määritellyllä tavalla. Tällä hetkellä eduskunnassa on käsiteltävänä hallituksen esitys laiksi valtioneuvoston tilannekeskuksesta (HE 261/2016 vp).

Turvallisuusympäristön kansainvälistymisen myötä ulkomaita koskeva tiedonsaanti on noussut aiempaa tärkeämpään asemaan. Valtioneuvoston ohjesäännön (262/2003) 13 §:n mukaan ulko- ja turvallisuuspolitiikka, ulkopoliittisesti merkittävät kansainväliset asiat sekä kansainväliset suhteet yleisesti kuuluvat ulkoasiainministeriön toimialaan. Ulkoasiainministeriön ohjauksessa ja valvonnassa toimivat ulkomaanedustukseen kuuluvat edustustot. Edustustojen ulkoasiainhallintolain (204/2000) mukaisena tehtävänä on muun muassa edustaa Suomen valtiota sekä valvoa Suomen poliittisia ja muita etuja. Tehtäviensä suorittamiseksi ulkomaanedustustot keräävät asemamaita sekä niiden olosuhteita koskevia tietoja. Muiden tietojen ohella ulkoasiainhallinto kerää tietoja ulkomaiden turvallisuustilanteesta kansalaispalveluna ylläpitämäänsä matkustustiedotejärjestelmää varten. Edustustojen tiedonkeruutehtävien toteuttamisen menetelmiä ei ole säädelty kansallisesti, vaan toiminnan oikeudellisen kehyksen muodostavat Suomea sitovat kansainväliset sopimukset (diplomaattisia suhteita koskeva Wienin yleissopimus (SopS 3-5/1970) ja konsulisuhteita koskeva Wienin yleissopimus (SopS 49 ja 50/1980)).

Liikenne- ja viestintäministeriön hallinnonalalla toimii Viestintävirasto, jonka tehtävät määritellään laissa viestintähallinnosta (625/2001). Viestintävirastoon perustettiin vuoden 2014 alussa valtioneuvoston periaatepäätöksellä kyberturvallisuuskeskus. Kyberturvallisuuskeskuksen kautta Viestintävirasto tuottaa tietoturvapalveluita koko yhteiskunnalle ja edistää Suomen varautumista kyberuhkiin ja niiden aiheuttamien häiriötilanteiden hallintaan. Kyberturvallisuuskeskuksen tehtäviin kuuluu tietoturvauhkien ja loukkausten havainnointi ja selvittäminen sekä kyberturvallisuuden tilannekuvan ylläpito. HAVARO-järjestelmä on huoltovarmuuskriittisille toimijoille ja valtionhallinnolle suunnattu tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä. Sen tarkoitus on tuottaa tietoa tietoturvaloukkauksista, jotta organisaatiot voivat suojautua loukkauksilta ja tarvittaessa rajoittaa niiden aiheuttamia vahinkoja. Viestintävirasto vastaa HAVARO-järjestelmän ylläpidosta. Järjestelmä on toteutettu yhdessä Huoltovarmuuskeskuksen kanssa. Lisäksi Viestintävirasto tarjoaa valtionhallinnon toimijoille GovHAVARO-palvelua.

Edellä käsiteltyjen viranomaisten tehtävät kuuluvat laajassa mielessä kansallisen turvallisuuden alaan. Kansallisen turvallisuuden ylläpitämisen tai tiedonhankinnan kansalliseen turvallisuuteen kohdistuvista uhkista ei kuitenkaan voida katsoa olevan niiden tehtävien ytimessä. Tiedonhankintalakityöryhmän mietintö määritteli kansallisen turvallisuuden siviiliviranomaiseksi suojelupoliisin, jonka lakisääteisen tehtävän ytimen muodostaa kansallisen turvallisuu-

den suojaaminen. Tämän esityksen keskeinen tavoite on säädöspohjan luominen suojelupoliisin tiedustelutoimivaltuuksille kansallisen turvallisuuden suojaamiseksi.

Suojelupoliisin tehtävät

Suojelupoliisi on sisäministeriön alainen valtakunnallinen poliisiyksikkö, jonka tehtävänä on poliisin hallinnosta annetun lain 10 §:n (860/2015) 1 momentin mukaan 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. Suojelupoliisin tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi. Pykälän 2 momentin mukaan 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. 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. Määrittelemällä tehtävät oikeushyvälähtöisesti on ilmeisesti haluttu varmistaa suojelupoliisin valtion keskeisiä turvallisuusetuja suojelevan toiminnan mukautettavuus muuttuviin olosuhteisiin sekä viraston torjuntatoimialan yleisyys. Suojelupoliisin keskeisenä tehtävänä onkin tuottaa valtion keskeisiin turvallisuusetuihin kohdistuvista uhkista analysoitua informaatiota. Tämän tehtävänsä toteuttamiseksi suojelupoliisi tuottaa strategista ilmiö- ja toimintaympäristötietoa turvallisuusviranomaisille ja ylimmän valtiojohdon turvallisuuspoliittista päätöksentekoa varten.

Kansalliseen turvallisuuteen kohdistuvien uhkien estämiseksi ja paljastamiseksi suojelupoliisi suorittaa tiedonhankintaa, jossa hankitaan tarvittavaa informaatiota, järjestetään se hyödynnettävään muotoon, analysoidaan sitä ja raportoidaan siitä tai ryhdytään muihin tarvittaviin toimenpiteisiin. Tietoa saadaan avoimista lähteistä, omalla operatiivisella toiminnalla, kotimaisilta yhteistyökumppaneilta ja ulkomaisilta turvallisuus- ja tiedusteluviranomaisilta. Viraston tehtävien toteuttaminen edellyttää aktiivista ja laaja-alaista kansainvälisen ja Suomen turvallisuusympäristön seurantaa ja ennakoivaa tiedonhankintaa.

Suojelupoliisilla on myös muissa laeissa kuten esimerkiksi turvallisuusselvityslaissa (726/2014) ja ulkomaalaislaissa (301/2004) säädettyjä tehtäviä.

Voimassa olevan sisäministeriön määräyksen (SMDno-2015-2080) mukaan suojelupoliisin tehtäviä ovat muun muassa seuraavat:

- Suojelupoliisi tuottaa strategista tietoa Suomen turvallisuusympäristöstä ja siihen liittyvistä ilmiöistä turvallisuusviranomaisille ja ylimmän valtiojohdon päätöksentekoa varten. Tehtävää toteutetaan turvallisuustiedustelulla ja ylläpitämällä ajantasaista kansallista ja kansainvälistä tilannekuvaa sekä analysoimalla ja raportoimalla turvallisuusviranomaisille toimialaan kuuluvista olennaisista havainnoista. Tehtävä on tiedustelullinen ja sen toteuttaminen edellyttää aktiivista ja laaja-alaista Suomen turvallisuusympäristön seurantaa ja ennakoivaa tiedonhankintaa. Suojelupoliisi tuottaa valtion keskeisiin turvallisuusetuihin kohdistuvien uhkien ennalta estämisen kannalta välttämätöntä ja analysoitua tietoa.

- Suojelupoliisi tekee sisäministeriölle vuosittain ehdotuksen tiedonhankintaprioriteeteiksi sekä tarvittaessa ehdotuksen prioriteettien muuttamiseksi.

- Suojelupoliisin operatiiviset päätehtävät ovat terrorismin torjunta sekä ulkovaltojen tiedustelutoiminnan seuranta ja sen Suomen kannalta vahingollisten vaikutusten torjunta, estäminen ja paljastaminen.

- Suojelupoliisi tekee yhteistyötä eri viranomaisten kanssa joukkotuhoaseiden leviämisen estämiseksi.

- Suojelupoliisi torjuu, estää ja paljastaa valtion sisäiseen turvallisuuteen liittyvää väkivaltaista radikalisoitumista ja laitonta ääriliikehdintää sekä seuraa järjestäytyneen rikollisuuden kansalliselle turvallisuudelle aiheuttamia uhkia ja osallistuu toimialansa osalta Keskusrikospoliisin ylläpitämään valtakunnalliseen tilannekuvaan kokonais- ja vakavasta rikollisuudesta sekä torjuntatilanteesta.

- Suojelupoliisi laatii tarvittaessa valtiovierailuihin ja mittaviin kokouksiin liittyvät uhka-arviot ja osallistuu vierailuiden ja kokouksien turvallisuussuunnitteluun.

- Suojelupoliisi vastaa toimialaansa kuuluvan valtion turvallisuusympäristön analysoinnista sekä ylläpitää toimialansa kansallista ja kansainvälistä tilannekuvaa ja huolehtii uhka-arvion sisältävän tilannekuvan välittymisestä sisäministeriön, Poliisihallituksen, poliisiyksiköiden ja muiden asianomaisten viranomaisten käyttöön.

- Suojelupoliisi raportoi valtionjohdolle toimialaansa kuuluvista keskeisistä asioista. Suojelupoliisi osallistuu myös osaltaan valtionjohdon turvallisuustilannekuvan muodostamiseen.

- Suojelupoliisi tekee toimialaansa liittyvää ennalta estävää turvallisuustyötä antamalla sekä viranomaisille että yksityisille yhteisöille ohjausta ja neuvontaa sekä tekemällä henkilö- ja yritysturvallisuusselvityksiä.

- Suojelupoliisi antaa lausuntoja erityisesti ulkomaalaisten maahantuloa, maassa oleskelua ja kansalaisuuden myöntämistä koskevissa sekä muissa toimialaansa liittyvissä asioissa.

- Poliisihallinnossa suojelupoliisi vastaa rikoslain 12 (maanpetosrikokset) ja 13 luvussa (valtiopetosrikokset) tarkoitettujen rikosten estämisestä, paljastamisesta ja myös niiden selvittämisestä. Suojelupoliisi vastaa esitutkinnasta myös, jos rikoslain 17 luvun 1 §:ssä tarkoitettu rikos (julkinen kehotus rikokseen), 15 luvun 10 §:n 1 momentissa tarkoitettu rikos (törkeän rikoksen ilmoittamatta jättäminen) tai 15 luvun 11 §:ssä tarkoitettu rikos (rikoksentekijän suojeleminen) liittyy maan- tai valtiopetosrikokseen.

- Rikoslain 34 a luvun terrorismirikosten osalta suojelupoliisin tehtävänä on niiden estäminen ja paljastaminen. Terrorismirikosten esitutkinta suoritetaan Poliisihallituksen alaisessa poliisiyksikössä, jonka kanssa suojelupoliisi toimii yhteistyössä ja avustaa tarvittaessa esitutkinnassa. Suojelupoliisi voi erityisestä valtion turvallisuuteen perustuvasta syystä suorittaa terrorismiin liittyvän rikoksen esitutkinnan siten kuin suojelupoliisin ja Poliisihallituksen kanssa on sovittu.

- Suojelupoliisi avustaa ja toimii yhteistyössä esitutkintaa suorittavan yksikön kanssa myös muiden kuin edellä mainittujen Suomen sisäisen ja ulkoisen turvallisuuden kannalta merkityksellisten rikosten esitutkinnassa. Näitä ovat esimerkiksi rikoslain 11 ja 14 luvuissa mainitut teot.

Poliisin hallinnosta annetun lain 4 a §:n mukaan suojelupoliisin on ilmoitettava tehtäviinsä kuuluvista yhteiskunnallisesti merkittävistä asioista sisäministerille sekä lisäksi poliisiylijohta-

jalle, jos niillä on merkittävää vaikutusta muuhun poliisitoimeen. 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.

Suojelupoliisille säädetyn ennalta estävän tehtävän hoitamiseksi tiedonantovelvollisuutta täsmennetään poliisin hallinnosta annetussa asetuksessa (158/1996). Asetuksen 8 §:n mukaan suojelupoliisin tulee lakisääteisen tehtävänsä toteuttamiseksi antaa viranomaisille ja yhteisöille sellaisia ohjeita, neuvoja ja tietoja, jotka ovat tarpeen kansallisen turvallisuuden ylläpitämiseksi tai siihen kohdistuvien loukkausten estämiseksi.

Suojelupoliisin tiedonhankinta

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.

Julkisesti saatavilla olevan tiedon hankkiminen ei edellytä perustakseen erikseen säädettyä viranomaistoimivaltuutta. 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 rikostorjunnallisia 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.

Poliisioikeudelliset periaatteet

Poliisilain 1 luvussa säädetään niin sanotuista poliisioikeudellisista periaatteista, perusoikeuksien ja ihmisoikeuksien kunnioittamisesta (2 §), suhteellisuusperiaatteesta (3 §), vähimmän haitan periaatteesta (4 §) ja tarkoitussidonnaisuusperiaatteesta (5 §) sekä mahdollisuudesta luopua tehtävästä tai siirtää sitä (9 §). Yleisellä tasolla säädetyt toiminnan periaatteet koskevat kaikkien poliisitehtävien hoitoa ja kaikkea poliisivaltuuksien käyttöä. Nämä periaatteet ovat yleisiä, mutta ilmenevät välillisesti uudelleen myös useiden poliisilakiin sisältyvien yksittäisten säännösten sanamuodosta. Korostetun tärkeätä näiden periaatteiden noudattaminen on voimakeinojen käytön yhteydessä ja salaisten tiedonhankintakeinojen yhteydessä sekä yleensäkin puututtaessa poliisitoimenpiteiden yhteydessä muutoin olennaisin tavoin kansalaisten oikeuspiiriin.

Perusoikeuksien ja ihmisoikeuksien kunnioittamisesta koskevan poliisilain 1 luvun 2 §:n mukaan poliisin on valtaansa käyttäessään valittava ajateltavissa olevista vaihtoehdoista se, joka parhaiten ja vähimmällä haitalla edistää näiden oikeuksien toteutumista.

Suhteellisuusperiaatteella tarkoitetaan sitä, että käytettävien keinojen ja niiden aiheuttamien haittojen tulee olla järkevässä suhteessa tavoiteltuun päämäärään. Suhteellisuusperiaatteen ilmaiseva poliisilain 1 luvun 3 § kuuluu seuraavasti: ”Poliisin toimenpiteiden on oltava puolustettavia suhteessa tehtävän tärkeyteen, vaarallisuuteen ja kiireellisyyteen, tavoiteltavaan päämäärään, toimenpiteen kohteena olevan henkilön käyttäytymiseen, ikään, terveyteen ja muihin vastaaviin häneen liittyviin seikkoihin sekä muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin.

Suhteellisuusperiaatteen ajatuksen ilmentävä erityissäännös on lisäksi poliisilain 1 luvun 9 §:ssä otsikolla ”Toimenpiteestä luopuminen ja sen siirtäminen”. Säännöksen mukaan poliisilla on oikeus luopua toimenpiteestä, jos sen loppuunsaattaminen voisi johtaa tavoiteltavaan tulokseen nähden kohtuuttomiin seurauksiin. Säännöksellä pyritään estämään sellaisten tilanteiden syntyminen, joissa poliisivaltuuksien käyttö saattaisi aiheuttaa asianosaiselle tai sivulliselle henkilölle suurempaa haittaa kuin torjuttava oikeudenloukkaus tai häiriö.

Vähimmän haitan periaate ilmentää toimenpiteen tarpeellisuuden vaatimuksen noudattamisesta. Aikaisemmin puhuttiin yleisesti tarpeellisuuden periaatteesta. Poliisin toimenpiteet on suoritettava puuttumatta kenenkään oikeuksiin enempää tai aiheuttamatta suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Poliisi saa arvioida toimenpiteen tarpeellisuutta lähtökohtaisesti vain poliisille kuuluvien päämäärien saavuttamiseen nähden. Poliisitehtäviä suoritettaessa ei ole siten toimivaltajärjestelmän soveltamiseen nähden mahdollista pitää silmällä yhteiskunnan ”yleistä hyvää”.

Poliisityössä ei saa käyttää valtaa enempää kuin tilanne välttämättä vaatii. Poliisitehtävän yhteydessä on usein mahdollista harkita erilaisia toimenpiteitä tilanteen ratkaisemiseksi. Valintaa ohjaa välttämättömyyden vaatimus. Keinovalikoimasta tulee ottaa käyttöön se, josta aiheutuva haitta jää pienimmäksi. Tämä voi käytännössä merkitä sitä, ettei poliisi voi valita sille itselleen parhaiten sopivaa, kätevintä ja halvinta toimintatapaa. Periaatteen käytännön merkitys ilmenee ehkä selvimmin niissä tilanteissa, joissa poliisi joutuu harkitsemaan erityyppisten voimakeinojen tai salaisten tiedonhankintakeinojen käyttöä.

Tarpeellisuuden vaatimus ilmenee myös siten, että vain sellaisen vallan käyttäminen on oikeutettua, joka on omiaan johtamaan poliisin tavoittelemaan tulokseen. Henkilöön ei esimerkiksi saa kohdistaa telekuuntelua, vaikka telekuuntelun edellytykset näennäisesti olisivatkin olemassa, mikäli tilanteen osalta tiedetään, että telekuuntelulla ei todellista tavoitetta kuitenkaan tulla saavuttamaan. Tarpeellisuuden periaatteen unohtaminen merkitsisi silloin poliisitoimenpiteen muuttumista perusteettomaksi puuttumiseksi perus- ja ihmisoikeuksiin.

Poliisitoiminnassa saatetaan joutua puuttumaan voimakkaasti ja sangen konkreettisestikin toimen kohteena olevan henkilön oikeusasemaan. Tämä korostaa ehdotonta lainmukaisuuden vaatimusta kaikissa poliisitehtävissä. Ylimpien laillisuusvalvojien ratkaisukäytännössä on toisinaan jouduttu kiinnittämään huomiota siihen, että poliisi saa käyttää valtuuksiaan kulloisenkin tehtävän yhteydessä ainoastaan tähän tehtävään nimenomaisesti liittyviin tarkoituksiin. Ei ole siis sallittua käyttää valtaa jonkin sellaisen tehtävän näennäiseen suorittamiseen, johon vallankäyttö sinänsä voisi sopia, jos kuitenkin todellisena tavoitteena onkin luoda toimivaltaa kokonaan toiseen, sellaiseen toimenpiteeseen, johon puheena olevia valtuuksia ei olisi lainkaan oikeutta liittää. Poliisilain 1 luvun 5 §:n mukaan poliisi saa käyttää toimivaltuuttaan vain säädettyyn tarkoitukseen.

Salaisten tiedonhankintakeinojen käytön 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).

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.

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.

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 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 edellä mainitut poliisioikeudelliset periaatteet, joilla on tärkeä merkitys salaisessa tiedonhankinnassa.

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 rangaistusuhan täyttävään 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.

Poliisin hallinnosta annetun lain 10 §:n mukaan suojelupoliisi torjuu paitsi valtakunnan turvallisuutta vaarantavia rikoksia myös sitä vaarantavia hankkeita. Hankkeen käsitettä ei täsmennetä poliisin hallinnosta annetussa laissa tai sen esitöissä. Suojelupoliisin salaisten tiedonhankintakeinojen rikosperusteisuudesta seuraa, ettei niitä voida käyttää tietojen hankkimiseksi valtion turvallisuutta vaarantavista hankkeista.

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittänyt työryhmä käsitteli kysymystä suojelupoliisin tiedonhankintatoimivaltuuksien ulottamisesta hankkeiden torjuntaan. Työryhmän loppuraportin mukaan suojelupoliisille olisi harkittava uusia tiedustelullisia toimivaltuuksia, jotta se kykenee vastaamaan toimintaympäristönsä muutokseen. Kyse olisi valtakunnan turvallisuutta vaarantavien hankkeiden torjumiseksi tarpeellisten tietojen hankkimisesta tietolähteinä toimivilta henkilöiltä ja tietoverkoista, vaikka hankkeet eivät olekaan edenneet estettävän, paljastettavan tai selvitettävän rikoksen asteelle.

LUONNOS

Teletiedonhankintakeinot

Teletiedonhankintakeinoja ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, suostumusperusteinen televalvonta sekä 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. Näitä ovat: 1) Suomen itsemääräämisoikeuden vaarantaminen; 2) sotaan yllyttäminen; 3) maanpetos, törkeä maanpetos; 4) vakoilu, törkeä vakoilu; 5) turvallisuussalaisuuden paljastaminen; 6) luvaton tiedustelutoiminta; 7) rikoslain 34 a luvun 1 §:n 1 momentin 2–7 kohdassa tai mainitun pykälän 2 momentissa tarkoitettu terroristisessa tarkoituksessa tehty rikos; 8) terroristisessa tarkoituksessa tehtävän rikoksen valmistelu; 9) terroristiryhmän johtaminen; 10) terroristiryhmän toiminnan edistäminen; 11) koulutuksen antaminen terrorismirikoksen tekemistä varten; 12) kouluttautuminen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta; 13) värväys terrorismirikoksen tekemiseen; 14) terrorismin rahoittaminen; 15) terroristiryhmän rahoittaminen, jos teon vakavuus edellyttäisi vankeusrangaistusta; tai 16) matkustamiseen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta.

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.

LUONNOS

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 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 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 1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta; 2) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn rikokseen, josta

säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta; 3) seksikaupan kohteena olevan henkilön hyväksikäyttöön tai paritukseen; 4) huumausainerikokseen; 5) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun taikka 6) törkeään tulliselvitysrikokseen.

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 1) rikokseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta; 2) rikokseen, jonka johdosta teleosoite tai telepäätelaite on oikeudettomasti toisen hallussa; 3) teleosoitetta tai telepäätelaitetta käyttäen tehtävään lähestymiskiellon rikkomiseen, rikoslain 17 luvun 13 §:n 2 kohdassa tarkoitettuun ilkivaltaan, rikoslain 24 luvun 1 §:n 3 kohdassa tarkoitettuun kotirauhan rikkomiseen; 4) muuhun kuin 3 kohdassa tarkoitettuun teleosoitetta tai telepäätelaitetta käyttäen tehtävään rikokseen; tai 5) seksikaupan kohteena olevan henkilön hyväksikäyttöön. 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 päätöksentekohetkeä 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.

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 1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta; 2) seksikaupan kohteena olevan henkilön hyväksikäyttöön tai paritukseen; 3) huumausainerikokseen; 4) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun; 5) törkeään tulliselvitysrikokseen; taikka 6) suunnitelmalliseen, järjestäytyneeseen, ammattimaiseen, jatkuvaan tai toistuvaan rikolliseen toimintaan liittyvään varkauteen tai kätkemisrikokseen. 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 5 luvun 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 1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta; 2) huumausainerikokseen; 3) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun; tai 4) törkeään tulliselvitysrikokseen. 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 teknisessä 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 rat-

kaissut 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 ja muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta. Pykälän 3 momentin mukaan lupa voidaan antaa tai päätös tehdä enintään kuudeksi kuukaudeksi 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 on tarkoitus säätää rajanveto 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. Laista tai sen perusteluista ilmenee ainakin välillisesti, että säännöksessä mainitulla viestin sisällöllä tarkoitetaan nimenomaan viestin sisältöä telekuuntelun ja teknisen kuuntelun tarkoituksessa esimerkiksi silloin, kun viestintä tapahtuu kahden ihmisen välillä reaaliaikaisesti esimerkiksi tietokoneelta tai älypuhelimesta. Siten kyseiselle laitteelle jo tallentuneet tai talletetut asiakirjat, jotka eivät ole tekniseen kuunteluun tai telekuunteluun reaaliaikaisessa yhteydessä, kuuluvat teknisen laitetarkkailun piiriin. 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

Peitetoiminnan ja valeoston käytön edellytykset on säädetty erityisen tiukoiksi johtuen niiden salaiselle tiedonhankinnalle epätyypillisestä luonteesta.

Poliisilain 5 luvun 28 §: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 pykälän 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 on asunnossa on sallittua vain, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella. Kotietsinnästä säädetään erikseen.

Poliisilain 5 luvun 29 §:ssä säädetään rikoksentekokiellosta ja 30 §:ssä järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun osallistumisesta. Peitetoimintaa koskevasta esityksestä ja suunnitelmasta sekä peitetoiminnasta päättämisestä säädetään 5 luvun 31 ja 32 §:ssä. Peitetoiminnan laajentamisesta ja ratkaisusta peitetoiminnan edellytyksistä säädetään 34 ja 33 §:ssä.

Ennen kuin päätös peitetoiminnasta voidaan tehdä, edellytetään peitetoimintaa koskevaa esitystä ja suunnitelmaa. Poliisilain 5 luvun 31 §:n 1 momentin mukaan peitetoimintaa koskevassa esityksessä on mainittava: 1) toimenpiteen esittäjä; 2) tiedonhankinnan kohteena oleva henkilö riittävästi yksilöitynä; 3) toimenpiteen perusteena oleva rikos riittävästi yksilöitynä; 4) peitetoiminnan tavoite; 5) peitetoiminnan tarpeellisuus; 6) muut peitetoiminnan edellytysten

arviointia varten tarvittavat tiedot. Pykälän 2 momentin mukaan 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.

Poliisilain 5 luvun 31 §:ssä säädetään peitetoiminnasta päättämisestä. Keskusrikospoliisin tai suojelupoliisin päällikkö päättää peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies (1 momentti). Peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan (2 momentti). Pykälän 3 momentin mukaan päätös peitetoiminnasta on tehtävä kirjallisesti. Päätöksessä on mainittava: 1) toimenpiteen esittäjä; 2) peitetoiminnan toteuttava poliisiyksikkö ja peitetoiminnan toteuttamisesta vastaava poliisimies; 3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä; 4) tiedonhankinnan perusteena oleva rikos; 5) peitetoiminnan kohteena oleva henkilö, jonka voidaan perustellusti olettaa syyllistyvän 4 kohdassa tarkoitettuun rikokseen; 6) tosiseikat, joihin epäily ja peitetoiminnan edellytykset perustuvat; 7) peitetoiminnan tavoite ja toteuttamissuunnitelma; 8) päätöksen voimassaoloaika; 9) voidaanko peitetoiminnassa tehdä 30 §:ssä tarkoitettuja toimenpiteitä, ja toimenpiteiden perusteena olevat tosiseikat sekä peitetoiminnan mahdolliset rajoitukset ja ehdot. Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös (4 momentti).

Poliisilain 5 luvun 33 §:ssä säädetään tuomioistuimen tekemästä ratkaisusta peitetoiminnan edellytyksistä. Sen mukaan, jos peitetoiminnalla saatua tietoa on tarkoitus käyttää oikeudenkäynnissä syyllisyyttä tukevana selvityksenä, peitetoiminnasta päättäneen poliisimiehen on saatettava tuomioistuimen ratkaistavaksi, olivatko 28 §:n 2 momentissa tarkoitetut peitetoiminnan edellytykset olemassa tai oliko kysymys peitetoiminnasta 3 §:ssä tarkoitetuissa tapauksissa.

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 turvallisuu-

tensa 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 poliisilain 5 luvun 40–43 §:ssä. Kyseisen 40 §:n 1 momentin mukaan tarkoitetaan muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun esitutkintaviranomaisen ulkopuoliselta henkilöltä (tietolähde). Pykälän 2 momentin mukaan Poliisi saa pyytää tähän tarkoitukseen hyväksyttyä, henkilökohtaisilta ominaisuuksiltaan 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.

Lain 5 luvun 41 §:ssä säädetään tietolähdettä koskievien tietojen käsittelystä ja palkkion maksusta. Pykälän 1 momentin mukaan tietolähdettä koskevat tiedot voidaan tallettaa henkilörekisteriin. Tietojen käsittelyyn sovelletaan henkilötietojen käsittelystä poliisitoimessa annettua lakia (761/2003). Pykälän 2 momentin mukaan rekisteröidylle tietolähteelle voidaan maksaa palkkio. Perustellusta syystä palkkio voidaan maksaa myös rekisteröimättömälle tietolähteelle. Palkkion veronalaisuudesta säädetään erikseen.

Tietolähteen ohjatusta käytöstä päättämisestä säädetään 5 luvun 42 §:ssä. Pykälän 1 momentin mukaan keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies päättää tietolähteen ohjatusta käytöstä. Pykälän 2 momentin mukaan tietolähteen ohjattua käyttöä koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Pykälän 3 momentissa säädetään päätöksessä mainittavista asioista sekä kirjallisuusvaatimuksesta. Päätöksessä on mainittava: 1) toimenpiteen esittäjä; 2) tiedonhankinnan toteuttava poliisiyksikkö ja sen toteuttamisesta vastaava poliisimies; 3) tunnistetiedot tietolähteestä; 4) toimenpiteen peruste; 5) tiedonhankinnan tavoite ja toteuttamissuunnitelma; 6) päätöksen voimassaoloaika; 7) mahdolliset tietolähteen ohjatun käytön rajoitukset ja ehdot. Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Tietolähteen ohjatun käytön lopettamisesta on tehtävä kirjallinen päätös (4 momentti).

Valvotusta läpilaskusta ja sen edellytyksistä säädetään 5 luvun 43 §:ssä. Pykälän 1 momentin mukaan Poliisi 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 estämiseksi (valvottu läpilasku). Pykälän 2 momentin mukaan poliisi saa käyttää valvottua läpilaskua sellaisen rikoksen estämiseksi, 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. Viranomaisyhteistyöstä valvotun

läpilaskun toteuttamiseksi säädetään erikseen. 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 44 §:ssä.

Esitutkintatoimivaltuudet ja pakkokeinot

Suojelupoliisi on esitutkintalaissa (805/2011) tarkoitettu esitutkintaviranomainen. Esitutkintalain 2 luvun 1 §:ssä säädetään viranomaisista esitutkinnassa. Pykälän 1 momentin mukaan esitutkinnan toimittaa poliisi. Pykälän 2 momentin mukaan poliisin lisäksi esitutkintaviranomaisia ovat rajavartio-, tulli- ja sotilasviranomaiset siten kuin niiden esitutkintatoimivallasta säädetään rajavartiolaissa (578/2005), rikostorjunnasta Tullissa annetussa laissa (623/2015) ja sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa (255/2014).

Pakkokeinolain (806/2011) 2 luvun 9 §:n 1 momentin 1 kohdassa säädetään pidättämiseen oikeutetuista poliisivirkamiehistä. Kyseisen lainkohdan mukaan pidättämisestä päättää pidättämiseen oikeutettu virkamies. Pidättämiseen oikeutettuja virkamiehiä ovat: 1) poliisiylijohtaja, Poliisihallituksen poliisijohtaja, poliisiylitarkastaja ja poliisitarkastaja, poliisipäällikkö, apulaispoliisipäällikkö, keskusrikospoliisin päällikkö ja apulaispäällikkö, suojelupoliisin päällikkö, esitutkintatehtäviin määrätty apulaispäällikkö, esitutkintatehtäviin määrätty osastopäällikkö, esitutkintatehtäviin määrätty ylitarkastaja ja tarkastaja, rikosylitarkastaja, rikostarkastaja, rikosylikomisario, ylikomisario, rikoskomisario ja komisario.

Suojelupoliisi voi tehtävänsä mukaisesti käyttää siten esimerkiksi rikoksen selvittämiseksi pakkokeinolain 10 luvussa säädettyjä salaisia pakkokeinoja ja 7 luvussa säädettyjä takavarikkoa ja asiakirjan jäljentämistä koskevia toimivaltuuksia. Koska suojelupoliisi suorittaa esitutkinnan vain harvoin, tulee pakkokeinolaki suhteellisen harvoin sovellettavaksi suojelupoliisin toiminnassa.

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportin mukaan jos suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, tulisi oikeudenmukaisen oikeudenkäynnin turvaamiseksi harkita suojelupoliisin esitutkintatehtävien ja – toimivaltuuksien rajoittamista. Suojelupoliisi voisi osallistua edelleenkin tarpeen mukaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa.

Suojelupoliisin ja muiden kansallisen turvallisuuden kannalta merkittävien viranomaisten välinen yhteistyö

Edellä mainitut viranomaiset tekevät keskenään tiivistä yhteistyötä kunkin viranomaisen tehtävän edellyttämällä tavalla toimialaansa koskien.

Suojelupoliisin ja poliisilaitosten toiminnan välillä on keskeisiä turvallisuuden ylläpitämiseen liittyviä yhtymäkohtia. Suojelupoliisi ja poliisilaitokset vaihtavat tietoa yleistä järjestystä ja turvallisuutta sekä rikostorjuntaa koskien sekä toimivat muutoinkin yhteistyössä. Keskusrikospoliisin kanssa suojelupoliisi tekee kiinteää yhteistyötä erityisesti terrorismintorjunnassa sekä toimii asiantuntijana terrorismirikostutkinnoissa. Lisäksi suojelupoliisi tekee salaiseen tiedonhankintaan liittyvää yhteistyötä keskusrikospoliisin kanssa.

Suojelupoliisi tekee kansallisen turvallisuuden suojaamiseksi yhteistyötä sotilastiedustelun kanssa. Sotilastiedustelun kanssa tehtävää yhteistyötä käsitellään tarkemmin mietinnön muissa osissa.

Maahanmuuttoviraston kanssa tehtävä yhteistyö liittyy erityisesti maahantulon edellytysten selvittämiseen. Tässä tarkoituksessa suojelupoliisi antaa maahanmuuttoviraston päätöksenteon tueksi lausuntoja. Suojelupoliisi antaa lausuntoja myös kansalaisuusasioissa sekä muissa asioissa, joissa tietojen antaminen maahanmuuttoviraston päätöksenteon tueksi on tarpeen. Lisäksi suojelupoliisi tekee tiedonvaihto- ja muuta yhteistyötä maahanmuuttoviraston tietopalvelun kanssa. Migrin maatietopalvelu tuottaa strategisen tason tietoa turvapaikanhakijoiden, kiintiöpakolaisten ja maahanmuuttajien lähtömaista. Tiedot koskevat muun muassa lähtömaiden poliittisia ja yhteiskunnallisia olosuhteita, ihmisoikeus- ja turvallisuustilannetta, lainsäädäntöä ja arkielämään liittyviä asioita. Migrin tiedontuotanto koskee osittain samoja maita kuin suojelupoliisin, mistä johtuen nämä viranomaiset vaihtavat keskenään strategisia toimintaympäristötietoja ja tekevät esimerkiksi keskinäistä koulutusyhteistyötä.

Suojelupoliisin ja rajavartiolaitoksen yhteistyö liittyy lähinnä rajavalvonnan, rajatarkastusten ja rikostorjunnan tehtäviin. Yhteistyön pääasiallisia muotoja ovat viranomaisten välinen tiedonvaihto ja virka-apu.

Poliisin- tullin ja rajavartiolaitoksen välisestä yhteistyöstä on lisäksi säädetty erikseen. Suojelupoliisi tekee tiivistä yhteistyötä kaikkien PTR- viranomaisten kanssa kansallisen turvallisuuden suojaamiseksi. Suojelupoliisi ei ole varsinainen PTR-viranomainen, mutta osallistuu toimialaansa liittyvissä asioissa PTR-viranomaisten tekemään yhteistyöhön.

Suojelupoliisi on Viestintäviraston kyberturvallisuuskeskuksen ylläpitämän tilannekuvatoiminnon asiakas ja tarpeen mukaan suojelupoliisi tuottaa sille tietoja tilannekuvaa varten. Kyberturvallisuuskeskuksen tilannekeskuksen kanssa suojelupoliisi tekee yhteistyötä kansalliseen turvallisuuteen kohdistuvien tietoturvauhkien ennakoimisessa ja tällaisten tietoturvaloukkausten selvittämisessä.

Tietoturvauhkien torjunta

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 tarvittavan tiedon käytettävyys, eheys ja luottamuksellisuus. Laissa säädetään turvallisuusverkosta (TUVE), joka yhdistää samaan tietoliikenneverkkoon valtion johdon, ministeriöt, puolustusvoimat, rajavartioston, poliisin ja pelastustoimen.

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 huoltovarmuuskriittisistä yrityksistä hyödyntää suojautumisessaan myös jäljempänä käsiteltävää Viestintäviraston vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä (HAVARO).

Sähköisen viestinnän palveluista annetun lain (917/2014) 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.

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 sähköisen viestinnän palveluista annetun lain 272 § sen, että yritys, yhteisö tai viranomainen ottaa viestin sisällön manuaaliseen käsittelyyn.

Viestintäviraston Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, joka muun muassa ennaltaehkäisee, kerää tietoa ja selvittää yleisiin viestintäverkkoihin liittyviä ja niiden kautta suomalaisiin tahoihin suuntautuvia tietoturvaloukkauksia sekä tiedottaa merkittävistä tietoturvauhkista. Kyberturvallisuusstrategian mukaan kyberturvallisuuskeskuksen tehtävänä on myös yhdistetyn 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 emoorganisaatiot 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, kuten esimerkiksi Yhdistyneessä kuningaskunnassa (Government Communications Headquarters, GCHQ).

HAVARO on Viestintäviraston kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille ja valtionhallinnon toimijoille tarjoama tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä, toiminta perustuu sähköisen viestinnän palveluista annetun lain 272 §:ään. HAVARO-n tarkoituksena on tunnistaa erilaisten tunnisteiden avulla haitallista verkkoliikennettä ja tietoturvaa vaarantavia kehittyneitä verkkohyökkäyksiä (Advanced Persistent 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.

Suojelupoliisin tiedonhankinta ulkomailla

Poliisin hallinnosta annetun lain 10 §:n mukaan suojelupoliisin tehtävänä on torjua ulkomaista alkuperää olevia valtion turvallisuuteen kohdistuvia uhkia. Ulkomaista alkuperää olevia uhkia ovat muun muassa kansainvälinen terrorismi, ulkovaltojen Suomeen ja sen etuihin kohdistama vakoilu sekä joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö. Suojelupoliisin voimassa olevan tehtävämääräyksen mukaan viraston tehtävänä on myös analysoida valtion turvallisuusympäristöä ja ylläpitää toimialansa kansainvälistä tilannekuvaa. Suojelupoliisi raportoi kansainvälisen turvallisuustoimintaympäristön kehittymisestä muille turvallisuusviranomaisille ja Suomen ylimmälle valtionjohdolle.

Poliisin hallinnosta annetun lain säätämisen taustalla ollut parlamentaarisen poliisikomitean mietintö (komiteanmietintö 1986:16) korostaa valtiollisesta itsenäisyydestä arvona seuraavan, että valtiolla on oltava jatkuva valmius ulkoisen turvallisuutensa suojelemiseen. Mietinnön mukaan ulkoista turvallisuutta saattavat vaarantaa kaikki sellaiset pyrkimykset, joilla on vahingollinen vaikutus valtakunnan oikeuksiin ja etuihin taikka Suomen ja ulkovaltojen suhteisiin. Parlamentaarisen poliisikomitean mukaan nimenomaan suojelupoliisilla on keskeinen rooli tällaisten vaarojen ja haittojen torjumisessa.

Suomen turvallisuusympäristö on voimakkaasti kansainvälistynyt sitten parlamentaarisen poliisikomitean mietinnön julkaisemisen. Ulkomaita koskevilla tiedoilla on yhä suurempi merkitys niiden turvallisuusetujen suojelemisessa, jotka kuuluvat suojelupoliisin vastuulle.

Suojelupoliisin tiedonhankinnasta ulkomailla ei ole säädetty. Suojelupoliisin tiedonhankinta perustuu poliisilain mukaisten rikoksen estämistä ja paljastamista koskevien toimivaltuuksien käyttöön. Näitä toimivaltuuksia voi käyttää vain Suomen alueella.

Suojelupoliisin ulkomaita koskeva tiedonsaanti nojaa käytännössä sen harjoittaman kansainvälisen tiedusteluyhteistyön, avointen lähteiden seurannan sekä suojelupoliisin oman yhdysmiestoiminnan varaan.

Suojelupoliisi ja sen edeltäjät ovat Suomen itsenäistymisestä lähtien tehneet laajaa kahden- ja monenvälistä yhteistyötä ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa. Yhteistyön avulla varmistetaan valtion turvallisuuden ylläpitämiseksi tarpeellisten ulkomaisten tiedustelutietojen saaminen. Turvallisuuskysymysten yleisestä globalisoitumiskehityksestä ja siitä seuranneesta ulkomaisten tiedustelutietojen merkityksen korostumisesta johtuen suojelupoliisi on viime vuosina suunnitelmallisesti laajentanut kansainvälistä yhteistyöverkostoaan siten, että sen tällä hetkellä on katsottava kattavan kaikkien Suomen turvallisuuden kannalta olennaisten maiden tiedustelu- ja turvallisuusviranomaiset.

Kansainvälisestä tiedusteluyhteistyöstä on pidettävä erillään rikostorjuntaa palvelevat kansainväliset yhteistyömenettelyt. Suojelupoliisin toimialalla niiden merkitys on vähäinen. Yksi keskeinen syy tähän on se, että suojelupoliisin suorittaman rikostorjunnan kohdehenkilöt yleensä toimivat vieraan valtion puolesta ja usein sen virkamiehinäkin Suomen etuja vastaan. Rikoksenteosta hyötyvä valtio ei käytännössä anna rikoksen estämiseksi, paljastamiseksi tai selvittämiseksi tarvittavaa apua sille valtiolle - esimerkiksi Suomelle - johon rikos kohdistuu.

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

Suojelupoliisilla on viime vuosina ollut lyhyt- ja pitkäaikaisia yhdyshenkilöitä sijoitettuna eräissä Euroopan ulkopuolisissa maissa toimiviin Suomen suurlähetystöihin. Suojelupoliisin yhdyshenkilöt osallistuvat valtion turvallisuuteen kohdistuvien ulkoisten uhkien torjuntaan muun muassa ylläpitämällä yhteyksiä asemamaan sekä siellä edustettuina olevien muiden maiden viranomaisiin. Yhdyshenkilöiden toiminta pohjautuu poliisin kansainvälistä tietojenvaihtoa koskevien, henkilötietojen käsittelystä poliisitoimessa annetun lain säännösten soveltamiseen.

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportissa esitetään harkittavaksi, tulisiko suojelupoliisin tiedustelullisia toimivaltuuksia kehittää. Työryhmän loppuraportista ilmenee, että toimivaltuustarpeiden taustalla oleva toimintaympäristön muutos koskee ennen kaikkea Suomen ulkoista turvallisuustoimintaympäristöä. Työryhmän ehdotus, jonka mukaan suojelupoliisin tulisi voida hankkia tietoja valtakunnan turvallisuutta vaarantavien hankkeiden torjumiseksi tietolähdetoiminnan avulla, koskee myös ulkomailla tapahtuvaa toimintaa.

Suojelupoliisin toiminnan ohjaus

Sisäministeriö vastaa perustuslain 68 §:n 1 momentin, valtioneuvostosta annetun lain (175/2003) ja valtioneuvoston ohjesäännön mukaisesti poliisia koskevista ministeriötehtävistä. Suojelupoliisi on poliisin hallinnosta annetun lain muutoksella (860/2015) siirretty 1.1.2016 lukien Poliisihallituksen alaisesta valtakunnallisesta poliisiyksiköstä sisäministeriön alaiseksi valtakunnalliseksi poliisiyksiköksi.

Suojelupoliisin uusi hallinnollinen asema ilmenee poliisin hallinnosta annetun lain 1 §:n 3 momentista. Kyseisestä momentista ja saman pykälän 1 momentista johtuu, että sisäministeriö vastaa suojelupoliisin ohjauksesta ja valvonnasta sekä erikseen ministeriölle säädettävistä suojelupoliisin toimialan tehtävistä. Sisäministeriöstä annetun valtioneuvoston asetuksen (1056/2013) 5 §:n mukaan ministeriön työjärjestyksessä säädetään ministeriön tehtävien ja ratkaisuvallan käytön lisäksi ministeriön hallinnonalan ohjauksesta. Kyseisen työjärjestyksen 13 §:n (1562/2015) mukaan poliisiosasto käsittelee asiat, jotka koskevat suojelupoliisin toimintaa ja tulosohjausta.

Poliisin hallinnosta annetun lain 10 §:n 1 momentissa todetaan suojelupoliisin tehtävien lisäksi, että suojelupoliisi toimii sisäministeriön ohjauksessa. Momentin nojalla sisäministeriö asettaa esimerkiksi suojelupoliisin tiedonhankintaprioriteetit (HE 346/2014 vp s. 15). Asettamalla vuosittain kyseiset prioriteetit sisäministeriö ohjaa suojelupoliisin toimintaa suuntaamalla sen tiedonhankintaa. Suojelupoliisin tiedonhankintaprioriteettien asettamista edeltää niiden valmisteleva käsittely ulko- ja turvallisuuspoliittisessa ministerivaliokunnassa. Kyse onkin kokonaisuutena arvioituna valtioneuvostotason ohjaus- ja yhteensovittamismekanismista. Tästä mekanismista ei ole annettu laintasoisia säännöksiä.

Suojelupoliisin toiminnallisen ohjauksen ohella sisäministeriö vastaa suojelupoliisin tulosohjauksesta ja resursoinnista. Koska suojelupoliisin muusta poliisista poikkeavat tehtävät edellyttävät sen kohdalla muusta poliisista poikkeavaa tulosmittaristoa ja resurssijakomallia, suojelupoliisin toimintamenot on eriytetty omalle momentilleen poliisin toimintamenomomentista. Lisäksi sisäministeriö kirjaa valtion talousarvioon suojelupoliisille alustavat tulostavoitteet.

Sisäministeri kantaa poliittista vastuuta suojelupoliisin toiminnasta ja siksi hänen tulee olla tietoinen viraston toimialaan kuuluvista keskeisistä asioista. Tämän vuoksi suojelupoliisin on ilmoitettava tehtäviinsä kuuluvista yhteiskunnallisesti merkittävistä asioista sisäministerille sekä, silloin kuin niillä on merkittävää vaikutusta muuhun poliisitoimeen, myös poliisiylijohtajalle. Suojelupoliisin päällikön on lisäksi pidettävä sisäministeriö, tarkemmin sanoen sisäministeri, kansliapäällikkö ja poliisiosaston ylijohtaja, tietoisena suojelupoliisia koskevista asioista (HE 346/2014 vp, s. 15). Poliisin hallinnosta annetun lain 4 a § 2 momenttiin perustuvan informointivelvollisuuden lisäksi suojelupoliisin on 10 §:n 3 momentin nojalla ilmoitettava sisäministeriölle sellaisesta suunnittelemastaan hallinnon sisäisestä ratkaisusta tai olosuhteiden muutoksesta, jolla voi olla laatunsa tai laajuutensa vuoksi merkittävää vaikutusta sisäministeriön hyväksymien suojelupoliisin tulostavoitteiden ja toimintalinjojen toteutumiseen. Suojelupoliisi informoi myös tasavallan presidenttiä, pääministeriä ja ulkoasiainministeriä sekä eduskunnan perustuslaki-, hallinto- ja ulkoasiainvaliokuntia pitääkseen heidät ajan tasalla ulko- ja turvallisuuspolitiikkaan liittyvistä asioista ja turvallisuustilanteesta (HE 58/2009 vp, s. 19).

Poliisin hallinnosta annetun lain 10 §:n 4 momentin mukaan sisäministeriö voi yksittäistapauksessa ottaa ratkaistavakseen eräitä suojelupoliisin hallinnon sisäisiä asioita. Oikeus pidättää päätösvalta koskee ensinnäkin sisäministeriön hyväksymiä tulostavoitteita ja toimintalinjoja taikka niihin vaikuttavia asioita. Koska tiedonhankintaprioriteetit ovat sisäministeriön suojelupoliisille osoittamia toimintalinjoja, päätösvallan pidättäminen voi koskea esimerkiksi kyseisiä prioriteetteja tai niihin vaikuttavia asioita. Kyse on tältä osin eräänlaisesta strategisen tason ohjauksesta sisäministeriön ja suojelupoliisin välisessä suhteessa. Devoluutio-oikeus pitää toiseksi sisällään suojelupoliisin ja muiden poliisiyksiköiden välistä yhteistyötä tai työnjakoa koskevat asiat. Sisäministeriölle on säädetty hallinnonalan sisäisen ongelmatilanteen varalta päätösvalta ratkaista se, jos suojelupoliisi ja Poliisihallitus eivät tähän sovinnollisesti kykene. Ministeri, ja yksittäistapauksessa kansliapäällikkö, osastopäällikkö, erillisen yksikön päällikkö ja tulosyksikön päällikkö, voi pidättää itselleen päätösvallan asiassa, jonka ministeriön virkamies muutoin saisi ratkaista (Sisäministeriön työjärjestys 40 §).

Suojelupoliisin toiminnan laillisuusvalvonta

Suojelupoliisiin kohdistuvan laillisuusvalvonnan oikeusperustasta

Tässä esityksessä siviilitiedusteluun kohdistettavaa oikeudellista valvontaa käsitellään siltä osin kuin siitä säädetään poliisia koskevassa lainsäädännössä. Tiedustelutoimintaan kohdistuvaa valvontaa sekä suojelupoliisin laillisuusvalvontaa tarkastellaan tarkemmin tähän esitykseen liittyvässä esityksessä, jossa ehdotetaan säädettäväksi tiedustelutoiminnan valvonnasta.

Suojelupoliisin suorittaman tiedustelutoiminnan valvontaa varten ei ole erillistä valvontajärjestelmää, vaan tiedustelutoimintaa valvotaan samoin kuin muutakin suojelupoliisin toimintaa. Suojelupoliisi on poliisin toimivaltuuksia käyttävä poliisiyksikkö, jonka laillisuusvalvonta on järjestetty samoin kuin muunkin poliisin. Suojelupoliisin hallinnollinen asema muuttui Poliisihallituksen alaisuudesta sisäministeriön alaiseksi poliisin valtakunnalliseksi yksiköksi 1.1.2016 lukien, jolloin Poliisihallituksen vastuu suojelupoliisin laillisuusvalvonnasta siirtyi sisäministeriölle.

Sisäministeriön suorittama laillisuusvalvonta

Perustuslain 2 §:n 3 momentin mukaan kaiken julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Perustuslain 21 §:n mukaan jokaisella on oikeus saada asiansa käsitellyksi asianmukaisesti ja ilman aiheetonta viivytystä lain mukaan toimivaltaisessa tuomioistuimessa tai muussa viranomaisessa sekä oikeus saada

oikeuksiaan ja velvollisuuksiaan koskeva päätös tuomioistuimen tai muun riippumattoman lainkäyttöelimen käsiteltäväksi. Käsittelyn julkisuus sekä oikeus tulla kuulluksi, saada perusteltu päätös ja hakea muutosta samoin kuin muut oikeudenmukaisen oikeudenkäynnin ja hyvän hallinnon takeet turvataan lailla. Perustuslain 22 §:n mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Perustuslain 68 §:n 1 momentin mukaan kukin ministeriö vastaa toimialallaan hallinnon asianmukaisesta toiminnasta. Perustuslain 118 §:n 1 momentin mukaan virkamies on vastuussa virkatoimiensa lainmukaisuudesta. Pykälän 2 momentin mukaan esittelijä on vastuussa siitä, mitä hänen esittelystään on päätetty, jollei hän ole jättänyt päätökseen eriävää mielipidettä.

Valtion virkamieslain (750/1994) 14 §:n mukaan virkamiehen on suoritettava tehtävänsä asianmukaisesti ja viivytyksettä. Virkamiehen on myös noudatettava työnjohto- ja valvontamääräyksiä. Virkamiehen on käyttäydyttävä asemansa ja tehtäviensä edellyttämällä tavalla.

Poliisin hallinnosta annetun lain 4 §:n mukaan Poliisihallituksen tehtävänä on suunnitella, kehittää, johtaa ja valvoa poliisitoimintaa ja sen tukitoimintoja alaistensa poliisiyksiköiden osalta. Lain 1 §:n 1.1.2016 voimaan tulleen muutoksen mukaan suojelupoliisi on sisäministeriön alainen valtakunnallinen poliisiyksikkö.

Salaisten tiedonhankintakeinojen valvonnasta säädetään poliisilain 5 luvun 63 §:ssä. Pykälän 1 momentin mukaan tässä luvussa tarkoitettua tiedonhankintaa valvovat salaisia tiedonhankintakeinoja käyttävien yksiköiden päälliköt sekä sisäministeriö suojelupoliisin osalta ja Poliisihallitus alaistensa yksiköiden osalta. Pykälän 2 momentin mukaan sisäministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Pakkokeinolain 10 luvun 65 §:n 1 ja 2 momentissa on vastaavanlainen sääntely salaisten pakkokeinojen osalta.

Sisäministeriö suuntaa laillisuusvalvontaa erityisesti sellaiseen toimintaan, joka on ulkopuolisen kontrollin vaikeammin tavoitettavissa ja asioihin, jotka liittyvät perus- ja ihmisoikeuksien toteutumiseen. Laillisuusvalvonnan keskeiset toimintamuodot ovat hallintokanteluiden, kansalaiskirjeiden ja omien aloitteiden käsitteleminen, laillisuusvalvontatarkastukset ja henkilötietojen käsittelyn valvonta.

Sisäisen laillisuusvalvonnan tehtävänä on viranomaistoiminnan lainmukaisuuden, virkavelvollisuuksien ja ohjeistuksen noudattamisen valvonta. Laillisuusvalvonta tuottaa viranomaisen johdolle päätöksenteon tueksi oikeaa, mahdollisimman ajantasaista ja riittävää tietoa viranomaisen toiminnan lainmukaisuudesta. Laillisuusvalvonnalla on pyrittävä estämään ennalta mahdolliset virheet sekä paljastamaan ja saattamaan asianmukaiseen menettelyyn virheellinen tai lainvastainen toiminta mahdollisimman varhaisessa vaiheessa.

Sisäministeriön poliisiosasto vastaa sisäministeriössä suojelupoliisin laillisuusvalvonnan asianmukaisesta järjestämisestä. Suojelupoliisin päällikkö vastaa laillisuusvalvonnan järjestämisestä, sen resursoinnista ja kehittämisestä suojelupoliisissa. Suojelupoliisin päällikön on valvottava, että suojelupoliisissa suoritetaan säännönmukaisia laillisuustarkastuksia ja muuta laillisuusvalvontaa tämän ohjeen ja suojelupoliisin ohjeistuksen mukaisesti. Rekisterinpitäjä vastaa henkilötietojen käsittelyn laillisuudesta ja valvonnasta.

Suojelupoliisi tekee säännönmukaisia vuosittaiseen suunnitelmaan perustuvia laillisuusvalvontatarkastuksia suojelupoliisissa. Suojelupoliisi laatii vuosittain helmikuun loppuun mennessä vuosittaisen suojelupoliisin päällikön vahvistaman tarkastussuunnitelman, joka toimitetaan tiedoksi sisäministeriön poliisiosastolle.

Sisäministeriön poliisiosasto tekee kaksi vuosittaiseen suunnitelmaan perustuvaa laillisuusvalvontatarkastusta suojelupoliisissa. Sisäministeriön poliisiosaston tarkastuskertomukset ja erityisesti niiden havainnot ja toimenpidesuositukset käsitellään osaston johtoryhmässä. Merkittävistä virheistä ja puutteista sekä lainvastaisesta toiminnasta on viipymättä ilmoitettava poliisiosaston osastopäällikölle. Tarkastushavaintojen käsittely, määrättävät toimenpiteet ja toimenpiteiden toteutuksen seuranta on dokumentoitava.

Sisäministeriön poliisiosasto toteuttaa laillisuusvalvontaansa sisäministeriön sisäistä laillisuusvalvontaa koskevan ohjeen (SMDno-2016-329) mukaisesti. Sisäministeriön poliisiosasto vastaa ministeriössä suojelupoliisin laillisuusvalvonnasta. Sisäministeriön laillisuusvalvontaohjeessa on erillinen suojelupoliisia koskeva osuus. Sisäministeriön poliisiosasto tekee suojelupoliisin kaksi säännönmukaista tarkastusta vuosittain. Salaisten pakkokeinojen ja salaisen tiedonhankinnan osalta noudatetaan Poliisihallituksen poliisilain ja pakkokeinolain mukaisten salaisten tiedonhankintakeinojen käyttöä koskevaa määräystä eräin poikkeuksin. Tarkastuskertomukset toimitetaan tiedoksi eduskunnan oikeusasiamiehen kansliaan.

Sisäinen laillisuusvalvonta

Suojelupoliisin valvonta koostuu sisäisestä laillisuusvalvonnasta, laadunvalvonnasta ja sisäisestä tarkastuksesta. Suojelupoliisin päällikkö vastaa laillisuusvalvonnan järjestämisestä, sen resursoinnista ja kehittämisestä suojelupoliisissa. Suojelupoliisin päällikön tulee valvoa, että suojelupoliisissa suoritetaan säännönmukaisia laillisuustarkastuksia ja muuta laillisuusvalvontaa sisäministeriön laillisuusvalvontaohjeen ja suojelupoliisin oman ohjeistuksen mukaisesti. Toiminnan laillisuudesta vastaa jokainen suojelupoliisin virkamies, lähiesimies ja tulosyksikön päällikkö. Strategista toimintaa johtava apulaispäällikkö vastaa laillisuusvalvonnan ohjauksesta. Laillisuusvalvonnan käytännön järjestämisestä vastaa tehtävään määrätty virkamies.

Suojelupoliisi tekee säännönmukaisia vuosittaiseen suunnitelmaan perustuvia laillisuusvalvontatarkastuksia suojelupoliisissa. Laillisuusvalvontatarkastuksesta laaditaan aina tarkastuskertomus. Suojelupoliisin sisäisessä laillisuusvalvonnassa kiinnitetään erityistä huomiota perus- ja ihmisoikeuksiin voimakkaasti puuttuvien toimivaltuuksien käyttöön eli erityisesti salaisiin pakkokeinoihin ja salaisiin tiedonhankintakeinoihin (muotomääräysten noudattaminen, laissa säädettyjen ilmoitusten tekeminen, määräaikojen noudattaminen ja dokumentointi) sekä henkilötietojen ja asiakirjojen käsittelyyn.

Salaisten pakkokeinojen ja salaisten tiedonhankinnan valvonnasta

Poliisin suorittamien salaisten pakkokeinojen ja salaisen tiedonhankinnan osalta valvonnasta on säädetty erikseen. Pakkokeinolain 10 luvun 65 §:n mukaan poliisin salaisten pakkokeinojen käyttöä valvovat niitä käyttävien yksiköiden päälliköt ja Poliisihallitus alaistensa yksiköiden osalta. Suojelupoliisin osalta valvonnan suorittaa sisäministeriö. Poliisilain 5 luvun 63 §:ssä säädetään salaisen tiedonhankinnan valvonnasta. Pykälän mukaan poliisilain 5 luvussa tarkoitettua tiedonhankintaa valvovat salaisia tiedonhankintakeinoja käyttävien yksiköiden päälliköt ja Poliisihallitus alaistensa yksiköiden osalta. Sisäministeriö valvoo toimintaa suojelupoliisin osalta. Sisäministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten pakkokeinojen ja niiden suojaamisen käytöstä ja valvonnasta sekä salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Oikeusasiamiehelle annettavista rikoksen estämiseksi tai paljastamiseksi käytettyä salaista tiedonhankintaa koskevista kertomuksista säädetään poliisilaissa.

Salaisen tiedonhankinnan valvonnasta säädetään lisäksi esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta annetun valtioneuvoston asetuksen (122/2014) 3 luvun 21 §:ssä.

Pykälän mukaan Poliisihallitus asettaa salaisten pakkokeinojen ja salaisten tiedonhankintakeinojen käyttöä seuraamaan ryhmän, jonka jäseniksi voidaan määrätä Poliisihallituksen, Keskusrikospoliisin, suojelupoliisin ja poliisilaitoksen edustajat. Ryhmän jäseneksi kutsutaan sisäministeriön edustaja, Rajavartiolaitoksen esikunnan nimeämä Rajavartiolaitoksen edustaja, pääesikunnan nimeämä puolustusvoimien edustaja ja Tullin edustaja. Saman pykälän 2 momentin mukaan ryhmän tehtävänä on toiminnan, yhteistyön ja koulutuksen seuranta, toiminnassa ja yhteistyössä havaittujen tai laillisuusvalvonnan kannalta tärkeiden seikkojen käsitteleminen ja raportoiminen Poliisihallitukselle, kehittämisehdotusten tekeminen ja eduskunnan oikeusasiamiehelle annettavien kertomusten valmistelun yhteensovittaminen.

Suojelupoliisi noudattaa poliisin salaisen tiedonhankinnan järjestämisestä, käytöstä ja valvonnasta annettua Poliisihallituksen määräystä (POL-2014-3305) eräin täsmennyksin. Suojelupoliisiin on muun muassa muodostettu määräyksen mukainen vastuuhenkilöjärjestelmä. Vastuuhenkilöt valvovat salaisia pakkokeinoja ja salaista tiedonhankintaa ennakollisesti ja reaaliaikaisesti. Luotujen järjestelyjen puitteissa järjestelmiin tehtävät pakkokeinokirjaukset ja niiden oikeudellinen perusta tarkastetaan reaaliaikaisesti. Tämän lisäksi suojelupoliisin laillisuusvalvoja tarkastaa puolivuosittain kattavasti salaiset pakkokeinot ja salaiset tiedonhankintakeinot.

2.3 Kansainvälinen kehitys sekä ulkomaiden lainsäädäntö

Yleistä

Kansainvälisen vertailun jaksossa käsitellään Norjan, Tanskan ja Saksan siviili- ja sotilastiedustelua koskevaa lainsäädäntöä aihealueittain. Tähän esitykseen liittyvässä puolustusministeriön sotilastiedustelulainsäädäntöä koskevassa esityksessä käsitellään vastaavilta osin Ruotsin, Hollannin ja Sveitsin lainsäädäntöä. Vertailuvaltioiden tiedustelua koskevaa oikeudellista ja parlamentaarista valvontaa käsitellään OM:n tähän esitykseen liittyvässä esityksessä tiedustelutoiminnan valvonnasta.

Tiedustelulla suojataan kansallista turvallisuutta. Kansallisen turvallisuuden on perinteisesti katsottu kuuluvan valtiosuvereenisuuden ydinalueeseen. Tästä huolimatta kansainväliset ihmisoikeussopimukset rajoittavat sitä kuinka valtiot voivat kansallisessa lainsäädännössään säätää kansallisesta turvallisuudesta ja tiedustelusta.

Jäljempänä käsiteltävien vertailumaiden taloudelliset panostukset tiedustelupalveluidensa toimintaan ovat turvallisuustoimintaympäristön muuttuessa viime vuosina merkittävästi lisääntyneet. Esimerkiksi Tanskassa sisäisten turvallisuusuhkien torjunnasta vastaavan poliisin turvallisuuspalvelu PET:n (Politiets Efterretningstjeneste) budjetti kasvoi vuoden 2013 ja 2017 välillä 43 prosentilla ollen jälkimmäisenä vuonna 107 miljoonaa euroa, kun taas ulkomaan tiedonhankinnasta vastaavan puolustusvoimien tiedustelupalvelu FE:n (Forsvarets Efterretningstjeneste) budjetti samalla aikavälillä kasvoi 42 prosenttia 118 miljoonaan euroon. Tanska kuluttaa meneillään olevan vuoden aikana näin ollen yhteensä 225 miljoonaa euroa turvallisuus- ja tiedustelupalveluidensa toimintaan. Julkisuudessa olleiden tietojen mukaan Saksan liittovaltiotason siviiliturvallisuuspalvelu Bundesverfassungsschutzin (BfV) budjetti kasvoi vuoden 2014 ja 2017 välillä noin 60 prosenttia 349 miljoonaan euroon ja ulkomaan tiedustelupalvelu Bundesnachrichtendienstin (BND) budjetti saman ajanjakson aikana 35 prosenttia 833 miljoonaan euroon ja Militärischer Abschirmsdienstin (MAD) budjetti 3,8 miljoonaan euroon. Yhteensä Saksa rahoittaa liittovaltion turvallisuus- ja tiedustelupalveluiden toimintaa vuonna 2017 1,4 miljardilla eurolla. Lukuun eivät lainkaan sisälly osavaltioiden turvallisuuspalveluiden menot. Saksan jokaisella kuudellatoista osavaltiolla on oma turvallisuuspalvelunsa.

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 joukkoosastoille. 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. Yhteistyön 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 esityksessä 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 tietoliikennetiedus-

telusta, 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 esityksessä 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.

Tanska

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 olosuh-

teista, 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.

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 sääde-

tään 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 väärentäminen, 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 kirjal-

lisessa 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 yhteiskuntajärjestykseen, olemassaoloon tai turvallisuuteen taikka Saksan ulkoiseen turvallisuuteen. Ilmoitusvelvollisuus koskee näin ollen sellaisia rikoksia, joiden laa-

jasti 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 omaaloitteisesti 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 laeissa säädetään edellytyksistä, joiden mukaan 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.

2.4 Kansainvälisten sopimusten ihmisoikeusvelvoitteet

Yleistä

Perus- ja ihmisoikeusnäkökulma on korostunut sellaisten toimivaltuuksien osalta, joita käytetään salaa niiden kohteelta, koska sellaisilla toimivaltuuksilla puututaan usein perustavaa laatua oleviin oikeuksiin, vieläpä niiden ydinalueelle. Siviilitiedustelussa puuttuminen kohdistuu erityisesti yksityiselämän ja luottamuksellisen viestin suojaan sekä oikeusturvaan.

Tässä osiossa käsitellään YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälinen yleissopimuksen ja Euroopan ihmisoikeussopimuksen olennaisia säännöksiä sekä niitä selventävää ratkaisukäytäntöä. Osiossa käsitellään erityisesti yksityiselämän suojasta ja erityisesti luottamuksellisen viestin salaisuudesta annettuja ratkaisuja.

LUONNOS

KP-sopimus

YK:n yleiskokouksen vuonna 1966 hyväksymä kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (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.

Euroopan ihmisoikeussopimus

Yksityiselämän suoja

Yleistä

Yksityiselämän ja luottamuksellisen viestin suojaan puuttuvien keinojen säätämisen sallittavuutta arvioitaessa on KP-sopimusta suurempi käytännön merkitys Euroopan neuvoston piirissä vuonna 1950 tehdyllä Euroopan ihmisoikeussopimuksella (SopS 63/1999, EIS), 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.

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 demokraattisessa yhteiskunnassa välttämätöntä 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.

EIS vakiintuneen ratkaisukäytännön mukaan EIS 8(1) artiklassa mainitut yksityiselämän ja kirjeenvaihdon käsitteet pitävät sisällään sekä puhelinviestinnän, sähköpostiviestinnän ja 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, 2.8.1984, Weber ja Saravia v. Saksa, 29.6.2006, P.G. ja J.H. v. Yhdistynyt Kuningaskunta, 25.9.2001). Tunnistamistietojen osalta tuomioistuin 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 käyttää 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, 4.12.2008). Pelkkä sellaisen lainsäädännön olemassaolo, joka mahdollistaa viestintäyhteyksien salaisen tarkkailun, puuttuu viestinnän osapuolten ja potentiaalistenkin 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. Kyseisen 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.

Edellä sanotusta myös seuraa, ettei henkilön, saadakseen 8 artiklan loukkaamista koskevan väitteensä tutkituksi EIT:ssä, välttämättä tarvitse konkreettisesti osoittaa, että viranomaiset olisivat puuttuneet hänen yksityiselämäänsä tai viestintäänsä. Riittävää on, että hän kuuluu sellaiseen ihmisryhmään, jonka voidaan kansallisen lain säännösten perusteella kohtuudella olettaa joutuvan salaisten valvontatoimenpiteiden kohteeksi. Jos kansallinen lainsäädäntö on luonteeltaan sellainen, että se mahdollistaa kenen hyvänsä henkilön viestintään kohdistuvan tarkkailun, ei asian tutkittavaksi saattaminen EIT:ssä edellytä edes tällaiseen ihmisryhmään kuulumista. Vastaavasti, vaikka henkilöön kohdistuvan salaisen tarkkailun todennäköisyys olisi sinänsä vähäinen, mutta tehokkaat kansalliset oikeussuojakeinot puuttuvat, on hänen voitava tutkituttaa EIT:ssä väitteensä EIS 8 artiklan mukaisten oikeuksiensa loukkaamisesta (Klass v. Saksa, Kennedy v. Yhdistynyt Kuningaskunta, 18.5.2010, Zakharov v. Venäjä, 4.12.2015, Szabo & Vissy v Unkari, 12.1.2016). Mahdollisuuksiin saada oikeussuojaa EIT:ssä vaikuttavat näin ollen niin valittajan tausta, kansallisen lainsäädännön luonne kuin myös kansallisten oikeussuojakeinojen riittävyys.

Sallittu puuttuminen EIS 8(1) artiklan mukaisiin oikeuksiin

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, kunhan se tapahtuu EIS 8(2) artiklan edellyttämissä puitteissa. EIS 8(2) 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.

Vaatimus puuttumisen perustumisesta lakiin

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,16.2.2000, Telegraaf Media Nederland Landelijke Media B.V. ja muut v. Alankomaat, 22.11.2012, Rotaru v. Romania, 4.5.2000).

EIT on ratkaisuissaan toistuvasti korostanut sitä, että yksityiselämän suojaan puuttuvat 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, 24.4.1990 Lambert ja muut v. Ranska, 5.6.2015). Sen on oltava tarpeeksi selkeä ["sufficiently clear in its terms"] antaakseen riittävän osoituksen ["an adequate indication"] siitä, missä olosuhteissa ja millä edellytyksillä kansalaiset voivat joutua salaisten viranomaistoimenpiteiden kohteeksi (Kopp v. Saksa, Kruslin v. Ranska, 24.4.1990 Huvig v. Ranska). Laki ei voi olla sellainen, että se mahdollistaa salaisen tarkkailun kohdistamisen sattumanvaraisesti keneen tahansa (Amann v. Sveitsi). Esimerkiksi pelkkä laissa oleva maininta siitä, että salaisia valtuuksia saadaan käyttää kansallisen turvallisuuden suojaamiseksi, ei ole riittävä ennakoitavuusvaatimuksen täyttämiseksi (Zakharov v. Venäjä). Toisaalta kansallisen lain ei voida edellyttää täsmällisesti ja tyhjentävästi luetteloivan kaikkia niitä tilanteita, joissa viranomaiset saavat käyttää salaisia valtuuksia. Lain säännöksen, jonka mukaan salaisten valtuuksien käyttöperusteena on terrorismin uhka, on esimerkiksi katsottava täyttävän ihmisoikeussopimuksen asettaman ennakoitavuusvaatimuksen (Szabo & Vissy v. Unkari).

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 (esim. Silver ja muut v. Yhdistynyt Kuningaskunta, 25.3.1983, 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, 30.7.1998, Prado Bugallo v. Espanja, 18.2.2003 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 tietoliikennetiedustelun tai siihen läheisesti vertautuvien menetelmien ihmisoikeussopimuksen mukaisuutta neljässä tärkeässä viime vuosina antamassaan ratkaisussa. Tapauksessa Liberty ja muut v. Yhdistynyt Kuningaskunta se katsoi tietoliikennetiedustelun 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. Loppuvuodesta 2015 antamassaan ratkaisussa Zakharov v. Venäjä tuomioistuin katsoi, että Venäjän lainsäädäntö oli ihmisoikeussopimuksen vastainen niin siksi, ettei se täyttänyt EIS 8 artiklan asettamia laatuvaatimuksia, kuin siksi, ettei sen mahdollistama puuttuminen ollut artiklassa tarkoitetulla tavalla demokraattisessa yhteiskunnassa välttämätön. Alkuvuodesta 2016 antamassaan ratkaisussa Szabo & Vissy v. Unkari tuomioistuin totesi Unkarin lain ihmisoikeussopimuksen vastaiseksi ennen kaikkea sillä perusteella, että se rikkoi puuttumisen välttämättömyyttä demokraattisessa yhteiskunnassa koskevaa vaatimusta vastaan. Luettavuuden helpottamiseksi kaikki neljä edellä mainittua tietoliikennetiedustelua koskevaa keskeistä ratkaisua käsitellään kokonaisuudessaan tämän otsikon alla. Yksittäisiä niistä esiin nousevia huomioita esitetään jäljempänä, käsiteltäessä EIS 8 artiklan vaatimusta puuttumisen välttämättömyydestä demokraattisessa yhteiskunnassa.

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 sisäministerin 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(2) 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.

Tuore ratkaisu Zakharov v. Venäjä on merkittävä siksi, että EIT siinä otti kantaa paitsi Venäjän lain muodolliseen sisältöön, myös laajasti lain käytännön soveltamiseen. Ratkaisu koski Venäjän sisäisen turvallisuuspalvelu FSB:n omasta puolestaan ja muiden viranomaisten toimeksiannosta harjoittamaa posti-, tele- ja muun viestiliikenteen valvontaa, josta oli säädetty kansallisessa laissa. Lain mukaan Venäjällä perusoikeutena voimassa olevaan luottamuksellisen viestin suojaan saatiin puuttua 1) tietyn vakavuusasteen rikosten estämiseksi, paljastamiseksi ja selvittämiseksi sekä sellaisiin rikoksiin syyllistyvien tai syyllistyneiden henkilöiden

tunnistamiseksi, 2) etsintäkuulutettujen ja kadonneiden henkilöiden jäljittämiseksi, ja 3) tiedon hankkimiseksi tapahtumista tai toiminnasta, joka vaarantavat Venäjän kansallista, sotilaallista, taloudellista tai ekologista turvallisuutta. Päätöksen luottamukselliseen viestintään puuttumisesta teki tuomioistuin, ja kansallinen laki sisälsi säännökset hankittujen tietojen tallentamisesta, käytöstä, hävittämisestä ja luovuttamisesta sekä tiedonhankinnan kohdehenkilölle ilmoittamisesta.

Tuomioistuin katsoi Venäjän lainsäädännön EIS 8 artiklan vastaiseksi ennen kaikkea seuraavilla perusteilla:

- Kansallinen laki ei lainkaan täsmentänyt tai kuvannut, millaisten tapahtumien tai millaisen toiminnan oli katsottava voivan vaarantaa Venäjän kansallista, sotilaallista, taloudellista tai ekologista turvallisuutta, mistä syystä laki ei täyttänyt EIS 8 artiklasta seuraavaa ennakoitavuusvaatimusta. Turvallisuusviranomaisille jätetty valta harkita, minkälaiset ja kuinka vakavat tapahtumat ja toiminnat perustivat oikeuden salaiseen valvontaan, oli lähes rajaton. Vaikka Venäjällä oli säädetty oikeudellisesta lupamenettelystä ja tällainen menettely normaalisti muodostaa tärkeä takeen viranomaistoiminnan mielivaltaisuutta vastaan, ei menettely tässä tapauksessa ollut riittävän tehokas johtuen siitä, että tuomioistuimen lupaharkintaa ohjaavat laissa säädetyt kriteerit olivat liian epämääräiset.

- Kansallinen laki ei sisältänyt säännöksiä siitä, missä tilanteissa salaisen tarkkailun käyttö oli lopetettava. Laki määritteli tarkkailutoimenpiteiden maksimaaliseksi kestoksi kuusi kuukautta, mitä tuomioistuin piti sinänsä asianmukaisena. Laissa ei kuitenkaan säädetty, että toimivaltuuden käyttö oli lopetettava ennen määräajan päättymistä, jos käytön edellytykset eivät enää täyttyneet. Sääntely ei näin ollen tältäkään osin sisältänyt riittäviä takeita toimivaltuuksien mielivaltaista käyttöä vastaan.

- Kansallisen lain mukaan tarkkailutoimenpiteillä hankitut tiedot oli hävitettävä kuuden kuukauden jälkeen, jos toimenpiteiden kohdehenkilöä vastaan ei ollut nostettu syytettä. Säilytysaikaa koskevaa sääntelyä tuomioistuin piti sinänsä asianmukaisena, mutta katsoi EIS:n vastaiseksi sen, että säilyttäminen koski myös tietoja, jotka olivat selvästi epäolennaisia. Laki ei toisin sanoen velvoittanut viranomaisia välittömästi hävittämään asiaankuulumattomiksi toteamiaan tietoja.

- EIT piti tärkeänä periaatteellisena oikeusturvatakeena sitä, että Venäjän lain mukaan luottamuksellisen viestin suojaan puuttuvista tiedonhankintakeinoista päätti tuomioistuin viranomaisen perustellusta hakemuksesta. Laki ei kuitenkaan sisältänyt riittäviä tuomioistuimen oikeudellista harkintaa ohjaavia kriteerejä. Uhat, jotka saattoivat antaa aiheen salaiseen tarkkailuun, oli määritelty laissa niin väljästi, että päätöksenteon tosiasiassa voitiin katsoa kuuluvan pikemmin hakemuksen esittävälle turvallisuusviranomaiselle kuin sen muodollisesti hyväksyvälle tuomioistuimelle. Laki ei myöskään asettanut hakemuksen hyväksymisen edellytykseksi, että hakemuksen kohteena olevan tiedonhankintakeinon käyttö oli välttämätöntä (necessary; katso käsitteen merkityssisältöä koskeva keskustelu otsikon "Puuttumisen välttämättömyys demokraattisessa yhteiskunnassa" alla) ja suhteellista. Lisäksi EIT totesi, että Venäjän tuomioistuimet eivät tosiasiassa yleensä edellyttäneet hakemusten perustelemista tai niitä tukevan kirjallisen aineiston esittämistä, vaan käytännössä hakemusten hyväksymiseen riitti, että turvallisuusviranomainen esitti yksilöimättömän väitteen kansallisen, sotilaallisen, taloudellisen tai ekologisen turvallisuuden vaarantumisesta.

- EIT viittasi aiempaan ratkaisukäytäntöönsä (mm. Klass v. Saksa, Liberty and others v. Yhdistynyt Kuningaskunta ja Kennedy v. Yhdistynyt Kuningaskunta), jonka mukaan luottamuksellisen viestin suojaan puuttuvaa tiedonhankintamenetelmää koskevasta päätöksestä on käy-

tävä selvästi ilmi toimenpiteen kohdehenkilö tai muu yksilöivä tekijä ("a specific person to be placed under surveillance or a single set of premises as the premises in respect of which the authorization is ordered"). Esimerkkeinä tällaisista yksilöivistä tekijöistä tuomioistuin mainitsi nimi-, osoite- ja puhelinnumerotiedot sekä "muut relevantit tiedot". (Ratkaisun Weber & Saravia v. Saksa perusteella tällaisia "muita relevantteja tietoja" voivat olla riittävän yksilöidyt hakuehdot.) Venäjän laki ei asettanut mitään kriteerejä sille, kuinka luottamuksellisen viestin suojaan puuttuvat toimenpiteet oli henkilöllisesti tai muutenkaan kohdennettava. Näin ollen tuomioistuimet olivat esimerkiksi myöntäneet lupia, jotka oikeuttivat kaikkien tietyllä alueella oleskelevien henkilöiden puhelinyhteyksien kuunteluun. Eräissä tapauksissa luvat eivät sisältäneet tietoa luvan voimassaoloajasta. Näin ollen viranomaisilla jäi erittäin laaja harkintavalta sen suhteen, keiden puhelinyhteyksiä ja kuinka kauan ne kuuntelivat.

- Kansallinen laki sääti kiiretilanteiden päätöksentekomenettelystä siten, että viranomaiset ilman tuomioistuimen lupaa saivat kuunnella luottamuksellisia viestiyhteyksiä 48 tunnin ajan. Viranomaisen oli ilmoitettava kiirepäätöksestään tuomioistuimelle 24 tunnin sisällä, ja jos tuomioistuin ei vahvistanut lupaa 48 tunnin kuluttua kuuntelun aloittamisesta, oli se lopetettava. EIT on aiemmassa ratkaisukäytännössään katsonut, että erityissäännökset kiiretilanteiden päätöksentekomenettelystä voivat olla hyväksyttäviä, jos kansallisesta laista selvästi ilmenee, että sellaista päätöksentekomenettelyä voidaan käyttää vain poikkeuksellisissa tapauksissa ja välttämättömien syiden ollessa käsillä (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria). Venäjän laki ei kuitenkaan täyttänyt näitä ehtoja, sillä se ei sisältänyt mitään kiiretilanteiden päätöksentekomenettelyn käyttöä rajoittavia kriteereitä. Niin ollen laki tosiasiassa jätti viranomaisille avoimen harkintavallan päättää, missä tilanteissa menettelyn käytölle oli peruste. Laki ei myöskään säätänyt tuomioistuimen mahdollisuudesta jälkikäteen arvioida, oliko menettelyn käyttö ollut perusteltua, eikä siitä, että perusteettoman viranomaispäätöksen nojalla kerätyt tiedot oli hävitettävä.

- Venäjän viestintäministeriö oli määräyksellään velvoittanut kaikki viestintäpalveluiden tarjoajat asentamaan tiloihinsa laitteistoa, joka antoi turvallisuusviranomaisille suoran pääsyn kaikkien henkilöiden kaikkiin matkapuhelinyhteyksiin. Lisäksi viestintäministeriö oli määrännyt palveluntarjoajat muodostamaan tietokantoja, joihin kolmen vuoden ajaksi tallennettiin kaikkien asiakkaiden kaikkia viestiyhteyksiä koskevat tiedot. Ministeriön määräyksen mukaan turvallisuusviranomaisille oli annettava tietokantoihin etäkäyttöyhteys. Venäjän laki puolestaan ei velvoittanut turvallisuusviranomaisia esittämään salaista tarkkailutoimenpidettä koskevaa tuomioistuimen lupaa palveluntarjoajalle ennen toimenpiteen toteuttamista. EIT:n mukaan järjestelmä, jossa viranomaisille oli teknisesti luotu mahdollisuus siepata kenen hyvänsä henkilön viestintä suoraan siihen katsomatta, oliko toimenpiteeseen lupa vai ei, oli erityisen altis väärinkäytöksille.

- EIT on aiemmassa ratkaisukäytännössään (mm. Kennedy v. Yhdistynyt Kuningaskunta) korostanut, että luottamuksellisen viestin suojaan puuttuvista viranomaistoimenpiteistä tulee pitää tarkkaa lokia laillisuusvalvontaa varten. Venäjän laki ei kuitenkaan edellyttänyt lokin pitämistä vaan suoranaisesti kielsi sen. Kun Venäjän viranomaisille oli annettu suora käyttöyhteys kansalaisten viestiyhteyksiä koskeviin tietoihin ja kun käyttöyhteyden avulla suoritettuja viranomaistoimenpiteitä ei toisaalta dokumentoitu mitenkään, seurasi tästä, ettei laillisuusvalvojalla ollut mitään reaalista mahdollisuutta saada tietoa viranomaisten lainvastaisista toimenpiteistä.

- Lupien myöntämisestä vastaaville tuomioistuimille ei ollut säädetty toimivaltaa valvoa, että luvat toimeenpantiin lainmukaisesti. Tämän sijaan laillisuusvalvonnan toteuttaminen oli kansallisessa laissa osoitettu syyttäjälaitoksen tehtäväksi. Aiempaan ratkaisukäytäntöönsä perustuen EIT katsoi, että syyttäjien asema Venäjällä ei ollut riittävän itsenäinen suhteessa valvot-

taviin. Jo ratkaisussaan Iordachi and Others v. Moldova EIT oli todennut, että laillisuusvalvontatehtävien osoittaminen valtakunnansyyttäjänvirastolle ja sen alaiselle syyttäjälaitokselle ei täytä laillisuusvalvonnan riippumattomuuden vaatimusta. Venäjän osalta EIT totesi nyt, että syyttäjälaitoksen riippumattomuuden toimeenpanovallasta on omiaan asettamaan kyseenalaiseksi se seikka, että syyttäjät nimitti ja heidät erotti viroistaan valtakunnansyyttäjä tämän neuvoteltua nimittämisestä tai erottamisesta alueellisten toimeenpanoviranomaisten kanssa. Lisäksi laillisuusvalvontatehtävien kuuluminen syyttäjille saattoi luoda eturistiriitatilanteita, sillä Venäjällä syyttäjät myönsivät luvan sellaisiin luottamuksellisen viestin suojaan puuttuviin toimenpiteisiin, jotka suoritettiin esitutkinnan aikana.

- Laillisuusvalvojan riippumattomuuden kyseenalaistamisen lisäksi EIT katsoi, että syyttäjille säädetyt laillisuusvalvontatoimivaltuudet olivat riittämättömät tehokkaan ja jatkuvan valvonnan suorittamiseksi. Venäjän laki sääti syyttäjien oikeudesta suorittaa turvallisuusviranomaisten toimintaan kohdistuvia laillisuusvalvontatarkastuksia, joiden puitteissa oli pääsy salassa pidettävään aineistoon. EIT:n mukaan syyttäjien pääsyä salassa pidettäviin tietoihin oli tästä huolimatta rajattu tavalla, joka kyseenalaisti laillisuusvalvonnan tehokkuuden, sillä oikeutta tutustua peitetoimintaa koskeviin tietoihin ei ollut. Laillisuusvalvojien oikeus tutustua turvallisuuspalvelun vastavakoilutehtäviin liittyviin luottamuksellisen viestinnän suojaan puuttuviin toimenpiteisiin taas rajoittui tapauksiin, joissa toimenpiteen kohdehenkilö oli kannellut toimenpiteestä. Kun turvallisuusviranomaisilla ei ollut velvoitetta ilmoittaa toimenpiteestä kohdehenkilölle, oli kantelun mahdollisuus olematon, mistä puolestaan seurasi, että turvallisuuspalvelun vastavakoilutoiminto oli tosiasiassa laillisuusvalvonnan ulottumattomissa.

- Kansallisten säännösten mukaan laillisuusvalvontaa toteuttavalla syyttäjällä oli oikeus määrätä turvallisuusviranomaiset lopettamaan lainvastaisen tiedonhankinnan samoin kuin ryhtyä toimenpiteisiin siitä vastaavien henkilöiden saattamiseksi oikeudelliseen edesvastuuseen. EIT:n totesi, ettei sääntely ollut riittävää, sillä laki ei edellyttänyt, että lainvastaisesti hankitut tiedot hävitetään.

- EIT piti laillisuusvalvontaa koskevaa sääntelyä puutteellisena myös siltä osin, ettei se edellyttänyt laillisuusvalvonnassa tehtyjen havaintojen riittävän läpinäkyvää raportointia. Kansallisen lain mukaan syyttäjien tuli raportoida valvontahavainnoistaan puolivuosittain valtakunnansyyttäjänvirastolle, mutta raportoinnissa ei eroteltu luottamuksellisen viestin suojaan puuttuvien tiedonhankintakeinojen käyttöä muusta tiedonhankinnasta. Lisäksi raportointi oli puhtaan numeerista - raporteissa esitettiin tiedonhankintatoimenpiteiden sekä laillisuusvalvonnassa havaittujen puutteiden lukumäärät, mutta ei kerrottu puutteiden eikä mahdollisten korjaavien toimenpiteiden luonteesta. Kun raportit vielä olivat kokonaisuudessaan salassa pidettäviä, ei laillisuusvalvonnan toteutumista ollut alistettu minkäänlaiselle julkiselle tarkastelulle.

- EIT totesi, ettei Venäjän hallitus ollut vastineissaan esittänyt ainoatakaan käytännön esimerkkiä tilanteesta, jossa laillisuusvalvoja olisi antanut valvonnan kohteelle kehotuksen havaitun lainvastaisuuden lopettamiseksi tai korjaamiseksi. Hallitus ei näin ollen ollut myöskään käytännössä kyennyt osoittamaan, että valvontajärjestelyt olivat toimivia ja tehokkaista.

- 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 kohteelle 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 Asso-

ciation 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 nyt Venäjän lainsäädäntöä 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.

Edellä kuvattujen lukuisten puutteiden johdosta EIT katsoi, ettei Venäjän lainsäädäntö vastannut EIS 8 artiklan kansallisille laeille asettamia laatu- ja ennakoitavuusvaatimuksia. Samoin se totesi, ettei Venäjän lainsäädäntö kyennyt rajoittamaan EIS 8 artiklan mukaisiin ihmisoikeuksiin puuttumista tasolle, joka on demokraattisessa yhteiskunnassa välttämätöntä. Vaikka Zakharov-tapaus läheisesti kytkeytyi myös kysymykseen EIS 13 artiklan mukaisten tehokkaiden kansallisten oikeussuojakeinojen olemassaolosta, ei EIT ottanut ratkaisussaan erikseen kantaa kyseisen artiklan loukkaamista koskevaan väitteeseen.

Toistaiseksi tuoreimmassa tietoliikennetiedustelua koskevassa tapauksessa Szabo & Vissy v. Unkari oli kyse Unkarin terrorisminvastaisen turvallisuuspalvelun harjoittamasta sähköiseen viestintään kohdistuvasta tiedustelusta. Kansallinen laki sääti tällaisen tiedustelun oikeuttaviksi perusteiksi yhtäältä terroritekojen estämisen ja toisaalta ulkomailla hädässä olevien Unkarin kansalaisten pelastamisen. Luvan tiedusteluun myönsi oikeusministeri terrorisminvastaisen turvallisuuspalvelun esityksestä. Turvallisuuspalvelun oli lupahakemuksessaan nimettävä henkilö tai henkilöryhmät, joiden sähköiseen viestintään oli tarkoitus puuttua, tai vähintään mainittava kyseisten henkilöiden tai henkilöryhmien tunnistamisen mahdollistavat tiedot. Lisäksi lupahakemuksessa oli tehtävä selkoa tiedonkeruun perusteena olevasta tiedustelutehtävästä sekä sen välttämättömyydestä.

EIT totesi asiassa olevan riidatonta, että puuttumisen perusteena oli kansallisen turvallisuuden suojaaminen, ja katsoi myös, että tiedustelun kohteena olevien uhkien laintasoinen erittely oli riittävän selkeä täyttääkseen 8 artiklan asettaman ennakoitavuusvaatimuksen. Tästä huolimatta EIT katsoi Unkarin lainsäädännön kokonaisarvioinnin perusteella ihmisoikeussopimuksen vastaiseksi. Tuomioistuimen kokonaisarviointiin vaikutti neljä seikkaa. Ensinnäkään laki ei edellyttänyt, että turvallisuuspalvelu lupahakemuksessaan olisi millään tavalla osoittanut, mikä oli lupahakemuksen kohteena olevien henkilöiden tai henkilöryhmien todellinen tai oletettu yhteys siihen uhkaan, josta tiedustelulla oli tarkoitus kerätä tietoa. Lisäksi vaikka turvallisuuspalvelun tuli lupahakemuksessaan perustella tiedustelutehtävän välttämättömyys, ei sen edellytetty esittävän tosiseikkoja hakemuksensa tueksi. Tuomioistuin totesi, että tosiseikkojen esittämistä koskeva vaatimus olisi mahdollistanut tiedustelutoimenpiteen välttämättömyyden arvioinnin perustuen kohdehenkilöitä tai -ryhmiä koskeviin yksilöllisiin epäilyihin. Toiseksi tuomioistuin totesi, että tiedustelutoimenpiteiden ajallista kestoa koskeva kansallisen lain säännös oli liian epämääräinen. Sen perusteella jäi epäselväksi, voitiinko tiedustelua koskeva lupa voimassaolon päättyessä uudistaa vain kerran vai toistuvasti. Kolmanneksi tuomioistuin katsoi, ettei laissa säädetty lupamenettely ollut asianmukainen. Tuomioistuimen mukaan näet menettely, jossa luvan ratkaisijana oli poliittisin perustein virkaansa nimitetty toimeenpanovallan edustaja, ei sisältänyt riittäviä takeita väärinkäytöksiä vastaan. Neljänneksi tuomioistuin totesi, ettei Unkarin lainsäädäntö suonut käytännössä minkäänlaisia oikeussuojakeinoja niiden

henkilöiden käyttöön, joiden oikeuksia mahdollisesti oli rikottu. Koska Unkarin lainsäädäntö ei missään tilanteessa edellyttänyt, että salaisista valvontatoimenpiteestä oli ilmoitettava niiden kohdehenkilöille, ei näillä ollut mitään mahdollisuuksia saattaa toimenpiteiden lainmukaisuutta kyseenalaiseksi.

Kansallinen turvallisuus puuttumisen oikeuttavana intressinä

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 uhkaavan 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). Tuomioistuimen 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. Zakharov-ratkaisun perusteella on toisaalta kuitenkin ilmeistä, että kansallisissa laeissa on jollain tarkkuudella kuvattava tai yksilöitävä ne tapahtumat ja tilanteet, jotka muodostavat uhkan kansalliselle turvallisuudelle ja jotka siten antavat perusteen 8 artiklan mukaisiin oikeuksiin puuttumiselle. Kansalliset lainsäädännöt eivät toisin sanoen jättää kansallisen turvallisuuden käsitettä täysin avoimeksi, sillä tämä ei vastaisi EIS 8 artiklan lainsäädännöille asettamaa ennakoitavuusvaatimusta. Szabo & Vissy -ratkaisun mukaan ennakoitavuusvaatimuksesta ei kuitenkaan seuraa, että uhkatilanteiden laintasoisen määrittelyn tulisi olla täysin täsmällinen tai tyhjentävä.

Puuttumisen välttämättömyys demokraattisessa yhteiskunnassa

Kolmas ja viimeinen ehto sille, että viranomaiset saavat puuttua EIS 8 artiklan takaamien oikeuksien käyttöön on se, että puuttuminen on välttämätöntä demokraattisessa yhteiskunnassa. Artiklan suomenkielisessä versiossa käytettyä sanaa "välttämätön" on pidettävä jossain määrin erottelukyvyttömänä, sillä EIT on lausunut sen englanninkielisen vastineen merkityssisällöstä seuraavaa: "the adjective "necessary" is not synonymous with "indispensable", neither has it the flexibility of such expressions as "admissible", "ordinary", "useful", "reasonable" or "desirable" (Handyside v. Yhdistynyt Kuningaskunta). Lienee siis katsottava, että artiklan tarkoittama välttämättömyys sijoittuu jonnekin korvaamattomuuden ja tarpeellisuuden välimaastoon. Jäljempänä kuitenkin ilmenee, että EIT on tuoreimmissa ratkaisuissaan tiukentanut välttämättömyysedellytyksen tulkintaa nimenomaan tietoliikennetiedustelun kontekstissa.

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.

Tietoliikennetiedustelua Weber & Saravia -ratkaisun tavoin koskevissa tuoreissa Zakharov- ja Szabo & Vissy -ratkaisuissaan EIT kuitenkin täsmensi välttämättömyyskriteeriä tavalla, joka näyttäisi eräiltä osin kaventavan yllä mainittua valtion harkintavaltaa. Silloin kun kyse on tietoliikennetiedustelun kaltaisen kehityksen kärkeä edustavan valvontateknologian käytöstä, on "välttämätön demokraattisessa yhteiskunnassa" -edellytystä tuomioistuimen mukaan tulkittava siten, että se edellyttää "ehdotonta välttämättömyyttä" (strict necessity) kahdessakin suhteessa. Ensinnäkin salaisen tarkkailutoimenpiteen tulee olla yleisellä tasolla ehdottoman välttämätön demokraattisten instituutioiden suojaamiseksi. Toiseksi toimenpiteen tulee olla yksittäisen tiedusteluoperaation yhteydessä ehdottoman välttämätön olennaisen tärkeän tiedon (vital information) saamiseksi.

EIT on perinteisesti korostanut, että kansallisen turvallisuuden nimissä käytettävät viranomaisten salaiset tarkkailu- ja valvontavaltuudet saattavat muodostaa vaaran demokraattiselle yhteiskuntajärjestykselle (mm. Antunes Rocha v. Portugali). Tästä syystä valtion tulee järjestää niiden käytön riippumaton valvonta ja tehokkaat oikeussuojakeinot. Riippumatonta valvontaa voi suorittaa yhtä hyvin kansanedustajista muodostettu elin (ainakin, jos siinä ovat edustettuina niin hallituspuolueet kuin oppositio) kuin parlamentin taikka pääministerin tehtäväänsä nimittämä elin, jonka jäsenillä on tuomarinvirkaan vaadittava pätevyys (Klass v. Saksa, Weber & Saravia v. Saksa, Leander v. Ruotsi, L. v. Norja, Kennedy v. Yhdistynyt Kuningaskunta). Viimeaikaisissa ratkaisuissa on korostettu erityisesti ammattimaisesti suoritetun oikeudellisen valvonnan merkitystä (Szabo & Vissy v. Unkari). Sen sijaan toimeenpanovaltaan liian läheiset suhteet omaava taho ei täytä valvojalle asetettua riippumattomuusvaatimusta. Näin ollen riippumattomuusvaatimuksen vastaisena voidaan yleensä pitää järjestelmää, jossa valvonnan suorittaminen kuuluu esimerkiksi ministerille - varsinkin, jos hän on osallisena tiedonhankintakeinojen käytöstä päättämisessä (Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria).

Valvontaa 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). Samoin laillisuusvalvonnan tulosten tulee olla siinä määrin julkisia, että kansalaiset voivat varmistua laillisuusvalvontajärjestelmän toimivuudesta ja laillisuusvalvonnan tehokkuudesta (Zakharov v. Venäjä). Demokratian suojelemisen kannalta mer-

kitystä on myös sillä, että kansanedustuslaitos osaltaan osallistuu salaisten tarkkailuvaltuuksien valvontaan (Campbell v. Yhdistynyt Kuningaskunta, Leander v. Ruotsi).

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).

Oikeus tehokkaaseen oikeussuojakeinoon

EIS 13 artiklan mukaan jokaisella, jonka Euroopan ihmisoikeussopimuksen 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.

EIS 13 artikla eroaa luonteeltaan edellä kuvatusta 8 artiklasta. 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 loukkausten varalta. Sopimusmääräystä voidaan pitää yhtenä ilmauksena siitä, että myös kansainvälisellä sopimuksella suojatut ihmisoikeudet tulisi prosessuaalisellakin tasolla ensisijaisesti turvata kansallisen oikeusjärjestyksen puitteissa.

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.

EIT on korostanut, että 13 artiklan tulkinnassa on jätettävä tiettyä tapauskohtaista joustovaraa ja vältettävä liiallista muodollisuutta. Kunkin yksittäisen tapauksen olosuhteilla on merkitystä tuomioistuimen 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.

Puhelinkuuntelua koskeneessa ratkaisussa Klass ja muut v. Saksa tuomioistuin 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.

Ratkaisussa Leander v. Ruotsi 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. Tuomioistuin 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 tuomioistuin korosti myös Ruotsin asianomaiseen järjestelmään liittyvää parlamentaarista valvontaa. Sitä vastoin 13 artiklan loukkaus vahvistettiin tapauksessa Segerstedt-Wiberg ja muut v. Ruotsi. 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.

Tapaus Al-Nashif v. Bulgaria, 20.6.2002 koski ulkomaalaisen karkottamista valtion turvallisuuteen liittyvistä syistä. Valittaja vetosi syihin, joiden johdosta 13 artikla tuli sovellettavaksi 8 artiklan perhe-elämän 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 ratkaisussa C.G. ja muut v. Bulgaria, 24.4.2008. 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 paikkaansa pitävyyttä 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. Ratkaisussa Vereinigung Demokratischer Soldaten Österreichs ja Gubi v. Itävalta, 19.12.1994 oli kysymys 10 artiklaan liittyvästä kiellosta levittää sanomalehteä kasarmialueella. 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. Ratkaisussa Stefanov v. Bulgaria, 22.5.2008 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.

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. Kun eräiden maiden kohdalla on toistuvasti tullut ilmi merkittäviä viivästyksiä kansallisten tuomioistuinten antamien tuomioiden ja päätösten täytäntöön panemisessa, on ihmisoikeustuomioistuin oikeuskäytännössään korostanut, että kansallisessa oikeusjärjestelmässä tulee olla riittävät oikeussuojatakeet myös tämäntyyppisiä viivytyksiä vastaan.

2.5 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 noudattaen. 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 EIT ratkaisukäytännöllä on näin ollen katsottava olevan relevanssia myös perusoikeuskirjan 7 artiklan tulkinnalle.

Euroopan unionin tuomioistuimen ratkaisukäytäntö

EU-oikeuden liityntä ja soveltuminen

EU:n perusoikeuskirjan (EUVL C 326, 26.10.2012) määräykset koskevat sen 51 artiklan 1 kohdan mukaan unionin toimielimiä, elimiä ja laitoksia toissijaisuusperiaatteen mukaisesti sekä jäsenvaltioita ainoastaan silloin, kun viimeksi mainitut soveltavat unionin oikeutta. EU:n perusoikeuskirjaa ei siten sovelleta tilanteissa, joissa on kysymys ainoastaan kansallisen lain soveltamisesta ja joita EU-oikeudessa ei säännellä. Kuitenkin EU-oikeuden soveltamisalan ulkopuolellakin perusoikeuskirjasta voidaan johtaa tulkinta-apua esimerkiksi tilanteissa, joissa EIT ei ole käsitellyt jotakin oikeutta tai siihen liittyvää kysymystä, josta on olemassa EU-tuomioistuimen oikeuskäytäntöä.

EU-oikeuden soveltuminen tiettyyn asiaan edellyttää, että asialla on ”riittävä liityntä” EU-oikeuteen (Määräys Burzio, C-497/14, 28–31 kohta; määräys Văraru, C-496/14, 21 kohta; määräys Petrus, C‑451/14, 18-20 kohta.). EU:lla olevan toimivallan olemassaolo ei yksinään riitä tuomaan asiaa EU-oikeuden soveltamisalan piiriin, vaan merkityksellistä on, onko unioni käyttänyt toimivaltaa antamalla sääntelyä asiasta. EU:n perusoikeudet tai yleiset oikeusperiaatteet sellaisinaan, ilman konkreettista liityntää EU-oikeuteen, eivät muodosta kyseisenkaltaista riittävää liityntää, eivätkä siten tuo asiaa EU-oikeuden soveltamisalan piiriin (Määräys Pondiche, C-608/14,21 kohta; tuomio Torralbo Marcos, C-265/13, 30 kohta; tuomio Pelckmans Turnhout, C-483/12, 20 kohta; määräys Balázs ja Papp, C-45/14, 23 kohta; tuomio Åkerberg Fransson, C-617/10, 22 kohta; määräys Nagy ym., C-488/12–C-491/12 ja C-526/12, 17 kohta; määräys Cholakova, C-14/13, 30 kohta).

Arvioitaessa EU-oikeuden soveltamista tiedustelulainsäädännön yhteydessä merkityksellisiä ovat EU-lainsäädäntöön sisältyvät poikkeukset, joiden perusteella EU-oikeuden soveltuminen on useissa säädöksissä rajattu kansallista turvallisuutta koskevien asioiden ulkopuolelle. Poikkeukset perustuvat Euroopan unionista tehdyn sopimuksen 3artiklan 2 kohdan määräykseen, jonka mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla. Unionilla ei siten ole kansallista turvallisuutta ainakaan suoraan koskevaa toimivaltaa. Mainitussa artiklassa ei kuitenkaan määritetä sitä, missä EU:n ja kansallisen toimivallan välinen rajanveto tarkkaan ottaen kulkee. EU-oikeus ulottuu lukuisille aloille, joilla on välitöntä tai välillistä merkitystä kansallisen turvallisuuden ja yleisen järjestyksen alalla. Samalla näiden intressien kansallinen ulottuvuus tunnustetaan mainitsemalla ne useissa EU:n perussopimuksen artikloissa ja EU-säädöksissä EU:n yhteistyöaloja koskevina poikkeus- tai oikeuttamisperusteina, joten EU-oikeuden soveltamisalan rajautuminen pois kansallista turvallisuutta koskevan poikkeuksen perusteella ei kuitenkaan ole aina käytännössä yksiselitteistä. Jäsenvaltion, joka vetoaa edukseen kansallista turvallisuutta koskevaan perusteeseen, on myös näytettävä toteen tarve turvautua kyseiseen perusteeseen (tuomio ZZ, C-300/11; tuomio Insinööritoimisto InsTiimi Oy, C-615/10, 35 kohta; tuomio komissio v. Suomi, C-284/05, 45 ja 47 kohta).

Luottamuksellisen viestin salaisuuden suoja

Säännös luottamuksellisen viestin salaisuuden suojasta sisältyy EU:n perusoikeuskirjan 7 artiklaan, jonka mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, ko-

tiaan sekä viestejään kunnioitetaan. Lisäksi perusoikeuskirjan 8 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan.

Yksityiselämän kunnioitusta ja henkilötietojen suojaa koskevien perusoikeuksien tärkeyttä on korostettu EU-tuomioistuimen oikeuskäytännössä erityisesti sähköisen viestinnän yhteydessä (mm. tuomio Tele2 Sverige AB and Secretary of State for the Home Department, yhdistetyt asiat C-203/15 ja C-698/15, 93 kohta, Schrems, C-362/14, 39 kohta; tuomio Rijkeboer, C-553/07, 47 kohta; tuomio Digital Rights Ireland ym., 53 kohta ja tuomio Google Spain ja Google, C-131/12, 53, 66 ja 74 kohta oikeuskäytäntöviittauksineen.)

Perusoikeuskirjaa koskevat selitykset on Euroopan unionista tehdyn sopimuksen 6 artiklan 1 kohdan kolmannen alakohdan ja perusoikeuskirjan 52 artiklan 7 kohdan mukaan otettava huomioon perusoikeuskirjan tulkinnassa. Perusoikeuskirjaa koskevien selitysten (EUVL C 303, 14.12.2007, s. 17–35) mukaan perusoikeuskirjan 7 artiklassa turvatut oikeudet vastaavat ja niillä on sama merkitys ja kattavuus kuin vastaavilla EIS 8 artiklassa turvatuilla oikeuksilla. EIS:ssa käytetty sana ”kirjeenvaihtonsa” on tekniikan kehityksen huomioon ottamiseksi korvattu perusoikeuskirjan 7 artiklassa sanalla ”viestiensä”.

Perusoikeuskirjan 52 artiklan 3 kohdassa määrätään, että siltä osin kuin perusoikeuskirjan oikeudet vastaavat EIS:ssa turvattuja oikeuksia, niillä on sama merkitys ja kattavuus kuin sopimuksessa turvatuilla oikeuksilla. Tämä määräys ei estä unionia myöntämästä tätä laajempaa suojaa.

Perusoikeuskirjan 52 artiklan 3 kohdan määräys EIS:een nähden laajemmasta suojasta merkitsee sitä, ettei perusoikeuskirjassa myönnetty suojan taso saa koskaan olla vastaavaa ihmisoikeussopimuksessa taattua suojan tasoa matalampi, mutta voi ylittää sen. EU:n oikeusjärjestyksessä tunnustettujen perusoikeuksien sisällön ja suojan tason tulkinnassa tulee ensisijaisesti tukeutua kyseistä oikeutta koskevaan EU-tuomioistuimen oikeuskäytäntöön (Lausunto EU:n liittyminen EIS:een, 2/13, EU:C:2014:2454, 170 kohta; tuomio Kadi ja Al Barakaat, C-402/05 ja C-415/04 P, 281–285 kohta; tuomio Internationale Handelsgesellschaft, C-11/70, 4 kohta).

EU:n perusoikeuskirjassa tunnustetut oikeudet ja vapaudet eivät pääsääntöisesti ole ehdottomia, vaan niiden käyttämistä voidaan rajoittaa. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

EU-tuomioistuimen oikeuskäytännön mukaan lailla säätämistä koskevan vaatimuksen mukaisesti rajoituksen oikeudellisen perustan on muun muassa oltava riittävän selkeä ja täsmällinen, ja perustassa itsessään on annettava tietty suoja mahdollisia oikeudenloukkauksia vastaan (Tuomio WebMind, C-419/14, 81 kohta). Kyseinen kriteeri muistuttaa läheisesti EIS:n vastaavaa oikeuksien rajoitusedellytyksiä koskevaa ”säädetty laissa” -perustetta, minkä vuoksi EIT oikeuskäytännöstä voidaan saada tätä kriteeriä koskevaa tulkinta-apua erityisesti sellaisten perusoikeuskirjan määräysten osalta, jotka vastaavat EIS:n sisältämiä oikeuksia.

Unionin tuomioistuimen oikeuskäytännöstä käy ilmi, että muun muassa ”vakavan rikollisuuden torjunta yleisen turvallisuuden takaamiseksi” (Tuomio Tsakouridis, C-145/09, 46 ja 47 kohta) ja ”kansainvälisen terrorismin torjuminen kansainvälisen rauhan ja turvallisuuden ylläpitämiseksi” (Tuomio WebMind, C-419/14, 76 kohta; tuomio Kadi ja Al Barakaat, C-402/05 P ja C-415/05 P, 363 kohta ja tuomio Al-Aqsa v. neuvosto, C-539/10 P ja C-550/10 P, 130

kohta) ovat unionin yleisen edun mukaisia tavoitteita. Lisäksi ”kansallinen turvallisuus” mainitaan nimenomaisesti Euroopan unionin toiminnasta tehdyn sopimuksen 4 artiklan 2 kohdassa ja se on vakiintuneesti hyväksytty unionin tuomioistuimen oikeuskäytännössä oikeutetuksi tavoitteeksi rajoittaa perusoikeuksia (Esim. tuomio komissio v. Suomi, C-284/05, 45, 47 ja 49 kohta).

EU-tuomioistuimen käytännössä perusoikeuksien rajoitusten suhteellisuusperiaatteen mukaisuuden arviointi on usein osoittautunut arvioinnin ratkaisevaksi vaiheeksi. Perusoikeuskirjan 52 artiklan 1 kohdan mukainen suhteellisuusperiaate kuuluu EU-oikeuden yleisiin periaatteisiin ja edellyttää EU-tuomioistuimen vakiintuneen oikeuskäytännön mukaan, että arvioitavana olevan toimen tai säädöksen oikeutetut tavoitteet ovat toteutettavissa unionin toimesta säädettyjen keinojen avulla ja että niillä ei ylitetä sitä, mikä on tarpeellista ja välttämätöntä näiden tavoitteiden toteuttamiseksi ja on tähän soveltuvaa (appropriate and necessary, esim. tuomio Schaible, C-101/12, 29 kohta; tuomio Sky Österreich, C-283/11, 50 kohta; tuomio Nelson ym., C-581/10 ja C-629/10, 71 kohta; tuomio Volker und Markus Schecke, C-92/09 ja C-93/09, 74 kohta ja tuomio Afton Chemical, C-343/09, 45 kohta).

Käytännössä kyse on hyväksyttävän tasapainon löytämisestä eri intressien välille. Perusoikeutta koskevien poikkeuksien ja rajoitusten tulee olla välttämättömiä niin, että toimenpiteillä puututaan kyseiseen perusoikeuteen mahdollisimman vähän samalla, kun myötävaikutetaan tehokkaasti kyseessä olevan EU:n sääntelyn tavoitteiden toteutumiseen (Tuomio WebMind, 82 kohta; tuomio Schecke, 87 ja 88 kohta; tuomio R., C-285/09, 45 kohta).

Tehdessään suhteellisuusperiaatteen mukaista arviointia tietosuojaa koskevissa asioissa EU-tuomioistuin on kiinnittänyt huomiota muun muassa arvioinnin kohteena olevan järjestelyn valvontaan (Tele2 Sverige AB and Secretary of State for the Home Department, 123 kohta ja Schrems, 40 kohta), käytettävissä oleviin riittäviin oikeussuojakeinoihin (mm. Schrems, 95 kohta ja UGT-Rioja ym., C-428/06–C-434/06, 80 kohta), tiedon antamiseen ja tietoturvaan sekä henkilöpiiriä, ennakkolupaa (Tuomio WebMind, 77 ja 78 kohta), tietoihin pääsyä, tietojen säilytysaikaa ja niiden hävittämistä koskeviin edellytyksiin (Tele2 Sverige AB and Secretary of State for the Home Department, 122 kohta ja Tuomio Digital Rights Ireland, 56-67 kohta).

Eduskunnan perustuslakivaliokunta esitti lausunnossaan PeVL 18/2014 vp EUT:n Digital Rights Ireland ym. eli niin sanottua data retention -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 EIT:n 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).

EU-tuomioistuin on käsitellyt vaatimusta perusoikeuden keskeisen sisällön kunnioittamisesta ratkaisussa Schrems. Tuomioistuimen mukaan säännöstön, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön, on erityisesti katsottava loukkaavan yksityiselämän kunnioitusta koskevan perusoikeuden keskeistä sisältöä (94 kohta). Lisäksi tuomioistuin totesi, että säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi, ei ollut tehokasta oikeussuojaa koskevan perusoikeuden keskeisen sisällön mukainen (95 kohta).

2.6 Nykytilan arviointi

Yleistä

Kansallisesta turvallisuudesta vastaavien viranomaisten tehtävänä on ennakoida ja hankkia tietoja sellaisesta toiminnasta, joka voi vaarantaa tai uhata erityisen tärkeiksi miellettyjä kansallisia etuja. Kansallisesta turvallisuudesta vastaavat viranomaiset harjoittavat lakisääteisten tehtäviensä hoitamisen edellyttämää tiedustelua. Tiedustelua varten ei kuitenkaan ole laissa säädettyjä toimivaltuuksia.

Yhteisenä piirteenä kansallisesta turvallisuudesta vastaavien viranomaisten tehtäville on, että ne koskevat uhkien torjuntaa. Uhkien torjuminen edellyttää, että ne kyetään havaitsemaan ja niistä saadaan tietoa riittävän varhain. Suojelupoliisin tehtävänä on rikosten estämisen, paljastamisen ja vähäisemmässä määrin selvittämisen ohella torjua sellaisia hankkeita, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Hankkeen käsitettä ei täsmennetä poliisin hallinnosta annetussa laissa tai sen esitöissä. Hankkeissa ei voida katsoa olevan kyse rikoksista, mistä johtuen viraston tehtävässä tältä osin on kyse tiedustelullisesta eikä rikostorjunnallisesta toimeksiannosta.

Kansalliseen turvallisuuteen kohdistuvia uhkia torjuvien viranomaisten tiedustelutoimivallasta ja tämän toimivallan jakautumisesta siviili- ja sotilasviranomaisten välillä ei myöskään ole säännöksiä. Nykysääntelyssä viranomaisten tiedonhankintatoimivaltuudet perustuvat tiedustelun sijaan yksinomaan rikostorjuntaan. Muuttuneeseen turvallisuusympäristöön liittyvät epävarmuustekijät korostavat tarvetta tuottaa objektiivista, 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.

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. Keskeistä olisi hankkia tietoa vallitsevasta tilanteesta ja analysoida sen merkitystä Suomen kansallisen turvallisuuden kannalta.

Kaikissa kansainvälisessä vertailussa olevissa valtioissa säädetään tiedustelusta samoin kuin suurimmassa osassa vertailun ulkopuolisissakin suvereeneissa länsidemokraattisissa valtioissa. Tiedustelua koskevaan lainsäädäntöön voi sisältyä säännöksiä tietoverkkoympäristön kautta tapahtuvasta tiedonhankinnasta. Sääntelytarkkuus vaihtelee maittain. Tästä syystä kaikkien vertailussa olleiden valtioiden lainsäädännöistä ei voida suoraan tehdä johtopäätöksiä käytössä olevista yksittäisistä tiedonhankintamenetelmistä. Myös siinä on eroja, miten tarkasti ne uhat, joiden torjumista varten tiedonhankintaa saa toteuttaa, on yksilöity lain tasolla.

Vertailussa olleiden valtioiden tiedustelutoiminnasta vastaa joko yksi tiedusteluviranomainen tai vaihtoehtoisesti toimivalta on jaettu siviili- ja sotilastiedustelupalveluiden kesken. Tiedustelutoimivaltuuksien jakaminen siviili- ja sotilasviranomaisten välillä perustuu pääsääntöisesti siihen, onko kyse siviili- vai sotilaallisluontoisesta uhasta. Tiedustelupalvelut toimivat yleensä joko puolustusministeriön, sisäministeriön tai molempien johdossa ja ohjauksessa. Tiedonhankintaa koskevat toimeksiannot voivat tulla valtiojohdolta, ohjaavilta ministeriöiltä tai esimerkiksi puolustusvoimien johdolta.

Suojelupoliisin tehtävät

Suojelupoliisi on sisäministeriön alainen valtakunnallinen poliisiyksikkö, jonka tehtävänä poliisin hallinnosta annetun lain 10 §:n 1 momentin mukaan 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. Suojelupoliisin tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi.

Poliisin hallintolain 10 §:ää 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. Pykälän kirjoittamistavassa on pyritty ottamaan huomioon ennalta estävän toiminnan korostunut merkitys suojelupoliisin tehtäväalueella.

Tässä esityksessä operatiivisessa toiminnassa käytettäviä toimivaltuuksia ehdotetaan muutettavaksi sekä ehdotetaan säädettäväksi tiedonhankinnasta ulkomailla, minkä seurauksena suojelupoliisin toiminnassa korostuu siten entisestään tiedonhankinnallinen ja tiedustelullinen toimintatapa. Suojelupoliisin tehtävää olisi tarpeen tarkistaa ja täsmentää siten, että suojelupoliisin tiedustelullinen ja tiedonhankinnallinen tehtävä ilmenisi siitä nykyistä selvemmin ottaen huomioon ehdotettavaksi säädettävät toimivaltuudet sekä se, että suojelupoliisi ryhtyisi aktiivisesti hankkimaan itse tietoa ulkomailla. Tiedustelullista luonnetta voitaisiin kuvata painottamalla suojelupoliisin tehtävässä sen tiedonhankinnallista luonnetta kansallisen turvallisuuden suojaamiseksi sekä sellaisten toimintojen, hankkeiden tai rikosten havaitsemisella, jotka voivat uhata yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Kansallisen turvallisuuden suojaaminen olisi tarpeen mainita myös poliisin tehtäviä koskevassa poliisilain 1 luvun 1 §:n 1 momentin säännöksessä, koska kansallisen turvallisuuden suojaamisessa olisi myös poliisille laajemmin kuuluva tehtävä, vaikka suojelupoliisi olisi ainoa poliisiyksikkö, joka voisi käyttää tiedustelumenetelmiä tiedon hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Kansallinen turvallisuus mainitaan nimenomaisesti Euroopan unionin toiminnasta tehdyn sopimuksen 4 artiklan 2 kohdassa ja se on vakiintuneesti hyväksytty unionin tuomioistuimen oi-

keuskäytännössä oikeutetuksi tavoitteeksi rajoittaa perusoikeuksia. Se on yksi niistä perusteista, joka EIS 8 artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. Tätä käsitellään tarkemmin esityksen osioissa 2.4 ja 2.5.

Ylimpien laillisuusvalvojien ratkaisukäytännössä (esim. eduskunnan apulaisoikeusasiamiehen päätökset 18.12.2003 dnro 1634/4/01 ja 18.12.2003, dnro 1634/4/01) todetaan, että tehtävämäärittelyä koskevat säännökset eivät kuitenkaan ole toimivaltasäännöksiä. Tehtäväsäännös ei siis perusta poliisille toimivaltaa ryhtyä minkä tyyppisiin toimiin tahansa noiden tehtävien suorittamiseksi eikä poliisi siis voi pelkästään sen perusteella puuttua ihmisten lailla suojattuihin oikeuksiin. Silloin kun poliisi puuttuu henkilön oikeuspiiriin, tulee toimivallan aina perustua nimenomaiseen säännökseen. Näin ollen kansallisen turvallisuuden suojaaminen ei itsessään osoittaisi kuin sen, että suojelupoliisilla olisi lainmukainen ja yhteiskunnallisesti toivottu motiivi menettelylleen. Tämä ei siis vielä sellaisenaan oikeuttaisi puuttumaan ihmisten perusoikeuksiin, vaan sille tulee löytyä toimivaltaperuste laista.

Toisaalta on otettava huomioon perustuslain 22 §, jonka mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Mainittu pykälä asettaa myös poliisille velvollisuuden käyttää tehtäväpiiriinsä kuuluvia toimivaltuuksia. Tätä näkökulmaa korostetaan myös EIT:n ratkaisukäytännössä. Esimerkiksi ratkaisussa Kontrova v. Slovakia 31.5.2007 on kysymys viranomaisten positiivisesta velvollisuudesta ryhtyä ehkäiseviin käytännöllisiin toimenpiteisiin suojellakseen yksilöä, jonka henki on vaarassa toisen yksilön rikollisen toiminnan vuoksi. Valtuuksien puitteissa on ryhdyttävä toimenpiteisiin, jotka järkevästi ajatellen ovat omiaan torjumaan sellaista vaaraa. Poliisin velvollisuuteen turvata perusoikeuksia ja ihmisoikeuksia sekä turvaamisen tapaan on puututtu myös esimerkiksi ratkaisuissa Surugiu v. Romania 20.4.2004, Ouranio Toxo ym. v. Kreikka 20.10.2005 ja Babylonova v. Slovakia 20.6.2006 (HE 224/2010 vp, s. 71–72).

Suojelupoliisin toimivaltuudet

Salaiset tiedonhankintakeinot

Suojelupoliisi käyttää tehtävässään poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja: telekuuntelua, tietojen hankkimista telekuuntelun sijasta, televalvontaa, tukiasematietojen hankkimista, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknisen tarkkailua (tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimista, peitetoimintaa, valeostoa, tietolähdetoimintaa ja valvottua läpilaskua rikoksen estämiseen, paljastamiseen tai vaaran torjumiseen.

Poliisilain 5 luvun salaisten tiedonhankintakeinojen voidaan olettaa olevan hyödyllisiä ja tehokkaita myös tiedustelutoiminnassa ja ne muodostavat hyvän pohjan, jolle tiedustelutoimivaltuudet voidaan rakentaa. Poliisilain 5 luvun sääntelyssä on otettu huomioon myös perus- ja ihmisoikeusnäkökohdat mukaan lukien tuomioistuimen osallistuminen tarvittaessa ratkaisutoimintaan.

Salaisille tiedonhankintakeinoille on ominaista se, että niitä käytetään kohdehenkilöltä salassa. Salaista tiedonhankintaa koskeva poliisilain 5 a luku on perusteltua rakentaa 5 luvun salaisia tiedonhankintakeinoja koskevan luvun säännöksille. Tämä liittyy edellä kerrotun lisäksi siihen, että säänneltävät menetelmät ovat samoja, jolloin johdonmukaisuus- ja tarkoituksenmukaisuusnäkökohdat puhuvat sen puolesta, että tiedustelumenetelmiä koskevien määritelmien ja menettelytapojen, kuten päätöksentekoa koskevan sääntelyn tulisi olla mahdollisimman pitkälle samoja. Tämä tarkoittaisi, että poliisilain 5 a luvun puolella tulisi poiketa 5 luvun sääntelystä vain, kun siihen on tiedustelutoiminnan erityispiirteiden johdosta perusteltu syy.

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 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 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).

Salaisilla tiedonhankintakeinoilla ei voida riittävän tehokkaasti ja varhaisessa vaiheessa havaita uhkia eikä ryhtyä niiden edellyttämiin toimenpiteisiin, koska salaisten tiedonhankintakeinojen käyttö on lainsäädännössä sidottu rikoksen käsitteeseen (estäminen tai paljastaminen). Suomeen ja sen väestöön mahdollisesti kohdistuvien uhkien tunnistamiseksi ja niiden torjumiseksi olisi tarpeen voida suojelupoliisin omin toimivaltuuksin hankkia tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta sekä suojata kansallista turvallisuutta ja ylläpitää sitä. 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 valtiojärjestystä tai yhteiskunnan perustoimintoja vakavasti uhkaavan toimintaan, kuten terrorismiin liittyvään toimintaan tai väkivaltaiseen radikalisoitumiseen taikka ulkomaisten tiedustelupalvelujen toimintaan.

Kansallinen turvallisuus on yksi niistä perusteista, joka EIS 8 artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. Valtioilla on varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuuttaan. EIT:n ratkaisukäytännön perusteella ainakin sotilaallinen maanpuolustus, terrorismintorjunta 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. Muunlainen ratkaisu olisi absurdi, koska ainoastaan ulkomaan tiedustelusta säätäminen johtaisi tilanteeseen, jossa suomalaisen tiedusteluviranomaisen tulisi lopettaa tiedustelutoimivaltuuksien käyttäminen Suomen rajan ulkopuolelle ja antaa seurattavan kohteen saapua Suomen rajojen sisälle, missä kohdetta ei kyettäisi seuraamaan puuttuvien toimivaltuuksien takia. Mainitun perusteella, kun jäljempänä käytetään henkilötiedustelun ja tietojärjestelmätiedustelun käsitteitä, niillä tarkoitetaan sekä kotimaan että ulkomaan tiedustelua.

Henkilötiedustelulla tarkoitetaan tiedustelua, joka perustuu henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin. Näin laajaa toimivaltuutta olisi toimivaltuussääntelyn täsmällisyys ja tarkkarajaisuus huomioon ottaen hankala säännellä. Siksi henkilötiedustelun keinot tulisi säännellä nykyinen toimivaltuussäännöskehikko huomioon ottaen. Henkilötiedustelun alaan kuuluisivat ainakin telekuuntelu, tietojen hankkimisen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, osin 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. Tätä vastaisi teknisenä tarkkailuna tehtävä tekninen laitetarkkailu ja osin tekninen kuuntelu.

Tiedustelutoimivaltuuksista voitaisiin säätää poliisilain uudessa 5 a luvussa. Toimivaltuuksia voitaisiin kutsua tiedustelumenetelmiksi, jotka keinollisesti ja määritelmällisesti olisivat samoja tiedonhankintakeinoja kuin poliisilain 5 luvussa. Tiedustelumenetelmien käytön edellytykset eroaisivat salaisten tiedonhankintakeinojen vastaavista. Näin ei aiheutuisi sekaannusta salaisten tiedonhankinta keinojen tai salaisten pakkokeinojen käsitteiden kanssa.

Salaisten tiedonhankintakeinojen käyttöedellytykset

Yleiset ja erityiset edellytykset

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. Sen lisäksi, mitä salaisten tiedonhankintakeinojen käytön erityisistä edellytyksistä jäljempänä säädetään, 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 edelly-

tyksiä. 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.

Rikoksen paljastamiseen yllä mainittuja salaisia tiedonhankintakeinoja voidaan käyttää vain, jos kysymyksessä on laissa tarkemmin säädetty maanpetos- tai terrorismirikos. Rikosten paljastamisen yhteydessä ei sovelleta salaisten tiedonhankintakeinojen keinokohtaisissa säännöksissä säädettyjä erityisiä edellytyksiä (HE 224/2010 vp, s. 92).

Poliisilain 5 a lukuun tulisi ottaa vastaavanlainen sääntely, jossa tiedustelumenetelmien käyttö porrastettaisiin sen mukaan, kuinka tuntuvasti niillä puututaan kohteena olevan henkilön perus- ja ihmisoikeuksiin. Tällöin voitaisiin edelleen käyttää jo nykyiseen 5 lukuun otettuja tuloksellisuusodotusta sekä ilmaisuja ”erittäin tärkeä merkitys” ja ”välttämätön”. Tiedustelumenetelmän käytön tarkoituksena ei olisi estää, paljastaa tai selvittää rikoksia, vaan hankkia tietoa kansallista turvallisuutta vakavasti uhkaavasta tai sitä vakavasti uhkaavasta toiminnasta. Kyseinen toiminta tulisi määritellä niin seikkaperäisesti kuin se ylipäänsä on mahdollista. Toimenpidekohtaisesti tulisi edelleen säätää muista keinojen käyttämisen edellytyksistä niin täsmällisesti ja tarkkarajaisesti kuin mahdollista, esimerkiksi siitä, kehen toimivaltuuden käyttö voidaan kohdistaa tai luvan tai päätöksen voimassaoloajasta.

Poliisilain 5 a luvussa säänneltävien tiedustelumenetelmien käyttämisen tavoitteena on saada tietoa toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Poliisilaissa tulisi määritellä, mitä kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan. Koska kansallista turvallisuutta vaarantava toiminta ei ole rikoksen estämistä, paljastamista tai selvittämistä, ja toiminta voi olla sellaista, ettei se ikinä konkretisoituessaan tulisi olemaan rikos, tiedusteluviranomaisella tulee olla mahdollisuus ryhtyä alhaisella kynnyksellä hankkimaan tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tällöin voidaan tiedustelumenetelmän käytön edellytykseksi perustellusti asettaa se, että tiedonhankinta kohdistuu yhteiskunnan näkökulmasta kaikkein merkittävimpiin uhkiin. Kansalliseen turvallisuuteen kohdistuvia uhkia (siviilitiedustelu kohteet) käsitellään tarkemmin poliisilakiehdotuksen 5 a luvun 3 §: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

Suojelupoliisilla on poliisilain 5 luvun 3 §:n mukaan oikeus käyttää salaisia tiedonhankintakeinoja rikoksen estämisen lisäksi seuraavien rikosten paljastamisessa: 1) Suomen itsemääräämisoikeuden vaarantaminen; 2) sotaan yllyttäminen; 3) maanpetos, törkeä maanpetos; 4) vakoilu, törkeä vakoilu; 5) turvallisuussalaisuuden paljastaminen; 6) luvaton tiedustelutoiminta; 7) rikoslain 34 a luvun 1 §:n 1 momentin 2–7 kohdassa tai mainitun pykälän 2 momentissa tarkoitettu terroristisessa tarkoituksessa tehtävä rikos; 8) terroristisessa tarkoituksessa tehtävän rikoksen valmistelu; 9) terroristiryhmän johtaminen; 10) terroristiryhmän toiminnan edistäminen; 11) koulutuksen antaminen terrorismirikoksen tekemistä varten; 12) kouluttautuminen

terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta; 13) värväys terrorismirikoksen tekemiseen; 14) terrorismin rahoittaminen; 15) terroristiryhmän rahoittaminen, jos teon vakavuus edellyttäisi vankeusrangaistusta; 16) matkustaminen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta. Kysymys on suojelupoliisin tehtäviin kuuluvien rikosten paljastamisesta (HE 224/2010 vp, s. 92).

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

Tiedonhankinnan kohteena oleva henkilö tulee pystyä yksilöimään vähintään henkilön roolin tai tehtävän kautta, vaikka hän olisikin poliisille vielä henkilöllisyydeltään tuntematon. Telekuuntelu tai televalvonta voidaan kohdistaa myös tuntemattomaan henkilöön esimerkiksi IP-osoitteen tai IMEI-koodin perusteella. 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 yhteisöiltä.

Tiedustelutoiminnalle tyypillistä on, ettei tietty henkilö ole aina tiedossa, vaan tiedustelun olennaisena tavoitteena olisi löytää sellaiset henkilöt, joiden toiminta vakavasti uhkaa kansallista turvallisuutta. Siksi tiedustelutoimivaltuuksia 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 uhkalähtöisesti. Salainen tiedonhankinta tulisi mahdollistaa sellaisen toiminnan kohdalla, joka vakavasti uhkaa Suomen kansallista turvallisuutta joko suoraan tai välillisesti. Kansallista turvallisuutta vakavasti uhkaava toiminta voi olla sellaista, joka konkretisoituessaan olisi rikos, 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.

Tiedon hankkimisen tulisi sisältää myös Suomeen kohdistuvien ulkoisten uhkien kartoittamisen. Kyse olisi siten esimerkiksi turvallisuusympäristön kehityksen seuraamisesta kansalliseen turvallisuuteen kohdistuvan tilannekuvan muodostamiseksi. Ilmaisu kattaisi myös jatkuvan tiedonhankinnan kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. 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). Kansallista turvallisuutta vakavasti uhkaavaa toimintaa käsitellään poliisilakiehdotuksen 5 a luvun 3 §: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.

Teletiedonhankintakeinot

Kansallista turvallisuutta vakavasti uhkaavaan toimintaan liittyy lähes poikkeuksetta viestintää. Koska tällainen toiminta on miltei aina luonteeltaan järjestäytynyttä, siihen osallistuvilla henkilöillä on tarve viestiä keskenään. Tämä koskee niin terrorismia, ulkovaltojen Suomeen kohdistamaa tiedustelua, joukkotuhoaseiden levittämistä, yhteiskunnan kriittistä infrastruktuuria uhkaavaa toiminta kuin valtio- ja yhteiskuntajärjestyksen väkivaltaiseen kumoamiseen tai muuttamisen tähtäävää toimintaa. Uhkaavan toiminnan kulloisestakin luonteesta riippuen viestintä voi koskea esimerkiksi toimintaan osallisten henkilöiden välisiä tehtäväksiantoja, tehtävien toteuttamista koskevaa raportointia, toiminnan suunnittelua, uhkan kohteita koskevaa tiedonhankintaa, osallisten motivointia ja radikalisointia tai uusien osallisten rekrytointia toimintaan. Nykyaikana viestintä on yleensä sähköistä ja se tapahtuu tietoverkoissa.

Tiedonhankinta henkilöiden välisistä sähköisistä viestiyhteyksistä on keskeisessä asemassa, kun tarvitaan kansalliseen turvallisuuteen kohdistuvista uhkista sellaista tietoa, joka mahdollistaa riittävän tilannekuvan ja uhkien torjumisen. Merkitystä on tiedonsaannilla niin sähköisen viestinnän sisällöstä kuin viestintään liittyvistä muista tiedoista kuten tunnistamistiedoista. Viestinnän sisällön perusteella voidaan muodostaa kuva kansallista turvallisuutta uhkaavan toiminnan konkreettisemmasta luonteesta ja toiminnan yksityiskohdista. Tunnistamistiedot saattavat olla välttämättömiä toimintaan osallistuvien henkilöiden hallussa olevien teleosoitteiden tai telepäätelaitteiden identifioimiseksi.

Suojelupoliisin käytössä olevia luottamuksellisen viestin salaisuuden suojaan puuttuvia rikoksen estämiseen tai paljastamiseen tarkoitettuja salaisia teletiedonhankintakeinoja 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 telekuuntelu 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 poliisin tuntema. 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 ongelmallista, sillä salaisessa tiedonhankinnassa on kyettävä ammattimaisten ja järjestäytyneesti toimivien uhkahenkilöiden kohdalla 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 (kännyköitä). Tämä aiheuttaa useassa tapauksessa sen, että telekuuntelu- ja televalvonta muodostuvat työläiksi käyttää ja niiden teho heikkenee salaisina tiedonhankintakeinoina. Lisäksi siitä aiheutuu tarpeettomia henkilöstökustannuksia esitutkintaviranomaiselle, 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 vähentämään lupaprosessin toimijoiden työmäärää. Esimerkiksi terroristisolut pyrkivät suojaamaan toimintaansa ja yhteydenpitoansa käyttäen useita eri henkilöllisyyksiä ja harhauttamaan tiedusteluviranomaista muun muassa käyttämällä useita eri puhelinliittymiä ja useita eri puhelimia.

Teletiedonhankintakeinojen tekniset reunaehdot

Teletiedonhankintakeinoja koskeva edellä kuvattu sääntely vaikuttaa siihen, kuinka telekuuntelu ja televalvonta toteutetaan teknisesti. Telekuuntelu ja televalvonta suoritetaan mahdollisimman lähellä 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 poliisilla 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 esimerkiksi 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.

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 salaisten teletiedonhankintakeinojen kohdistamista koskevista edellytyksistä sekä tiedonhankintakeinojen erityisistä edellytyksistä.

Telekuuntelu soveltuu puutteellisesti uhkien havaitsemiseen ja tunnistamiseen yleisessä viestintäverkossa. Sen kannalta ei ole ratkaisevaa merkitystä esimerkiksi sillä, onko telekuuntelun ja -valvonnan käytön perusteena nykyiseen tapaan rikoksen estäminen vai voidaanko kyseisiä tiedonhankintakeinoja käyttää myös tiedustelumenetelminä tietojen hankkimiseksi kansallista turvallisuutta uhkaavasta toiminnasta. Menetelmien tiedusteluperusteisenkin käytön nimenomaisena edellytyksenä olisi uhkan, sen taustalla olevien henkilöiden ja heidän käyttämiensä konkreettisten viestintävälineiden tiedossa olo sillä hetkellä kun telekuuntelun tai -valvonnan käyttöön ryhdytään. Tiedusteluperusteisesta telekuuntelusta ja televalvonnasta säätäminen ei näin ollen merkittävästi lisäisi suomalaisen yhteiskunnan kykyä havaita ja tunnistaa yleisessä viestintäverkossa sen keskeisiin turvallisuusetuihin kohdistuvia tuntemattomia uhkia ja niiden taustalla olevia henkilöitä. Tästä erillinen asia on, että tiedusteluperusteisesta telekuuntelusta ja televalvonnasta säätämisen voidaan arvioida merkittävällä tavalla parantavan tiedonsaantia sellaisesta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, jossa kyse ei ole rikoksesta tai joka ei ole edennyt konkreettisen ja yksilöidyn 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 kansallista turvallisuutta vakavasti uhkaavan toiminnan muotoja, jotka nykyisin eivät ole rangaistavia. Teletiedonhankintakeinojen käytön erityisenä edellytyksenä olevien perusterikosten laajentaminen ei muuttaisi näiden tiedonhankintakeinojen perusluonnetta.

Suojelupoliisin toimialaan kuuluvien vakavien turvallisuusuhkien yhä yleisempi piirre on se, että niihin osalliset henkilöt oleskelevat Suomen rajojen ulkopuolella, 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 tiedustelu- ja turvallisuuspalveluiden kansainvälisen tietojenvaihdon seurauksena on jollain tarkkuudella tiedossa kun taas viestinnän Suomessa oleva osapuoli on tuntematon. Kyse voi olla esimerkiksi tilanteista, joissa ulkomailla toimivan terroristiverkoston tiedetään tai epäillään radikalisoivan tai värväävän Suomessa olevia henkilöitä tai ohjaavan tänne lähetettyjä tai täällä muuten oleskelevia jäseniään, tai joissa on saatu tietoa, jonka mukaan vieraan valtion tiedustelupalvelu on lähettänyt Suomeen peitteellä toimivia tiedusteluupseereita. Jos toimintaan osallistuvat Suomessa oleskelevat henkilöt ja heidän käyttämänsä viestintävälineet eivät 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 kansallisen turvallisuuden uhkaan osallisten Suomessa oleskelevien henkilöiden havaitsemiseen eikä heidän tunnistamiseensa, vaikka henkilöiden havaitseminen ja tunnistaminen olisi edellytys uhkia koskevalle täsmällisemmälle tiedonhankinnalle ja viime sijassa uhkien estämiselle. Tämä on merkittävä puute tilanteessa, jossa Suomen turvallisuusympäristö on lähes kaikilla osalohkoillaan ratkaisevasti heikentynyt ja oletettavasti jatkaa heikkenemistään.

Suomen turvallisuusympäristö on kehittynyt ja kehittyy ilmeisesti jatkossakin suuntaan, jossa kansalliseen turvallisuuteen kohdistuvien vakavien uhkien ajoissa havaitseminen ja tunnistaminen muuttuvat entistä vaikeammaksi. Taustalla olevaa uhkaympäristön monimuotoistumista on käsitelty muun valtioneuvoston sisäisen turvallisuuden selonteossa (VNS 5/2016vp) ja ulko- ja turvallisuuspoliittisessa selonteossa (VNS 7/2016vp). Uhkien havaitseminen ja tunnistaminen ajoissa sekä uhkaympäristön muutosten ennakoiminen ovat samalla muuttuneet myös entistä tärkeämmäksi, sillä teknologian kehittyminen on mahdollistanut kansallista turvallisuutta vaarantavien tekojen toteuttamisen entistä lyhyemmällä valmisteluajalla ja vakavammin seurauksin.

Kansalliseen turvallisuuteen kohdistuvien uhkien havaitsemisen ja tunnistamisen järjestäminen sähköisessä viestintäympäristössä on teknisesti mahdollista. Havaitsemis- ja tunnistamiskyvyn luominen kuitenkin edellyttää poliisin nykyisistä teletiedonhankintakeinoista perusominaisuuksiltaan poikkeavaa ratkaisua, jossa tiedonhankinta toteutetaan viesti- ja tietoliikennevirtaa suodattavan järjestelmän avulla. Verkkotopologisesti tämä merkitsee sitä, että tiedonhankinta toteutetaan - päinvastoin 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 kansallista turvallisuutta vakavasti uhkaavaan 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, joka on ainoastaan uhkaviestintään osallistuvien henkilöiden käytössä.

Esityksen jaksosta 2.3. ilmenee, että 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 pääosin tiedustelumenetelmänä, vaikka joissain maissa sitä voidaan käyttää myös vakavien rikosten torjunnan keinona. Tiedustelun tarkoituksena on havaita ja tunnistaa keskeisimpiin kansallisiin turvallisuusetuihin kohdistuvia uhkia sekä jakaa uhkia koskevia analysoitua tietoa sitä tarvitseville tahoille. Sen tarkoituksena ei siis ole hankkia tulevaa rikosprosessia varten tietoa sellaisesta ennalta tunnetusta henkilöstä, jonka voidaan perustellusti olettaa syyllistyvän tai epäillä syyllistyneen tietyn vakavuusasteen rikokseen. Tietoliikennetiedustelu poikkeaa poliisin perinteisistä tele- ja muista tiedonhankintakeinoista ja myös useimmista tiedustelupalveluiden käyttämistä menetelmistä juuri sen vuoksi, että se teknisten ominaispiirteidensä johdosta mahdollistaa aiemmin tuntemattomien uhkien havaitsemisen ja tunnistamisen.

Tietoliikennetiedustelun avulla hankitaan vertailumaissa paitsi valtiojohdon ulko- ja turvallisuuspoliittista päätöksentekoa palvelevaa tietoa, myös tietoa, joka on tarpeen uhkien estämiseksi mahdollisimman varhaisessa vaiheessa. Uhkien torjunnan mahdollistamiseksi tietoliikennetiedustelulla hankittua tietoa voidaan yleensä tietyin edellytyksin luovuttaa poliisille, joka saamansa tiedon perusteella voi puuttua esimerkiksi terrorististen hankkeiden valmisteluun. Tietoa voidaan maasta riippuen ja erilaisin menettelyin luovuttaa myös muille hallintoviranomaisille, esimerkiksi maahantulosta ja sen valvonnasta vastaaville viranomaisille, jolloin uhkaava toiminta hallinnollisin toimenpitein saadaan torjuttua jo ulkorajalla. Tiedon luovuttamista poliisille ja muille viranomaisille on yleensä kuitenkin jollain tavalla rajoitettu, sillä asialliseksi ei ole katsottu, että tietoliikennetiedustelun kaltaista erityisen tehokasta ja muista tiedonhankintakeinoista luonteeltaan poikkeavaa menetelmää voitaisiin käyttää tiedon hankkimiseksi mistä tahansa rikoksesta, uhkasta tai riskistä.

Tietoliikennetiedustelussa käytettävät seulontaparametrit, joista voidaan käyttää nimitystä hakuehdot, voivat seuloa tiedustelujärjestelmän läpi virtaavan viesti- ja tietoliikenteen 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.

Esityksen jaksoissa 2.4 ja 2.5 on kuvattu tietoliikennetiedustelun järjestämisen kannalta relevanttia EIT:n ja Euroopan unionin tuomioistuimen oikeuskäytäntöä. Kuvauksesta ilmenee, että ihmisoikeustuomioistuin on pitänyt tietyin verrattain tiukoin reunaehdoin järjestettyä tietoliikennetiedustelua ihmisoikeussopimuksen 8 artiklan mukaisena.

Kun arvioidaan tietoliikennetiedustelun sallittavuutta EIS:n 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 niin sanotun 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.

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, 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 pidetään sitä, ettei tietoliikennetiedustelu voi olla tavanomaisena pidettävän verkko- tai muunkaan massarikollisuuden tutkintaa varten käytettävä menetelmä. Tiedonhankintalakityöryhmä menee kuitenkin tätä pidemmälle ja suosittaa tietoliikennetiedustelusta säätämistä harkittaessa otettavan lähtökohdaksi, ettei sen käyttöä rikostutkinnallisena menetelmänä tulisi sallia (mietinnön s. 62–63).

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. Hakuehtojen ja suullisten kuvailujen hyväksymisen tulisi tapahtua tiedusteluviranomaisesta erillisen lupaviranomaisen toimesta, ja niiden käyttö tiedustelussa tulisi kattavasti dokumentoida jälkikäteistä valvontaa varten. Lupaviranomaiseksi tiedonhankintalakityöryhmä ehdottaa tuomioistuinta, ja jälkikäteisen valvonnan toteuttamiseksi se ehdottaa harkittavaksi uuden riippumattoman laillisuusvalvontaelimen perustamista (mietinnön s. 67-69).

Tiedonhankintalakityöryhmä suosittelee, 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. Näin ollen edellä käsiteltyjen vertai-

lumaiden lainsäädännöistä otettiin poikkeava ja niitä tiukempi kanta 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 (mietinnön s. 64).

Hakuehtojen avulla tapahtuva viesti- ja tietoliikenteen seulonta on perustelua suorittaa 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. 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 tietoliikennetiedustelun tarkoituksena olisi hankkia tietoa ulkoisista uhkista Suomen rajan ylittävästä tietoliikenteestä, on perusteltua, että tietoliikennetiedustelun piiriin teknisistä syistä tuleva Suomessa oleskelevien osapuolten välinen tietoliikenne olisi hävitettävä (mietinnön s. 68).

Mitä tulee tietoliikennetiedustelulla saatujen tietojen käsittelyyn yleisemmin, mietinnössä todetaan, että EIT:n ratkaisukäytäntö 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.

Tiedonhankintalakityöryhmä toteaa, että tietoliikennetiedustelusta säätäminen sen ehdottamalla tavalla ei johtaisi sellaiseen laajamittaiseen, erittelemättömään, pitkäaikaiseen ja rajoittamattomaan tunnistamistietojen tallentamiseen, jota kansainvälisten tuomioistuinten oikeuskäytännössä on pidetty suhteellisuusperiaatteen vastaisena. Kyseinen 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.

Tietojen hankkiminen tietoverkkouhkista

Kansallista turvallisuutta uhkaavat tahot voivat kuitenkin käyttää sähköisiä viestintäverkkoja paitsi uhkia koskevaan viestintään, myös uhkien toteuttamiseen. Viestintäverkkojen välityksellä suoritetut kyberteot - esimerkiksi kybervakoilu, kyberterroriteot, 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 tuotekehittelytiedon.

Kyberuhkien havaitseminen riittävän varhaisessa vaiheessa on niiden estämisen tai ainakin niiden aiheuttamien vahinkoseurausten rajaamisen edellytys. Poliisin tele- ja muut tiedonhankintakeinot soveltuvat erittäin huonosti kyberympäristössä suoritettujen tekojen havaitsemiseen. Heikon soveltuvuuden syynä ovat yhtäältä edellä esityksessä käsitellyt teletiedonhankin-

takeinojen ominaispiirteet, jotka tässä yhteydessä voidaan yleistää kaikkia poliisin salaisia tiedonhankintakeinoja koskeviksi. Poliisin salaisten tiedonhankintakeinojen 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.

Poliisin tiedonhankintakeinojen heikko soveltuvuus kyberuhkien havaitsemiseen johtuu toisaalta myös kyberuhkien ominaispiirteistä. Suomeen ja sen kansalliseen turvallisuuteen kohdistetut kyberteot pannaan yleensä toimeen maan rajojen ulkopuolelta eikä toteuttaminen edellytä minkäänlaista fyysistä läsnäoloa täällä. 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 toteutumisen 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 vakavasti uhkaavilla 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 sähköisen viestinnän palveluista annetun lain 272 §:ssä säädettyihin toimivaltuuksiin. Säännös 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. Säännös sallii myös viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen, tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä ja muiden tähän rinnastettavien teknisluonteisten toimenpiteiden suorittamisen.

Haitalliset ohjelmat ja käskyt tunnistetaan ensi vaiheessa 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 sähköisen viestinnän palveluista annetun lain 272 § sen, että yritys, yhteisö tai viranomainen ottaa viestin sisällön manuaalisen käsittelyn kohteeksi.

Kansallisen turvallisuuden kannalta erityistä merkitystä omaavat tahot eivät välttämättä käytä sähköisen viestinnän palveluista annetun lain 272 §:ssä tarkoitettuja toimintaoikeuksia ainoastaan itse, vaan niiden tietoverkkoja saattaa suojata myös niin sanottu HAVARO-järjestelmä. HAVARO on Viestintäviraston Kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille ja valtionhallinnon toimijoille tarjoama tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä, jonka toiminta perustuu sähköisen viestinnän palveluista annetun lain 272 §:ään. HAVAROn tarkoituksena on tunnistaa erilaisten tunnisteiden avulla haitallista verkkoliikennettä ja tietoturvaa vaarantavia kehittyneitä verkkohyökkäyksiä (Advanced Persistent Threat, yleisesti APT). Järjestelmän toisena tarkoituksena on tukea paremman tilannekuvan muodostamista suomalaisiin tietoverkkoihin kohdistuvista tietoturvauhkista.

Sähköisen viestinnän palveluista annetun lain 272 §:n mukaisten toimintaoikeuksien käytössä - tapahtui se sitten tietoturvastaan huolehtivan yrityksen, yhteisön tai viranomaisen toimesta

taikka HAVARO-järjestelmän puitteissa - on tekniseltä kannalta kyse pitkälti samankaltaisesta hakuehtojen käyttöön perustuvasta tietoliikenteen seulonnasta ja seulonnassa esiin nousseiden viestien jatkokäsittelystä kuin tietoliikennetiedustelussa. Sähköisen viestinnän palveluista annetun lain 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 yhteistyönsä puitteissa. Kyberturvallisuuskeskuksen keskeisiä kansainvälisiä yhteistyökumppaneita ovat eri maiden valtionhallinnoissa toimivat niin sanotut 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 sähköisen viestinnän palveluista annetun lain 272 §:ssä tarkoitettujen toimintaoikeutettujen tahojen käytössä eivätkä ne myöskään ole syötettävissä HAVARO-järjestelmään. Toiminnan havaitsemiseksi tarvittavat tunnisteet ovat sellaista korkean suojaustason 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 niitä tunnisteita, joiden merkitys kansallisen turvallisuuden suojaamiseksi olisi suurin.

Sähköisen viestinnän palveluista annetun lain 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 torjuntaan. Tietoturvatoimenpiteiden suorittajan näkökulmasta sellaiset kansallisen turvallisuuden ylläpitämisen kannalta olennaiset tiedot kuten vakavimpien tietoturvaloukkausten syyt, olosuhteet, tekijät ja taustamotiivit eivät ole keskeisiä.

Edellä on todettu, että sähköisen viestinnän palveluista annetun lain 272 §:ssä tarkoitettu toiminta teknisesti muistuttaa läheisesti vertailuvaltioiden 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 kyberuhkien 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.

Tarkkailutyyppiset keinot

Poliisin rikosten estämiseksi, paljastamiseksi ja vaaran torjumiseksi käytettävistä tarkkailutyyppisistä keinoista säädetään poliisilain 5 luvussa. Tarkkailutyyppisiin keinoihin kuuluvat tarkkailu, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu ja teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkiminen sekä näitä keinoja tukeva laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen.

Tarkkailutyyppiset keinot olisivat niiden tehokkuuden ja toiminnallisen luonteen sekä miedon perusoikeuspuuttumisen takia tärkeitä tiedustelumenetelmiä siviilitiedustelussa. Tiedustelutoimivaltuuksien tarkoituksena olisi hankkia tietoa kansallista turvallisuutta vakavasti uhkaavasta tai sitä vakavasti uhkaavasta toiminnasta. Tiedonhankinnassa tarkkailutyyppisten keinojen rooli olisi tärkeä. Siviilitiedustelussa käytettävien toimivaltuuksien mahdollisimman varhaisessa vaiheessa tapahtuva ja oikea kohdentaminen vähentäisi niiden henkilöiden piiriä, joihin tiedustelu kohdentuu.

Erityisesti tarkkailutyyppisillä keinoilla saatavalla reaaliaikaisella tiedolla voidaan merkittävästi parantaa kansallisen turvallisuuden tilannekuvaa ja tätä kautta helpottaa päätöksentekoa siviilitiedustelun suuntaamisessa sekä sen painopisteiden asettamisessa. Myös tarkkailutyyppisillä keinoilla saatujen tietojen avulla pystyttäisiin tehostamaan siviilitiedustelun 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 ja vaikka kyse olisi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, niin henkilön yksilöimisellä ei olisi niin merkittävää roolia kuin rikosperusteisten toimivaltuuksien käytössä. Tietyn henkilön yksilöinti ei kaikissa tilanteissa olisi tarpeen erityisesti silloin, kun pyritään selvittämään tiedustelulla niin sanottua piilevää uhkaa, joka ei olisi viranomaisen tiedossa vasta kuin ilmiönä tai hankkeena. Tiedustelutoimivaltuuksien kohdalla ei olisi perusteltua tarvetta arvioida toimivaltuuden käytön erityisiä edellytyksiä nykyistä vastaavalla tavalla, 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 henkilöryhmän organisaatiosta, ryhmään kuuluvista henkilöistä ja henkilöryhmän aktiivisuudesta tietyillä alueilla sekä ryhmän toiminnan eri muodoista. Tiedoilla voi olla merkitystä niin operatiivisessa kuin valtion ylimmän johdon päätöksenteossa. Muun muassa edellä kerrotuista syistä johtuen myös tarkkailutyyppisiä toimivaltuuksia tulisi voida kohdistaa rajattuun henkilöryhmään.

Peitellystä tiedonhankinnasta säädettiin ensimmäistä kertaa nykyisessä poliisilaissa ja pakkokeinolaissa. Peitellyllä tiedonhankinnalla tarkoitetaan tiettyyn henkilöön kohdistuvaa lyhytkestoisessa vuorovaikutuksessa tapahtuvaa tiedonhankintaa, jossa poliisimiehen tehtävän salaamiseksi käytetään vääriä, harhauttavia tai peiteltyjä tietoja.

Peitelty tiedonhankinta toimivaltuuden käytön lyhytkestoisuudesta johtuen sijoittautuu suunnitelmallisen tarkkailun ja peitetoiminnan välimaastoon. Menetelmässä on selkeästi peitetoiminnan kaltaisia piirteitä, mutta toiminnassa ei muodostu samanlaista luottamusta suhdetta toimijan ja kohteen välille. Peitetoimintaa voi nykyisin rikosperusteisesti kohdistaa tiettyyn henkilöön, jonka ei tarvitse olla henkilö, jonka voidaan olettaa syyllistyvän rikokseen. Tiedustelutoiminnassa peitellyn tiedonhankinnan kohteena tulisi voida olla myös henkilöryhmä, vaikkakin varsinainen kanssakäyminen ja henkilön kohtaaminen olisi toiminnallisesti kohdistettavissa henkilöryhmässä oleviin yksittäisiin henkilöihin.

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 käyvät tilanteet, joissa yksi tai useampi rakennus tai maastonkohta täytyy saada ympärivuorokautiseen valvontaan eivätkä suojelupoliisin poliisimiehet voisi hoitaa tarkkailua valvottavan kohteen erityispiirteiden vuoksi.

Siviilitiedustelussa olisi oleellista saada mahdollisimman ajantasaista sekä yksilöityä tietoa viestinnän sisällöstä. *Tekninen kuuntelu* mahdollistaisi kattavan ja yksityiskohtaisen tiedonsaannin kansallista turvallisuutta vakavasti uhkaavasta toiminnasta sekä sellaiseen toiminaan liittyvistä henkilöistä ja henkilöryhmistä. Teknisessä kuuntelussa tarkoituksena olisi yhtä lailla joko kohdehenkilön tai -henkilöryhmän tunnistaminen tai tiedonhankinta heidän toiminnasta.

Henkilöiden, henkilöryhmien ja kuljetusten (esine, aine tai omaisuus) liikkeiden valvominen teknisen seurannan keinoin antaa suojelupoliisille mahdollisuuden suunnitella ja kohdentaa toimenpiteitään. *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 siviilitiedustelussa suojelupoliisimiesten suorittamaa tavanomaista tarkkailua. On kuitenkin syytä mainita, ettei tekninen seuranta, teknisen katselun ja kuuntelun tavoin, kaikissa tilanteissa täysin korvaa poliisimiehen tekemiä havaintoja. Henkilön tekninen seuranta sitä vastoin puuttuisi perus- ja ihmisoikeuksiin, kuten liikkumisvapauteen ja yksityiselämän suojaan.

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 rikoksen estämiselle merkityksellisen seikan tutkimiseksi.

Tiedonhankintalakityöryhmä on esittänyt säädettäväksi ulkomaan tietojärjestelmätiedustelusta, jolla tarkoitetaan ulkomailla sijaitsevassa tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin menetelmin tapahtuvaa tiedustelua. Käytännössä tietojärjestelmätiedustelu käsittäisi teknisestä kuuntelua ja teknisestä laitetarkkailua koskevat toimivaltuudet.

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.

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.

Siviilitiedustelussa käytettävien toimivaltuussäännösten tulisi kyetä vastaamaan toimintaympäristön teknisen kehittymisen asettamiin haasteisiin, mikä on otettava huomioon voimassa olevan lainsäädännön toimivuutta arvioitaessa. Tämä koskee niin käytettäviä menetelmiä kuin niiden kohteena olevaa toimintaakin.

Teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkimista koskevasta toimivaltuudesta olisi tarpeen säätää myös siviilitiedustelussa. Keinolla pystyttäisiin hankkimaan tietoja, joilla luottamuksellisen viestin suojaan puuttuvien toimivaltuuksien (telekuuntelu ja televalvonta) käyttö olisi mahdollista kohdistaa siviilitiedustelun kohteeseen, henkilön hallussa olevaan teleosoitteeseen tai telepäätelaitteeseen, joka 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. Erityisesti ulkomaan tiedustelussa olisi tarpeen mahdollistaa laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen myös telekuuntelun tai televalvonnan yhteydessä, koska niiden käyttäminen edellyttää lähtökohtaisesti teleoperaattorille tehtävää pyyntöä kytkentöjen tekemiseksi tai tietojen luovuttamiseksi. Ulkomaan tiedustelussa kyseisten toimivaltuuksia olisi tarkoituksenmukaista toteuttaa viranomaisen omilla laitteilla.

Peitetoiminta ja valeosto

Peitetoiminnalla tarkoitetaan poliisilain 5 luvun 28 §:n 1 momentin mukaan 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. Peitetoiminnan määritelmässä ei erikseen mainita henkilöryhmää. Peitetoimintaa koskevassa esityksessä ja päätöksessä yksilöitäväksi vaaditut henkilöt luonnollisesti voivat muodostaa ryhmän. Aiemmin henkilöryhmään kohdistuva peitetoiminta oli mahdollista.

Nykyisin peitetoiminnan kohteena olevat henkilöt tulisi voida yksilöidä vähintään heidän rikolliseen toimintaan liittyvien tehtäviensä avulla. Tämä puolestaan ei edellytä henkilön nimeämistä. Siviilitiedustelussa peitetoiminta tulisi voida kohdistaa myös tiettyyn henkilöryhmään, 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 rajattuun ihmisryhmään ja tätä kautta hankkia tietoa heidän toimintaansa ohjaavasta taustaorganisaatiosta ja kyseisen organisaation henkilöistä. Kyse voisi olla esimerkiksi valtiollisen henkilöryhmän hybridivaikuttamisesta Suomen oloihin.

Peitetoiminnan ja valeoston käyttäminen edellyttää, että se on välttämätöntä rikoksen estämiseksi tai paljastamiseksi. Peitetoiminnan kohdalla sen käytön edellytyksenä on lisäksi, että tie-

donhankintaa on rikollisen toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena. Yhtä tiukoista peitetoiminnan ja valeoston edellytyksistä on perustelua säätää myös siviilitiedustelussa tiedustelumenetelminä käytettävien peitetoiminnan ja valeoston yhteydessä, vaikka niiden tarkoituksena ei olisikaan hankkia tietoa rikoksen estämiseksi, paljastamiseksi ja selvittämiseksi.

Poliisilain 5 luvun 29 §:ssä säädetään rikoksentekokiellosta, joka vastoin pykälän otsikkoa sisältää oikeuden peitetoimintaa suorittavalle poliisimiehelle 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 perustein 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 edistää 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 rangaistussäännöstä, 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 siviilitiedustelun näkökulmasta, niin katsontakanta on vielä kauempana rikoksesta eikä toimivaltuuksien rikosperusteinen käyttö ei tulisi lainkaan kyseeseen. Muun muassa näistä syistä myöskään siviilitiedustelussa ei ole vastaavalla tavalla tarpeen osallistua järjestäytyneen rikollisryhmän toimintaan tai tehdä rikkomustyyppisiä rikoksia. Jos tällaiselle ilmenisi tarvetta, niin silloin tulisi soveltaa poliisilain 5 lukua (tai pakkokeinolain 10 lukua) ja siinä säädettyjä toimivaltuuksia.

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 peitetoiminnalla 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 järjestelmäämme nähden. Vastaavanlaista jännitettä ei voida katsoa sisältyvän tiedusteluperusteisesti käytettävään peitetoimintaan ja valeostoon, joiden perimmäisenä tarkoituksena ei ole hankkia tietoa rikosprosessia varten eikä muun kuin tiedusteluviranomaisen toiminnan suuntaamiseksi. Tästä käyttöedellytysperustasta huolimatta valeoston ja peitetoiminnan vahva lähtökohtainen salassa pidettävyys on välttämätöntä turvallisuussyistä ja tiedusteluoperaatioiden tuloksellisuuden kannalta. Paljastuessaan valeosto voi aiheuttaa peitepoliisin henkeen tai terveyteen kohdistu-

van uhkan kostotoimien muodossa. Kostotoimenpiteet voiva kohdistua myös poliisimiehen läheisiin sekä ulkopuolisiin henkilöihin, jotka ovat mahdollisesti toimineet suojelupoliisin 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 terroristiorganisaation sekä siihen kuuluvien solujen selvittäminen mahdottomaksi. Valeosto- ja peitetoiminnan kattava salassapito voi joka tapauksessa osoittautua ongelmalliseksi tilanteissa, joissa kyseisillä keinolla saadut tiedot etenevät käytettäväksi näyttönä. Tämä tulee huomioiduksi poliisilakiehdotuksen 5 a luvun 44 §:ssä.

Kun otetaan huomioon peitetoiminnan suorittaminen soluttautumalla ja tiedustelutoiminnan erityispiirteet, viittausta poliisilain 5 luvun 29 §:ään ei voida kuitenkaan pitää riittävänä. Maanpetosrikoksia koskevassa rikoslain 12 luvussa säädetään rangaistavaksi rikoksia, joiden tunnusmerkistön peitetoiminnan mukainen yhteydenpito saattaa täyttää. Näin ei useassa tapauksessa ole, koska peitetoimintaa suorittavalla virkamiehellä ei ole luvun rangaistussäännöksessä edellytettyä tarkoitusta tai koska hänen teollaan ei aiheuteta rangaistussäännöksessä tarkoitettua seurausta. Toisaalta esimerkiksi maanpetosta koskeva rikoslain 12 luvun 3 § soveltuu muun ohessa tilanteisiin, joissa Suomen kansalainen tietyissä uhkatilanteissa eli Suomea koskevan sodan, aseellisen selkkauksen tai miehityksen välittömästi uhatessa ryhtyy yhteistoimintaan vihollisen kanssa. Luvattomana tiedustelutoimintana (rikoslain 12 luvun 9 §) on puolestaan rangaistavaa esimerkiksi se, että tekijä vierasta valtiota vahingoittaakseen hankkii tietoja vieraan valtion maanpuolustuksesta, turvallisuudesta tai niihin välittömästi vaikuttavista seikoista ja siten aiheuttaa vahinkoa tai vaaraa Suomen ulkomaansuhteille. Rikoslain 12 luvun 11 §:ssä on lisäksi maanpetoksellista yhteydenpitoa koskeva rangaistussäännös, joka kattaa yhteydenpitoon ryhtymisen vieraan valtion tai sen asiamiehen kanssa luvussa tarkoitetun rikoksen tekemistä varten.

Oikeuskäytännön varaan ei voida jättää sitä, miten tiedustelutoiminnassa käytettävä peitetoiminta suhtautuu rikoslain 12 luvun säännöksiin. Toisaalta on huomattava, että rikoslain 12 luvussa kaikkien maanpetosrikosten tekotapoja ei ole sidottu pelkästään peitetoiminnalle ominaiseen kanssakäymiseen toisen henkilön tai henkilöryhmän kanssa. Rikoslain 12 luvun 5 §:n mukaista vakoilua voidaan toteuttaa myös teknisillä tiedonhankintakeinoilla. Myös tietoliikennetiedustelua koskevan lain mukainen toiminta voi kohdistua vieraan valtion tietoliikenteeseen. Tämän vuoksi rajanvetoa ei tule tehdä pelkästään peitetoimintaan, vaan yleisemmin tiedustelutoimintaan eli ehdotetun poliisilain 5 a luvun mukaisten ja ehdotetun tietoliikennetiedustelusta siviilitiedustelussa annettavan lain mukaisten tiedustelumenetelmien käyttöön. Koska vastaavat tiedonhankintakeinot tulisivat käyttöön myös sotilastiedustelussa (ehdotettu laki sotilastiedustelusta), vastaavat näkökohdat koskisivat myös sotilastiedustelussa käytettäviä tiedustelumenetelmiä. Selvyyden vuoksi rajanveto rikoslain 12 luvussa rangaistavaksi säädettyjen tekojen ja tiedustelumenetelmien käyttämisen välillä on syytä tehdä lisäämällä mainitun luvun loppuun rajanvetoa koskeva säännös

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. Toiminnan laillisuuden rajojen koettelemista ei voida jättää suorittavalle tasolle, vaan ne pitää olla operatiivisesta toiminnasta vastaavan tahon hyväksymiä.

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

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, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun esitutkintaviranomaisen ulkopuoliselta henkilöltä.

Nykysääntely mahdollistaa tietolähteen ja tietoa hankkivan poliisimiehen yhteydenpidon salaamiseen poliisilain 5 luvun 46 §:ssä (tiedonhankinnan suojaaminen) säädetyin edellytyksin. 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 tässä pykälässä tarkoitettu suojaus ja vain he voisivat sitä käyttää tiedonhankinnan suojaamiseksi.

Suojelupoliisilla 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. Erityisen vakavasti tulee suhtautua silloin, kun tietolähteen henkeen ja terveyteen kohdistuva uhkan lähde on valtiollinen toimija. Kyse voi olla esimerkiksi poliittisen turvapaikan hakemisesta, jolloin lähtömaan valtiolla voi olla suuri intressi vaikuttaa tietolähteenä olevan henkilön toimintaan. Tällöin tietolähteen suojaaminen edellyttää erilaista intensiteettiä mitä 5 luvun tietolähdetoiminnassa. Suojelupoliisin 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 laissa todistajansuojeluohjelmasta (65/2014). Edellä kerrotusta johtuen olisi tarpeen säätää tietolähteen turvaamisesta, joka voitaisiin aloittaa ennakollisesti.

Valvotussa läpilaskussa on lähes poikkeuksetta kysymys laittomasti hallussa pidettävien esineiden, aineiden tai omaisuuden kuljetuksen seurannasta ja tarkoituksena on puuttumista siirtämällä selvittää taustalla olevaa vakavaa ja usein myös järjestäytynyttä rikollisuutta. Valvotussa läpilaskussa tarkoituksena voi olla selvittää koko jakeluketju ja se, mihin kuljetus lopulta päätyy. Puuttumisen siirtäminen liittyy lähes yksinomaan siihen, että kuljetus, joka päästetään valvottuna läpi, niin kuljetuksen sisältämän lastin hallussapito on säädetty rangaistavaksi tai se täyttää valmistelutyyppisen rikoksen esimerkiksi kaksikäyttötuotteiden kohdalla. Tiedustelutoiminnassa ei ole lähtökohtaisesti tarkoitus hankkia rikosta koskevaa tietoa, vaan rikosperusteisista toimivaltuuksista säädetään erikseen. Valvotusta läpilaskusta ei näin ollen ole tarpeen säätää tiedustelumenetelmänä.

Päätöksenteko

Päätösvalta eräiden salaisten tiedonhankintakeinojen käyttämisestä on edellä olevassa jaksossa lainsäädäntöä ja käytäntö osioissa kuvatulla tavalla jakautunut tuomioistuimelle tai pidättämiseen oikeutetulle poliisimiehelle. Tuomioistuimen päätösvaltaan kuuluvat poliisilain 5 luvussa tarkoitetut salaiset tiedonhankintakeinot ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, tekninen kuuntelu tietyiltä osin, tekninen katselu tietyiltä osin, tekninen seuranta tietyiltä osin ja tekninen laite-tarkkailu. Sellaisissa kiireellisissä tilanteissa, joissa poliisi voi tilapäisesti itse päättää tuomioistuimen päätösvaltaan kuuluvien toimivaltuuksien käytöstä, asia on saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta. Poliisi voi kuitenkin päättää tietyistä salaisista tiedonhankintakeinoista henkeä tai terveyttä

uhkaavan vaaran torjumiseksi sekä henkilön suostumuksella tehtävästä televalvonnasta epäiltäessä sellaisia rikoksia, jotka suoraan liittyvät teleosoitteeseen tai telepäätelaitteeseen.

Poliisi päättää itsenäisesti suunnitelmallisen tarkkailun, peitellyn tiedonhankinnan, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisen, peitetoiminnan ja valeoston, tietolähteen ohjatun käytön sekä valvotun läpilaskun käyttämisestä.

Tuomioistuimen päätösvaltaan kuuluva salaisen tiedonhankintakeinon käyttöä koskeva lupavaatimus 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 tiedonhankintakeinoa 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.

Kun harkitaan tiedustelumenetelmiä koskevasta päätöksenteosta säätämistä, niin ei ole syytä poiketa poliisilain 5 luvun salaisten tiedonhankintakeinojen käyttöä koskevista valinnoista. Poliisilain 5 a luku olisi myös tältä osin perusteltua rakentaa olennaisilta osiltaan 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 pakkokeinolainsäädännön uudistamisen yhteydessä (Oikeusministeriön komiteanmietintö 2009:2) perustuslakivaliokunnan kannanotot mukaan lukien. Siksi myös 5 a luvussa tiedustelumenetelmien päätöksentekoa koskevien perusratkaisujen kohdalla on perusteltua seurata mahdollisimman pitkälle 5 luvussa omaksuttua sääntelyä.

Tiedustelumenetelmien lisäksi tulee säätää ulkomaan tiedustelusta päättämisestä. Tuomioistuimella ei lähtökohtaisesti ole toimivaltaa päättää toimivaltuuden käytöstä muualla kuin Suomessa. Operatiivista päätöksentekoa ei myöskään ole tarkoituksenmukaista viedä oikeudellisessa järjestelmässä uusille toimijoille ulkomaan tiedusteluun liittyvien ulkopoliittisesti sensitiivisten elementtien takia. Kansainväliseen vertailuun kuuluvien joidenkin maiden kohdalla ulkomaan tiedustelusta päättää tiedusteluviraston päällikkö. Ulkomaan tiedustelua kos-

kevasta päätöksenteosta siviilitiedustelussa on perusteltua säätää vastaavalla tavalla. Suojelupoliisin päällikkö päättää nykyisinkin kaikkein kovimpien keinojen, peitetoiminnan ja valeoston käyttämisestä, joiden päätösarviointiin liittyy vakavuudeltaan vastaavantyyppisiä seikkoja mitä ulkomaan tiedusteluun.

Myös tiedustelumenetelmien käytöstä ilmoittamista koskeva sääntely olisi perusteltua mainituista syistä säännellä vastaavalla tavalla mitä poliisilain 5 luvussa siviilitiedusteluun liittyvät erityispiirteet huomioiden.

Kaikille salaisille tiedonhankintakeinoille yhteiset säännökset

Tiedonhankinnan suojaaminen

Salaisen tiedonhankinnan suojaamisesta säädetään poliisilain 5 luvun 46 §:ssä. Pykälän 1 momentti koskee poliisin mahdollisuutta siirtää puuttumista rikokseen salaisen tiedonhankintakeinon käytön aikana. Edellytyksenä on, että 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). Suojaamisen 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.

Vääriä merkintöjä ei kuitenkaan saa jättää rekistereihin, vaan pykälän 3 momentissa säädetään rekisterimerkintöjen oikaisuvelvollisuudesta.

Vastaavanlaisesta tiedonhankinnan suojaamisesta, kuin mitä edellä mainituissa 2 ja 3 momenteissa säädetään, on korostunut tarve säätää myös siviilitiedustelun suojaamiseksi. Lähtökohtana on, että koko siviilitiedustelutoimintaa tulee voida suojata. Tiedustelutoimintaan liittyy monenlaisia herkkyyksiä ja toiminnan 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 tämän tahdonvastaisesti. Paljastumisriskin minimoimiseksi suojauksen käyttäminen tulisi mahdollistaa jo aikaisessa vaiheessa. Esimerkiksi tiedustelutehtävässä toimivan virkamiehen suojaus soluttautumalla tiettyyn organisaatioon edellyttää erittäin intensiivisiä suojaustoimia ja niiden aloittamista hyvin varhaisessa vaiheessa. Siviilitiedustelutoiminnassa suojauksen käyttämisen kohdalla ei olisi myöskään vastaavanlaisia oikeusturvaongelmia mitä rikosperusteisia toimivaltuuksia käytettäessä, sillä siviilitiedustelun lähtökohtaisena tarkoituksena olisi hankkia tietoa toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Ilmaisukielto

Poliisilain 5 luvun 48 §:ssä säädetään salaista tiedonhankintaa koskevasta ilmaisukiellosta. Kyseisen pykälän 1 momentin sääntelystä ilmenee, ettei ilmaisukieltoa voida antaa kenelle tahansa henkilölle, esimerkiksi taloyhtiön asukkaalle tai muulle sivulliselle, joka sattumalta havaitsee teknisen tarkkailun laitteen asennuksen. Ilmaisukiellon määräämisen edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytön toteuttamisessa. Pykälän 2 momentin mukaan ilmaisukielto voidaan antaa enintään vuodeksi kerrallaan. Kielto on annettava saajalleen kirjallisena todisteellisesti tiedoksi ja siinä on yksilöitävä kiellon kohteena olevat seikat, mainittava kiellon voimassaoloaika ja ilmoitettava sen rikkomiseen liittyvästä rangaistusuhasta.

Tiedustelumenetelmiä käytettäessä saatetaan joutua tilanteisiin, joissa ulkopuolisen avun käyttäminen on välttämätöntä. Esimerkiksi teknisen tarkkailun laitteiden asennuksessa saatetaan tarvita ulkopuolista asiantuntemusta tai rakennuksen huoltoyhtiön palveluksia. Näin ollen sivulliset voivat saada tietoja, joiden ilmaiseminen voi vaarantaa tiedustelumenetelmän käytön ja koko tiedustelutoiminnan. Ilmaisukiellon tarkoituksena olisi suojata tiedustelumenetelmän käytön sekä tiedustelutoiminnan paljastumista, mutta myös salassa pidettäviä taktisia ja teknisiä menetelmiä. Ilmaisukiellosta on tarpeen säätää myös tiedustelumenetelmien yhteydessä.

Kuuntelu- ja katselukiellot

Poliisilain 5 luvun 50 §:ssä säädetään kuuntelu- ja katselukielloista. 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 ri-

koksesta 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. Siviilitiedustelussa 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 siviilitiedustelun kohdehenkilöiden asemaa ja henkilörelaatioita voi olla hankala tunnistaa alkuvaiheessa eikä oikeudenkäymiskaaren 17 luvun 17 §:ssä tarkoitettujen läheisten välinen viestinnän suojaaminen ole yhtä merkityksellisessä asemassa mitä rikosprosessissa.

Siviilitiedustelun 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 kui-

tenkaan 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

Poliisilakiin 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 koskevien 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 kansallista turvallisuutta uhkaavaa tietoa. Monessa tapauksessa kyseinen tieto tulisi välittömästi hävittää irrelevanttiusperusteella, mutta osa kansallisen turvallisuuden kannalta merkityksettömästä tiedosta saattaisi koskea vakavaa rikosta. Siksi tarvitaan sääntelyä ohjaamaan tällaisen tiedon eteenpäin saattamista paitsi relevanteille tiedonsaajille ylipäätään, erityisesti myös esitutkintaviranomaisille. Siviilitiedustelun ja rikosprosessin rajapintaan asemoitava, ja siinä tiedon luovuttamista esitutkintaviranomaisille säätelevä normi olisi monitahoinen ja periaatelatautunut. Rikoksen täyttymistä edeltävässä vaiheessa sen estämistavoitteella on etusija esitut-

kintavaihetta 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. Siviilitiedustelussa puolestaan kansallisen turvallisuuden suojaamistavoitteella on lähtökohtainen etusija rikoksen estämisintressiin ja selvittämisintressiin nähden. Siviilitiedustelussa 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 luovuttamisesta rikostorjuntaan, sillä siinä ei ole otettu huomioon siviilitiedustelun kansalliseen turvallisuuteen kytkeytyvää suojaamisintressiä.

Ensimmäinen lähtökohta tiedon luovuttamista rikostorjuntaan koskevalle säännökselle on, että siinä olisi asetettava ilmoitusvelvollisuus esitutkintaviranomaiselle viime kädessä sellaisista rikoksista, joista säädetty ankarin rangaistus on kuusi vuotta vankeutta, 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 siviilitiedustelun 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 siviilitiedustelu osaltaan pyrkii 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 kuin 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 hyväksynyt 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 yksilöinti-

tietojen 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, ilmoitusta 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 poliisilain 5 a luvussa. Koska siviilitiedustelulla tarkoitetaan suojelupoliisin suorittamaa tiedonhankintaa, ilmoituksen lykkäämistä ja kokonaan ilmoittamatta jättämistä koskevan vaatimuksen esittäjäksi tulisi säätää suojelupoliisin päällystöön kuuluva poliisimies. Ilmoittamisen lykkääminen ja kokonaan ilmoittamatta jättäminen on syytä jättää tuomioistuimen harkintaan, jossa eri osapuolten oikeudet ja tiedonsaantitarpeet pystytään parhaiten arvioimaan. Ottaen huomioon, että poliisilain 5 a luvun sääntely rakentuisi tiedonhankinnalle kansallista turvallisuutta uhkaavasta toiminnasta, ilmoittamisen lykkäämisen ja kokonaan ilmoittamatta jättämisen perusteisiin tulisi lisätä kansallisen turvallisuuden varmistaminen. Lisäksi olisi arvioitava, minkälainen ilmoittamisjärjestely olisi niin kohteen oikeusturvan kuin käytännöllisten ilmoittamismahdollisuuksienkin kannalta asianmukaisin poliisilain 5 a lukuun uutena ehdotettavien

menetelmien eli paikkatiedustelun ja jäljentämisen sekä erillisessä laissa säädettäväksi ehdotetun tietoliikennetiedustelun osalta. Tiedustelumenetelmän käytöstä ei olisi velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos tiedonhankinnan kohteena olisi vieraan valtion viranomainen tai sen lukuun toimiva.

Suojelupoliisin käyttämät pakkokeinot

Etsintä

Poliisilaissa ei nykyisin ole tiedonhankintatarkoituksessa paikanetsintää tai kotietsintää koskevia säännöksiä. Pakkokeinolain 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 yhteydessä 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 suojelupoliisin tiedonhankinta paljastuisi tiedonhankintatoimenpiteen kohdehenkilölle, vaarantaisi tämä siviilitiedustelun tiedonhankinnan tarkoituksen toteutumisen sekä saattaisi aiheuttaa suojelupoliisin virkamiehelle hengen tai terveyden vaaran.

Kohdehenkilö voi muuttaa toimintatapojansa salatakseen ne tiedusteluviranomaiselta, ryhtyä viranomaisiin kohdistuviin muihin vastatoimiin tai varoittaa potentiaalisia muita tiedustelun kohteita siitä, että hän on tiedonhankinnan kohteena. Näin ollen liian aikaisessa vaiheessa aktualisoituva suojelupoliisin ilmoitusvelvollisuus voi tehdä tyhjäksi koko sen tarkoituksen, jossa tiedonkeruuta harjoitetaan.

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

Esimerkiksi terroristiryhmän toiminta on luonteeltaan suunnitelmallista, systemaattisesti rikolliseen päämäärään pyrkivää ja kollektiivista. Kollektiivisuuden yksi seuraus on se, että terrorististen hankkeiden mahdollistamiseksi välttämättömät osatoimenpiteet jaetaan suoritettaviksi useille jäsenille. 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 suojelupoliisin tiedonhankintakeinot eivät aina tuota sellaista tietoa, jonka avulla rikos voitaisiin estää ennalta tai paljastaa.

Edellä kerrotusta huolimatta on tosiasia, että terroristien toiminta 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, matkustusasia-

kirjoja, 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 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 suojelupoliisi saa luotettavana pidettäviä tietoja siitä, että jonkin tuntemattoman tahon on määrä tavata kohdehenkilöä ja toimittaa tälle tärkeä suunnitelma. Suojelupoliisilla on tieto toimituksesta, mutta ei sen tarkasta ajankohdasta. Jos suojelupoliisi 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 tässä yhteydessä kutsua paikkatiedusteluksi.

Jäljentäminen

Siviilitiedustelussa 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 poliisilain 5 a 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 siviilitiedustelutoiminnan ja siinä käytettävien tiedustelumenetelmien on tarkoitus pysyä sen kohteelta salassa, niin myös henkilölle kuuluvan asiakirjan, esineen tai omaisuuden haltuunottaminen ei tule kyseeseen. Siksi jäljentäminen on välttämätön keino, jotta pystyttäisiin välttämään tehtyjen havaintojen ja löytöjen taltioiminen ja samalla minimoimaan paljastumisriski, kuten esimerkiksi tiedusteluoperaation paljastuminen paikkatiedustelun yhteydessä. Jos siviilitiedustelussa, 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 siirrytään tiedustelumenetelmien käytöstä rikosperusteisten toimivaltuuksien käyttöön ja asia siirrettäisiin keskusrikospoliisille eräin poikkeuksin.

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. Jäljentämisessä on kuitenkin huomioitava sen kohde. Jos jäljentämisen kohteena on asiakirja, joka sisältää henkilöiden välistä viestintää, niin silloin jäljentämisen käyttöedellytykset tulisi säätää korkeammiksi kuin muun kuin luottamuksellisen viestin suojaan kohdistuvan jäljentämisen.

Ulkomaantiedustelu

Suojelupoliisin toimintaympäristössä viime vuosina tapahtuneiden muutosten taustalla on sisäiseen ja kansalliseen turvallisuuteen kohdistuvien uhkien ja niihin liittyvien ilmiöiden kiihtyvä kansainvälistyminen ja tietoteknistyminen. Sisäisen ja ulkoisen turvallisuuden väliset rajat ovat hämärtyneet, ja sisäisen turvallisuuden ulkoinen ulottuvuus on korostunut. 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 kansallisen turvalli-

suuden 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 kansalliselle turvallisuudelle 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 yleissopimuksen 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 voi pitää myöskään kansainvälisoikeudellisesti kielletyksi, koska lähes kaikki valtiot harjoittavat tätä toimintaa. Kyse on maailmanlaajuisesti vakiintuneesta toiminnasta, johon yksittäisten valtioiden asennoituminen määräytyy sen mukaan, ovatko ne kulloisessakin tapauksessa tiedustelevan valtion tai kohdevaltion roolissa.

Vaikka tiedustelutoimintaa ei olekaan säännelty, osoittavat useat kansainväliset esimerkit, että toiminnassa on hyödynnetty kansainvälisen sopimusjärjestelmän mahdollisuuksia. Toiminnassa on käytetty diplomaattisia suhteita koskevalla Wienin yleissopimuksella (SopS3-5/1970) taattua diplomaattisen edustajan koskemattomuutta ja vapautta kohdevaltion rikosoikeudellisesta tuomiovallasta.

Suojelupoliisin tiedonhankinta ulkomailla

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

Kansainvälisestä vertailusta voidaan havaita, että ulkomailla tehtävää tiedonhankintaa koskeva päätöksenteko vaihtelee maittain. Päätöksenteosta voi vastata esimerkiksi tiedusteluviranomainen itse tai jokin poliittisesti vastuunalainen taho. Jos päätöksenteosta vastaa tiedusteluviranomainen, tapahtuu se yleensä valtiojohdon linjausten puitteissa. Tiedustelussa käytettävät menetelmät kohdistuvat vieraan valtion suvereniteettiin kohdemaassa ja myös mahdollisesti kolmannessa valtiossa, jonka kautta tiedonhankintaa tehdään. Tämän vuoksi ulkomaan tiedustelun poliittinen ulottuvuus korostuu. Tiedustelun mahdolliset vaikutukset ja riskit vaikuttaisivat päätöksentekomenettelyyn. Ulkomailla tehtävästä siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättäisi aina suojelupoliisin päällikkö. Suomalaisilla tuomioistuimilla ei ole toimivaltaa päättää menetelmien käytöstä Suomen alueen ulkopuolella eikä se tästä syystä tule kyseeseen päätöksentekotahona. Lisäksi ulkomaantiedustelun ulkopoliittisten herkkyyksien vuoksi on perusteltua, että riskin menetelmien käyttämisestä kantaisi ulkomaantiedustelua suorittava taho eli suojelupoliisi. Siviili- ja sotilastiedustelutoiminnan yhteensovittamisesta säädettäisiin erikseen. Ulkomaantiedustelun ulkopoliittisia ulottuvuuksia käsiteltäisiin siten myös siviili- ja sotilastiedustelun yhteensovittamisen yhteydessä, jolloin mukana olisivat keskeiset ulkopoliittiset tahot.

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

Kansainvälinen yhteistyö

Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä. Poliisin kansainvälisestä yhteistoiminnasta säädetään poliisilain 9 luvun 9 §:ssä. Poliisin osalta voimassa oleva kansallinen sääntely mahdollistaa oikeus- ja virka-avun antamisen vieraan valtion poliisille ja vastaavasti poliisin vieraan valtion poliisilta saaman oikeus- ja virka-avun, jos siitä on erikseen säädetty tai sovittu. Vastaavasti vieraan valtion poliisimiehen oikeudesta käyttää suomalaisen poliisimiehen toimivaltuuksia on voimassa, mitä siitä erikseen säädetään tai on Suomea velvoittavassa kansainvälisessä sopimuksessa sovittu. Suojelupoliisin tekemässä turvallisuus- ja tiedustelupalveluiden kanssa tehtävässä kansainvälisessä yhteistoiminnassa ei kuitenkaan noudateta poliisin oikeus- ja virka-apua koskevaa sääntelyä.

Suojelupoliisin kansallisen turvallisuuden suojaamiseen liittyvään työhön kuuluu olennaisesti yhteistoiminta muiden maiden turvallisuus- ja tiedustelupalveluiden kanssa. Tähän yhteistyöhön kuuluu muun muassa luottamuksellinen tiedonvaihto erilaisista turvallisuusuhkista. Kansainvälisen tiedusteluyhteistyön osalta ei ole olemassa monenvälisiä kansainvälisiä eikä myöskään Suomen osalta kahdenvälisiä valtiosopimuksia. Yhteistoiminnan ja tiedustelutiedon vaihdon osalta on kuitenkin vuosien varrella muotoutunut kansainväliset vakiintuneet menettelytavat. Suojelupoliisin ja ulkomaalaisten turvallisuus- ja tiedusteluviranomaisten välillä vaihdettuja tietoja koskee kansainväliseen vakiintuneeseen tapaoikeuteen perustuva käyttötarkoitussidonnaisuuslauseke, joka estää tietojen luovuttamisen kolmannelle osapuolelle ilman luovuttajamaan nimenomaista suostumusta. Suojelupoliisikin on kansainvälisessä toiminnassaan sitoutunut noudattamaan tätä sopimuslauseketta. Tietojen vaihdon lisäksi kansainvälistä yhteistoimintaa on myös esimerkiksi tekninen tuki, koulutus, virkamiesvaihto ja kansainvälinen yhdyshenkilötoiminta.

Kansainvälisestä turvallisuus- ja tiedustelupalveluiden välisestä yhteistoiminnasta ei ole säädetty voimassa olevassa poliisilaissa. Siksi olisi tarpeen mahdollistaa kansainväliset siviilitiedustelun alalla tehtävät yhteisoperaatiot siten, että suojelupoliisin poliisimies voisi osallistua niihin ulkomailla ja vieraan valtion turvallisuus- tai tiedustelupalvelun virkamies voisi osallistua sellaiseen Suomen alueella säätämällä tästä lailla.

Suojelupoliisin oikeudellinen valvonta

Poliisin salaisia tiedonhankintakeinoja valvovat poliisilain 5 luvun 63 §:n 1 momentin mukaan salaisia tiedonhankintakeinoja käyttävien yksiköiden päälliköt sekä sisäministeriö suojelupoliisin osalta ja Poliisihallitus alaistensa yksiköiden osalta. Sisäministeriön on 2 momentin perusteella annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta. Vastaavalla tavalla säädetään pakkokeinolain 10 luvun 65 §:n kohdalla salaisten pakkokeinojen käytöstä.

Salaisten tiedonhankintakeinojen kirjaamisesta, seurannasta ja tiedonhankintakeinoista laadittavista selvityksistä säädetään myös esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankin-

nasta annetussa valtioneuvoston asetuksessa. Lisäksi viranomaisilla on sisäisiä tiedonhankintaa koskevia määräyksiä.

Eduskunnan oikeusasiamiehen salaisiin tiedonhankintakeinoihin kohdistuva valvonta perustuu pääosin tarkastuksiin ja muuhun oma-aloitteiseen valvontaan. Kanteluita salaisten tiedonhankintakeinojen käytöstä tehdään vain vähän, vuosittain kymmenkunta. Oikeusasiamies antaa eduskunnalle joka vuodelta kertomuksen toiminnastaan sekä lainkäytön tilasta ja lainsäädännössä havaitsemistaan puutteista. 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 omaa sisäistä laillisuusvalvontaa ja että sitä voidaan luonnehtia valvonnan valvonnaksi.

Henkilötietojen käsittely

Voimassa olevassa poliisin henkilötietojen käsittelystä poliisitoimessa annetussa laissa säädetään paitsi suojelupoliisiin toiminnallisesta tietojärjestelmästä niin myös henkilötietojen käyttämisestä poliisilain 1 luvun 1 §:ssä säädetyissä tarkoituksissa sekä tiedonvaihdosta muiden poliisiyksiköiden, muiden viranomaisten sekä muiden valtioiden toimivaltaisten viranomaisten kanssa. Tiedonvaihdosta säädetään myös muissa laeissa. Poliisin henkilötietolaissa sen sijaan ei säädetä toimivaltuuksista. Esimerkiksi suojelupoliisin salassapitosäännösten estämättä tapahtuvasta tiedonsaantioikeudesta sekä tiedonluovuttamisoikeudesta ja -velvollisuudesta säädettäisiin jatkossakin poliisilaissa.

Suojelupoliisin toimivaltuuksia ehdotetaan tässä esityksessä muutettavaksi. Suojelupoliisin tehtävää esitettäisiin niin ikään muutettavaksi poliisin hallinnosta annetussa laissa siten, että se käsittäisi tiedon hankkimisen myös kansallisen turvallisuuden suojaamiseksi. Myös poliisilain 1 luvun 1 §:n 1 momenttia ehdotettaisiin muutettavaksi siten, että siihen lisättäisiin poliisin tehtäväksi kansallisen turvallisuuden suojaaminen. Suojelupoliisin lakisääteinen tehtävä pitäisi muutoksineen sisällään jatkossakin aktiivisen Suomen turvallisuusympäristön seurannan, turvallisuusuhkia koskevan ennakoivan tiedonhankinnan ja hankittujen tietojen analysoinnin. Tietoa hankitaan ja saadaan esimerkiksi avoimista lähteistä tai muilta viranomaisilta erikseen säädetyillä tiedon-saantioikeuksilla. Suojelupoliisi hankkii tietoa siten laajemmin kuin pelkästään tehtävän suorittamiseksi säädetyillä salaisilla tiedonhankintakeinoilla tai tässä esityksessä säädettäväksi esitettävillä uusilla tiedustelutoimivaltuuksilla.

Sisäministeriö asetti 28.1.2016 lainsäädäntöhankkeen, jonka tarkoitus on uudistaa poliisin henkilötietojen käsittelyä koskeva lainsäädäntö. Poliisin henkilötietolain kokonaisuudistuksen on tarkoitus tulla voimaan vuoden 2019 aikana. Koska uusilla tiedustelutoimivaltuuksilla saa-

taisiin muiden tietojen ohella myös henkilötietoja ja koska tiedustelutoimivaltuuksista mahdollisesti säädettäisiin siten, että ne tulisivat voimaan jo ennen uudistettavaa poliisin henkilötietolakia, niin voimassa olevaa poliisin henkilötietolakia ehdotettaisiin muutettavaksi. Voimassa olevaan poliisin henkilötietolakiin ei ole tässä yhteydessä havaittu merkittäviä muutostarpeita. Poliisin henkilötietolaista ainoastaan suojelupoliisin toiminnallista tietojärjestelmää koskeva 5 §, poliisin oikeutta saada tietoja eräistä rekistereistä ja tietojärjestelmistä koskeva 13 § sekä tarkastusoikeutta koskeva 45 § ehdotettaisiin muutettavaksi.

Suojelupoliisilla on tehtävänsä suorittamista varten ylläpidettävä suojelupoliisin toiminnallinen tietojärjestelmä. Suojelupoliisi ei talleta tehtävänsä kannalta tarpeellisia henkilötietoja muihin rekistereihin. Siten esitettäisiin, että myös uusilla toimivaltuuksilla saatavat henkilötiedot talletettaisiin tähän järjestelmään. Lakia esitettäisiin muutettavaksi siten, että järjestelmään voitaisiin tallettaa henkilötietoja, joita on tarpeen käsitellä kansallisen turvallisuuden suojaamiseksi, oikeus- ja yhteiskuntajärjestystä tai valtion turvallisuutta vaarantavien hankkeiden tai rikosten estämiseksi, paljastamiseksi tai selvittämiseksi.

Järjestelmään voisi siten tallettaa suojelupoliisin lakisääteisen tehtävän suorittamiseksi tarpeellisia henkilötietoja. Suojelupoliisin tehtävä määriteltäisiin jatkossakin laajasti ja se muodostuisi muustakin kuin sitä varten säädetyistä toimivaltuuksista. Valtion turvallisuuden turvaaminen ja kansallisen turvallisuuden suojaaminen eivät ole synonyymeja, mutta kumpaakin käytetään jo voimassa olevassa lainsäädännössä ja niiden on käsitteinä käytännössä tarkoitettu tarkoittavan suunnilleen samaa. Tässä yhteydessä kummallakin termillä kuvattaisiin suojelupoliisin tehtävää. Tästä syytä kansallisen turvallisuuden suojaamisella ja valtion turvallisuuden turvaamisella tarkoitettaisiin poliisin henkilötietolaissa käytännössä samaa asiaa ja samaa asiaa kuin mitä säädetään suojelupoliisin tehtävästä. Kansallisen turvallisuuden suojaamisella tai valtion turvallisuuden turvaamisella tarkoitetaan tehtävää oikeus- ja yhteiskuntajärjestyksen ylläpitämiseksi siten, että kansalaisten perusturvallisuus ja yhteiskunnan toiminnot turvataan. Henkilötietoja voitaisiin siten käsitellä samalla tavoin siten kuin sekä kansallista turvallisuutta että valtion turvallisuutta koskien säädetään. Koska näiden käsitteiden voitaisiin katsoa poliisin henkilötietolaissa tarkoittavan samaa asiaa, ei tässä yhteydessä ehdotettaisi näiden käsitteiden yhtenäistämistä koko poliisin henkilötietolakia koskien. Poliisin henkilötietojen käsittelyä koskevassa kokonaisuudistuksessa sen sijaan käsitteet olisi tarkoitus yhtenäistää ja siten käyttää vain käsitettä kansallinen turvallisuus niissä tilanteissa, joissa ei olisi esimerkiksi tarpeen erikseen mainita kaikkia suojelupoliisin tehtäviä.

Suojelupoliisin tehtävän ja siihen liittyvien henkilötietojen käsittelyn kannalta keskeistä on, että eri toimivaltuuksilla saatuja henkilötietoja voitaisiin suojelupoliisissa käsitellä samalla tavoin ja samassa rekisterissä eikä niiden luovuttamiselle olisi eriasteisia kynnyksiä riippuen niiden saantitavasta. Suojelupoliisin tehtävän suorittamiseksi henkilötietoja käsiteltäisiin joko käyttötarkoitussidonnaisuuden edellyttämällä tavalla tai siitä poiketen valtion turvallisuuden turvaamiseksi tai kansallisen turvallisuuden suojaamiseksi.

Esitutkintatoimivaltuudet

Poliisihallinnossa suojelupoliisi vastaa rikoslain12 (maanpetosrikokset) ja 13 luvussa (valtiopetosrikokset) tarkoitettujen rikosten estämisestä, paljastamisesta ja myös niiden selvittämisestä. Suojelupoliisi vastaa esitutkinnasta myös, jos rikoslain 17 luvun 1 §:ssä tarkoitettu rikos (julkinen kehotus rikokseen), 15 luvun 10 §:n 1 momentissa tarkoitettu rikos (törkeän rikoksen ilmoittamatta jättäminen) tai 15 luvun 11 §:ssä tarkoitettu rikos (rikoksentekijän suojeleminen) liittyy maan- tai valtiopetosrikokseen.

Rikoslain 34 a luvun terrorismirikosten osalta suojelupoliisin tehtävänä on niiden estäminen ja paljastaminen. Terrorismirikosten esitutkinta suoritetaan Poliisihallituksen alaisessa poliisiyksikössä, jonka kanssa suojelupoliisi toimii yhteistyössä ja avustaa tarvittaessa esitutkinnassa. Suojelupoliisi voi erityisestä valtion turvallisuuteen perustuvasta syystä suorittaa terrorismiin liittyvän rikoksen esitutkinnan siten kuin suojelupoliisin ja Poliisihallituksen kanssa on sovittu.

Suojelupoliisi voi käynnistää myös sen tietoon tulleen, valtion johtoon kuuluvaan henkilöön kohdistuvan laittoman uhkauksen tai muun vastaavan rikoksen esitutkinnan, jos teko ilmeisesti liittyy valtakunnan sisäiseen tai ulkoiseen turvallisuuteen ja jos esitutkinnan välitön aloittaminen on tarpeen ennalta estävien turvallisuustoimenpiteiden kiireelliseksi suorittamiseksi. Tutkinta on esitutkinnan jatkuessa siirrettävä viipymättä muulle poliisiyksikölle.

Muut poliisiyksiköt avustavat suojelupoliisia esitutkinnassa Poliisihallituksen kanssa sovittavalla tavalla. Suojelupoliisi avustaa ja toimii yhteistyössä esitutkintaa suorittavan yksikön kanssa myös muiden kuin edellä mainittujen Suomen sisäisen ja ulkoisen turvallisuuden kannalta merkityksellisten rikosten esitutkinnassa. Näitä ovat esimerkiksi rikoslain 11 ja 14 luvuissa mainitut teot.

Suojelupoliisin hallinnollista asemaa, tulosohjausta sekä valvontaa pohtineen työryhmän tuli myös arvioida suojelupoliisin toiminnan kehittämistarpeita tulevien turvallisuusuhkien varalle. Keskeisenä tavoitteena oli selvittää suojelupoliisin toimintaedellytyksiä, toimivaltuuksia ja valvontaa ottaen huomioon kansallinen ja kansainvälinen operatiivinen tilanne sekä turvallisuuspalvelujen kansainväliset kehityssuuntaukset.

Kyseisen työryhmän mukaan suojelupoliisin tiedonhankintaprioriteettien vuosittaista asettamista varten tulisi muodostaa mekanismi, joka toimisi niin, että prioriteettien asettamisen tapahtuisi sisäministeriön johdolla. Ennen prioriteettien vahvistamista ne käsiteltäisiin valmistelevasti ja yhteen sovittavasti valtioneuvoston ulko- ja turvallisuuspoliittisessa ministerivaliokunnassa sekä niistä tulisi antaa selvitys eduskunnan asianomaisille valiokunnille (perustuslakivaliokunta, ulkoasiainvaliokunta ja hallintovaliokunta).

Työryhmä katsoi, että suojelupoliisille olisi harkittava uusia tiedustelullisia toimivaltuuksia, jotta se kykenee vastaamaan toimintaympäristönsä muutokseen. Kyse olisi valtakunnan turvallisuutta vaarantavien hankkeiden torjumiseksi tarpeellisten tietojen hankkimisesta tietolähteinä toimivilta henkilöiltä ja tietoverkoista, vaikka hankkeet eivät olekaan edenneet estettävän, paljastettavan tai selvitettävän rikoksen asteelle. Asiaa harkittaessa on selvitettävä tarkemmin tiedustelutoimivaltuuksien mahdollisen laajentamisen oikeudellisia edellytyksiä muun ohella perus- ja ihmisoikeuksien näkökulmasta.

Tietojen vastaanottamisesta tietolähteinä toimivilta henkilöiltä eli tietolähdetoiminnasta rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi säädetään jo nykyisellään poliisilain 5 luvussa ja tietolähdetoiminnasta rikoksen selvittämiseksi pakkokeinolain 10 luvussa. Poliisilaissa ja pakkokeinolaissa säädettyä salaisen tiedonhankinnan suojaamista voidaan käyttää myös tietolähdetoiminnan yhteydessä. On harkittava tietolähdetoimintaa ja sen suojaamista koskevan sääntelyn ulottamista koskemaan nimenomaisesti myös valtakunnan turvallisuutta vaarantavien hankkeiden torjumista.

Tietolähdetoiminnassa valtakunnan turvallisuutta vaarantavien hankkeiden torjumiseksi tulisi tietoja voida hankkia myös ulkomailta. Ennen kuin tietoja ryhdytään hankkimaan ulkomailta, tulisi Suomen kansallisen lainsäädännön asettamien vaatimusten lisäksi ottaa tapauskohtaisesti huomioon Suomea sitovat kansainväliset velvoitteet ja sen valtion kansallinen lainsäädäntö,

josta tietoja on tarkoitus hankkia. Ulkomailla toimimisen edellytykset sekä toiminnan ohjaus- ja vastuusuhteet tulisi täsmentää mahdollisen kansallisten säännösten jatkovalmistelun yhteydessä. Kun tietojen hankkimiseen ulkomailta voi liittyä myös Suomen kansainvälisiin suhteisiin liittyviä näkökohtia, tällaisesta tiedonhankinnasta olisi ennen siihen ryhtymistä neuvoteltava ainakin suojelupoliisia ohjaavan ministeriön (valtioneuvoston osan) ja ulkoasiainministeriön kanssa.

Työryhmä totesi melko yksiselitteisesti, että mikäli suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, tulisi oikeudenmukaisen oikeudenkäynnin turvaamiseksi harkita suojelupoliisin esitutkintatehtävien ja -toimivaltuuksien rajoittamista. Tällöin suojelupoliisilla olisi myös harkintavaltaa sen suhteen, miten ja missä vaiheessa se ilmoittaa tietoonsa tulleesta rikosepäilystä varsinaiselle esitutkintaviranomaiselle. Suojelupoliisi voisi osallistua edelleenkin tarpeen mukaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa.

Suojelupoliisin hallinnollista asemaa, tulosohjausta sekä valvontaa arvioinut työryhmä arvioi ainoana niin sanottuna uutena toimivaltuutena tietolähdetoiminnan ulottamista ulkomaan tiedusteluun. Kyseisen toimivaltuuslaajennuksen osalta työryhmä päätyi siihen johtopäätökseen, että suojelupoliisin esitutkintatehtäviä ja -toimivaltuuksia tulisi rajoittaa. Tässä esityksessä ehdotetaan säädettäväksi sekä kotimaassa että ulkomailla toteutettavasta siviilitiedustelusta ja siinä käytettävistä tiedustelumenetelmistä, joten on ilmeistä, että suojelupoliisin esitutkintatehtävien ja -toimivaltuuksien rajoittaminen tai kokonaan poistaminen tulee harkittavaksi.

3 Esityksen tavoitteet ja keskeiset ehdotukset

3.1 Tavoitteet

Kansainvälinen turvallisuusympäristö muuttuu nopeasti. Muun muassa hybridivaikuttamisen ja digitalisaation myötä tapahtuneessa toimintaympäristön murroksessa Suomen on kyettävä entistä paremmin hankkimaan ilmiö- ja uhkaperustaista tietoa. Lainsäädäntöä on tarpeen kehittää, jotta pystytään toimimaan muuttuneessa toimintaympäristössä. Nykyisillä rikostorjuntatoimivaltuuksilla ei voida tehokkaasti riittävän varhaisessa vaiheessa havaita yhteiskunnan turvallisuutta vaarantavia uhkia eikä ryhtyä 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. Ehdotettavan lainsäädännön keskeisin tavoite on kansallisen turvallisuuden parantaminen. Tavoitteena on parantaa suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuuteen kohdistuvilta vakavilta uhkilta. Lainsäädännön tavoitteena on edelleen tukea valtion ylimmän johdon päätöksentekoa ja varmistaa sen perustuminen oikeaan, ajantasaiseen ja luotettavaan tietoon. Lainsäädännöllä mahdollistettaisiin myös suojelupoliisin sekä muiden kansallisen turvallisuuden viranomaisten ryhtyminen uhkien torjuntaan aikaisessa vaiheessa ja myös parannettaisiin suojelupoliisin tiedonhankintaa tämän tehtäviin liittyvistä vakavista kansainvälisistä uhista siten, että suojelupoliisilla olisi tosiasialliset mahdollisuudet suoriutua sille säädetystä tehtävästään.

Tiedonhankintalakityöryhmä on mietinnössään ehdottanut, että Suomeen tulisi luoda säädöspohja tietoliikennetiedustelulle, ulkomaan henkilötiedustelulle ja ulkomaantietojärjestelmätiedustelulle. Tämän lisäksi olisi välttämätöntä luoda säädöspohja Suomessa käytettäville tiedustelutoimivaltuuksille samoista syistä kuin ulkomaan tiedustelulle. Vaikka Suomeen kohdistuvat vakavimmat uhkat ovat pääsääntöisesti ulkomaista alkuperää, voi tällainen uhka toteutua myös Suomessa. Uhkan torjumisen mahdollistavan tiedonhankinnan olisi oltava tehokasta uh-

kan läheisyydestä riippumatta. Itsestään selvää lienee, että mitä lähempänä Suomea uhka olisi, sitä perustellumpaa on aloittaa tiedustelutoimenpiteet välittömästi.

Tiedonhankintalakityöryhmän tarkoittamat tiedustelulajit eivät korvaa toisiaan, koska ne ovat luonteeltaan osittain erilaisia. Tietoliikennetiedustelulla on ennen kaikkea tarkoitus havaita toimintaa, joka vakavasti uhkaa kansallista turvallisuutta. Henkilötiedustelulla ja tietojärjestelmätiedustelulla hankittaisiin pääasiassa tietoa tunnistetuista uhista. Tiedustelutoimivaltuuksista muodostuu siten kokonaisuus, johon kuuluu useita eri tiedustelumenetelmiä, jotka täydentävät toisiaan. Kuten kansainvälisestä vertailusta ilmenee, valtioiden tiedusteluviranomaisilla on käytössään samankaltaisia tiedusteluun tarkoitettuja toimivaltuuksia, mistä Suomessa on säädetty ainoastaan rikostorjunnan tarpeisiin. Rikostorjuntatoimivaltuuksilla ei ole mahdollista saada kaikkea kansallisen turvallisuuden kannalta tarpeellista tietoa.

Tämä hallituksen esitys sisältää ehdotuksen siviilitiedustelua koskevaksi lainsäädäntökokonaisuudeksi. Lakiehdotukset on kirjoitettu siten, että niistä ilmenevät riittävän täsmällisesti ja tarkkarajaisesti suojelupoliisin sekä muiden toimijoiden toimivaltuudet, oikeudet ja velvollisuudet. Lakiehdotusten valmistelussa perusoikeuksien suojaan puuttuminen on pyritty rajaamaan niin vähäiseksi kuin toiminnan tehokkuudelle ja tuloksellisuudelle asetettavat vaatimukset huomioon ottaen on mahdollista. Esityksen valmistelussa on kiinnitetty erityistä huomiota Suomea velvoittaviin kansainvälisiin ihmisoikeussopimuksiin sekä Euroopan ihmisoikeussopimuksen ja Euroopan unionin tuomioistuimen ratkaisukäytäntöön.

Tietoliikennetiedustelua koskevan lainsäädännön tavoitteet

Tietoliikennetiedustelun erityispiirteiden vuoksi siitä esitetään säädettäväksi omassa laissaan. Se on tästä huolimatta elimellinen osa siviilitiedustelutoimivaltuuksien laajempaa kokonaisuutta. Kaikkien tiedustelumenetelmien, myös tietoliikennetiedustelun, tarkoituksena on tuottaa välttämätöntä tietoa ylimmän valtiojohdon päätöksenteon tueksi. Lisäksi tiedustelun tarkoituksena on mahdollistaa ajantasaisen turvallisuustilannekuvan muodostaminen, kansallisen turvallisuuden vakaviin uhkatilanteisiin varautuminen ja uhkien torjunta.

Tietoliikennetiedustelun, samoin kuin muidenkin tiedustelumenetelmien, käyttö edellyttäisi aina tosiasiatietoa kansalliseen turvallisuuteen kohdistuvan vakavan uhkan olemassaolosta ja uhkan perustosiseikoista. Uhkan olemassaoloa koskeva tieto olisi voitu saada esimerkiksi kansallisen viranomaisyhteistyön tai kansainvälisen tiedusteluyhteistyön puitteissa.

Siviilitiedustelulainsäädännölle asetettujen kokonaistavoitteiden lisäksi tietoliikennetiedustelulla olisi erityspiirteistään johtuen tärkeä muita tiedustelumenetelmiä täydentävä ja niiden käytön mahdollistava funktio. Sen menetelmällinen erityisluonne mahdollistaa kansalliseen turvallisuuteen kohdistuvien uhkien lähteiden paikantamisen sekä uhkien taustatahojen tunnistamisen. Tietoliikennetiedustelun avulla tehdyt havainnot olisivat monessa tapauksessa välttämätön edellytys sille, että toisenlaiseen kohdentamislogiikkaan perustuvia poliisilain 5 a luvun mukaisia tiedustelumenetelmiä ylipäätään voitaisiin käyttää.

Lainsäädännön erityistavoitteena olisi myös parantaa Suomen kykyä suojautua vakavimpia tietoverkkouhkia vastaan. Tietoverkkouhkien riittävän varhaisessa vaiheessa tapahtuva havaitseminen on niiden estämisen tai ainakin niiden aiheuttamien vahinkoseurausten rajaamisen edellytys. Tietoliikennetiedustelun voidaan arvioida merkittävästi parantavan kykyä havaita erityisesti sellaisia kehittyneiden haittaohjelmien avulla toteutettuja kybertekoja, joiden taustalla ovat valtiotoimijat. Tietoliikennetiedustelun suureen merkitykseen yhteiskunnan kybersuojautumiskyvyn kannalta kiinnitetään huomiota muun muassa Suomen kyberturvallisuuden nykytilaa ja tavoitetilaa kuvaavassa tuoreessa tutkimuksessa (Valtioneuvoston selvitys- ja tut-

kimustoiminnan julkaisusarja 30/2017) ja Norjan niin sanottu Lysne II -komitean loppumietinnössä (Digital Grenseforsvar (DGF)) vuodelta 2016. Tietoliikennetiedustelusta säätäminen täydentäisi näin ollen nykyistä sähköisen viestinnän palveluista annetun lain säännöksiin pohjautuvaa havainnointijärjestelmää erityisesti kaikkein vakavimpien tietoverkkouhkien osalta.

Kansainvälisessä vertailujaksossa käsitellään kuuden Euroopan valtion tiedustelulainsäädäntöä. Kaksi vuotta sitten vertailuvaltioista ainoastaan Ruotsi ja Saksa olivat säätäneet tietoliikennetiedustelusta. Sen jälkeen siitä on säätänyt tai säätämistä on ryhtynyt valmistelemaan kolme muutakin vertailuvaltiota. Vertailuvaltioiden valmisteluasiakirjoissa korostetaan voimakkaasti tietoliikennetiedustelun merkitystä tiedustelumenetelmien muodostamassa kokonaisuudessa.

Tietoliikennetiedustelusta säätämisen voidaan arvioida merkittävästi parantavan esimerkiksi Suomen kykyä estää terrorismia. Kansainvälisenä vertailutietona on syytä mainita, että Ruotsin turvallisuuspoliisi kertoi tammikuussa 2015 estäneensä edeltävän puolentoista vuoden aikana kaksi terrori-iskua signaalitiedustelupalvelulta saamiensa tietoliikennetiedustelutietojen avulla. Asiasta tiedottaminen on poikkeuksellista, sillä tiedustelusta säätäneet maat eivät salassapitosyistä yleensä käsittele julkisuudessa sitä, millä nimenomaisella tiedustelumenetelmällä jotkin tietyt uhkatiedot on hankittu.

Tiedonhankintalakityöryhmä kuuli ulkomaisia asiantuntijoita sen selvittämiseksi, mikä merkitys tietoliikennetiedustelulla on valtiollisen päätöksenteon kannalta. Kuultavat korostivat tietoliikennetiedustelun merkitystä strategisen tiedon hankinnassa valtion ylimmän päätöksenteon pohjaksi. Kuultavien mukaan nykyaikainen ulko- ja turvallisuuspoliittinen päätöksenteko voi perustua vain ajanmukaiseen tiedustelutietoon, johon tietoliikennetiedustelu tuo olennaisen osan (mietinnön s. 69).

Säädettäväksi ehdotettava laki tietoliikennetiedustelusta siviilitiedustelussa perustuu pääministeri Juha Sipilän strategisen hallitusohjelman kirjaukseen, jonka mukaan hallitus esittää säädösperustan luomista tietoliikennetiedustelulle, ja kirjauksen taustalla olleeseen tiedonhankintalakityöryhmän mietintöön. Siltä osin kuin säädösehdotuksessa poiketaan tiedonhankintalakityöryhmän kannanotoista, käsitellään poikkeamisen syy ja luonne jäljempänä keskeisissä ehdotuksissa.

Ehdotettava laki tietoliikennetiedustelusta siviilitiedustelussa on kirjoitettu siten, että siitä täsmällisesti ilmenisivät tietoliikennetiedusteluun osallistuvien tahojen toimivaltuudet, oikeudet ja velvollisuudet. Lakiehdotusta laadittaessa luottamuksellisen viestin suojaan puuttuminen on pyritty rajaamaan niin vähäiseksi kuin toiminnan tehokkuudelle ja tuloksellisuudelle asetettavat vaatimukset huomioon ottaen on mahdollista. Laki sisältäisi useita sellaisia viestintäsalaisuuden suojaamisen tarkoituksessa tietoliikennetiedustelun käytölle asetettuja rajoitteita, joille ei ole vastinetta vertailuvaltioissa. Näistä merkittävin koskisi sitä, että tietoliikennetiedustelussa ei saataisi käyttää viestin sisältöä kuvaavaa hakuehtoa muuten kuin tarkoin rajatuissa poikkeustapauksissa.

Tietoliikennetiedustelun tietoliikenteeseen puuttumisen laajuutta käsitellään muun muassa tietoyhteiskuntavaikutuksia koskevassa osiossa.

3.2 Toteuttamisvaihtoehdot

Rikostorjuntatoimivaltuuksien käyttöalan laajentaminen

Nykyisin Suomessa ei ole tiedustelulainsäädäntöä eikä suojelupoliisille ole säädetty erityisiä toimivaltuuksia tiedon hankkimiseksi toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Suojelupoliisi toteuttaa tehtäväänsä käyttämällä poliisin toimintaa sääntelevissä yleislaeissa olevia toimivaltuuksia.

Rikostorjuntatoimivaltuuksien käyttöalaa olisi mahdollista laajentaa esimerkiksi säätämällä kansallista turvallisuutta vakavasti uhkaava toiminta nykyistä laajemmin rangaistavaksi sekä laajentamalla vastaavasti salaisten tiedonhankintakeinojen käytön erityisinä edellytyksinä olevien perusterikosten alaa.

Harkittaessa tämänlaista vaihtoehtoa on huomioitava, että rikoslainsäädäntöön kohdistuu rajoituksia perustuslaista ja Suomea sitovista kansainvälisistä ihmisoikeusvelvoitteista. Perustuslaissa asetetut rajoitukset johtuvat keskeisimmin perusoikeuksista. Ne asettavat rajoja sille, mitä tekoja voidaan säätää rangaistavaksi ja millaisia rangaistuksia tai muita seuraamuksia rikoksiin voidaan liittää. Kun otetaan huomioon voimassa olevat rikosperusteiset toimivaltuudet, nykyisten tutkintakeinojen tai rikosten estämistä koskevien toimivaltuuksien puute ei siten sinänsä ole peruste säätää joitakin tekoja rangaistavaksi. Kriminalisointitarpeista keskusteltaessa rangaistavaksi säätämisen perusteena toisinaan esiin tuodaan se, että ilman kriminalisointia viranomaisilla ei ole toimivaltuuksia puuttua tiettyyn kielteiseksi arvioitavaan käyttäytymiseen. Tämä näkökohta on tuotu esiin myös siviilitiedustelulainsäädäntöhankkeen yhteydessä. Jotakin tekoa ei kuitenkaan säädetä rangaistavaksi sen vuoksi, että sen estämiseksi tai paljastamiseksi voitaisiin käyttää poliisilain mukaisia salaisia tiedonhankintakeinoja. Jos rikoslainsäädännön käytölle asetettavien yleisten edellytysten ja kriminalisointiperiaatteiden perusteella teon rangaistavaksi säätämiselle on riittävät perusteet, sen estämisessä ja selvittämisessä tarvittavien tiedonhankintakeinojen käytettävissä oleminen on harkittava ja arvioitava erikseen. Mahdollisuus käyttää laajasti poliisilain mukaisia tiedonhankintakeinoja ei ole myöskään rikoksen rangaistusasteikon säätämisessä merkityksellinen peruste (ks. esim. HE 18/2014 vp, s. 13).

Jäljempänä esityksessä käsitellään siviilitiedustelun kohteena toimintaa, joka vakavasti uhkaa kansallista turvallisuutta. Aiemmin esityksessä on myös todettu, että on olemassa sellaisia uhkia, jotka eivät voisi edetä rikokseksi, kuten 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. Näin pitkälle menevät tai väljät kriminalisoinnit olisivat rikosoikeudellisen laillisuusperiaatteen kannalta ongelmallisia. 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). Rikoksen tunnusmerkistö on lisäksi 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). Edellä kerrotut edellytykset saattaisivat muodostaa merkittäviä haasteita tai suoranaisen esteen mainitunlaisen toiminnan kriminalisoinnille.

Tiedustelulakihankkeen aikana on myös tuotu esille, että tietoliikennetiedustelu voitaisiin korvata telekuuntelun ja televalvonnan käyttöalan aineellisen ja alueellisen soveltamisalan laajentamisella.

Tässä esityksessä ehdotetaan, että telekuuntelun ja televalvonnan käytön aineellista ja alueellista soveltamisalaa laajennetaan tiedusteluperusteiseksi, mutta ei kriminalisointien kautta. Li-

säksi tiedustelutoimivaltuuksien käytön alueellinen soveltamisala laajenisi Suomen ulkopuolelle. Tämä ei kuitenkaan poista tarvetta säätää tietoliikennetiedustelusta omana toimivaltuutenaan. Telekuuntelu ja -valvonta eivät menetelminä sovellu rikosten tai uhkien havaitsemiseen ja niiden taustalla olevien henkilöiden tunnistamiseen katsomatta siihen, miten niiden aineellinen tai alueellinen käyttöala on määritelty. Ne eivät menetelminä myöskään sovellu tietoverkkouhkien havaitsemiseen tai niitä koskevaan tiedonhankintaan.

Telekuuntelun ja televalvonnan käyttöalan laajentamista tietoliikennetiedustelusta säätämisen sijasta on perusteltu erityisesti sillä, että ensin mainittu vaihtoehto ei jälkimmäisestä poiketen perustuisi tietoliikenteen suodattamiseen eikä se siten mahdollistaisi viranomaisten pääsyä sellaisten henkilöiden luottamukselliseen viestintään, joilla ei ole yhteyttä vakaviin rikoksiin. Vaikka huomio suomalaisen viranomaistoiminnan osalta pitää paikkansa, ei tästä seuraa, että sivullisen asemassa olevien suomalaisten henkilöiden luottamukselliseen viestintään ei jo nykyisin kohdistuisi tiedustelua. Suomesta on nykyisin meri- ja maakaapeleissa kulkevia tietoliikenneyhteyksiä Ruotsiin, Saksaan, Viroon ja Venäjälle. Tämän mietinnön kansainvälisestä vertailuosuudesta ja kansainvälisen oikeuskäytännön kuvauksesta ilmenee, että edellä mainituista maista ainakin Ruotsi, Saksa ja Venäjä harjoittavat oman valtiorajansa ylittäviin, siis myös Suomesta lähtöisin oleviin, tietoliikenneyhteyksiin kohdistuvaa tiedustelua. Tästä seuraa, että Suomesta lähtevät tietoliikenneyhteydet ja niissä kulkeva suomalaisten luottamuksellinen viestintä ovat jo nyt kattavasti ulkovaltojen harjoittaman tietoliikenteen suodatukseen perustuvan tiedustelun piirissä. Tätä suomalaisten luottamukselliseen viestintään ulottuvaa tiedustelua ei harjoiteta Suomen kansallisen turvallisuuden suojaamiseksi, vaan tiedustelevan valtion omien intressien ja tarkoitusperien mukaisesti.

Edellä sanotun lisäksi rikostorjuntatoimivaltuuksia ei olisi mahdollista käyttää Suomen rajojen ulkopuolella johtuen niiden käytön alueellisesta soveltamisalasta.

Edellä mainituilla perusteilla ei ole tarkoituksenmukaista, että nykyisten rikostorjuntatoimivaltuuksien käyttöalaa laajennettaisiin.

Tiedonhankintalakityöryhmän ehdotus

Tiedonhankintalakityöryhmä ehdotti mietinnössään, että kansallisesta turvallisuudesta vastaaville sotilas- ja siviiliviranomaisille säädettäisiin toimivaltuudet ulkomaan henkilötiedusteluun, ulkomaan tietojärjestelmätiedusteluun ja rajat ylittävään tietoliikenteeseen kohdistettavaan tiedusteluun. Tiedonhankintalakityöryhmän tarkoittama kansallisesta turvallisuudesta vastaava siviiliviranomainen oli suojelupoliisi.

Ulkomaan henkilötiedustelulla tarkoitettiin tiedonhankintalakityöryhmän mietinnössä ulkomaita koskevaa tiedustelua, joka perustuu henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin. Ulkomaan tietojärjestelmätiedustelulla tarkoitettiin puolestaan ulkomailla sijaitsevassa tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin menetelmin tapahtuvaa tiedustelua. Tietoliikennetiedustelulla tiedonhankintalakityöryhmä tarkoitti Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua.

Tiedonhankintalakityöryhmän esittämässä ulkomaan tietojärjestelmätiedustelussa ja ulkomaan henkilötiedustelussa oli kyse ulkomailla tapahtuvasta toiminnasta (ulkomaan tiedustelu).

Sekä tietoliikennetiedustelun että ulkomaantiedustelun tarkoituksena olisi hankkia kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa vakavista kansainvälisistä uhista. Toiminnalla tuettaisiin valtion ylimmän johdon päätöksentekoa ja varmistettaisiin sen perustumi-

nen oikeaan, ajantasaiseen ja luotettavaan tietoon. Toiminnalla myös mahdollistettaisiin toimivaltaisten viranomaisten ryhtyminen uhkien torjuntaan.

Rajapinta tiedustelun ja torjuntatoimien välillä olisi järjestettävä erikseen. Tiedustelun tuottaman tiedon johdosta toimivaltaisen viranomaisen olisi voitava ryhtyä tarvittaviin toimiin uhan torjumiseksi.

Tiedustelua olisi valvottava sekä oikeudellisesti että parlamentaarisesti. Eri tiedustelumenetelmien valvonta olisi aiheellista järjestää mahdollisimman yhdenmukaisesti.

Tiedonhankintalakityöryhmä ehdotti, että siviilitiedustelua koskevat toimivaltuudet valmisteltaisiin sisäministeriössä ja sotilastiedustelua koskevat toimivaltuudet puolustusministeriössä. Koska tietoliikennetiedustelu olisi tarpeen molemmille hallinnonaloille, tulisi harkita, säädettäisiinkö tietoliikennetiedustelusta erillislakina.

Tiedonhankintalakityöryhmä ei kuitenkaan ottanut kantaa, missä sisäministeriön tai puolustusministeriön esittelyvastuulla olevissa laeissa toimivaltuuksista, päätöksenteosta ja tiedustelutoiminnan valvontamekanismeista säädettäisiin, vaan jätti lainsäädäntöratkaisun näiltä osin auki.

Siviilitiedustelulakityöryhmän ehdotus

Tämä hallituksen esitys perustuu pääosin siviilitiedustelulakityöryhmän mietinnön pohjalle.

Siviilitiedustelulakityöryhmä omaksui työssään tiedonhankintalakityöryhmän tekemät keskeiset ratkaisut. Työnsä edetessä siviilitiedustelulakityöryhmä kuitenkin otti toimivaltuustarpeet kokonaisvaltaisemman tarkastelun kohteeksi kuin tiedonhankintalakityöryhmä. Siviilitiedustelulakityöryhmä katsoi perustelluksi, että ulkomaan tiedustelutoimivaltuuksien eli henkilötiedustelun ja tietojärjestelmätiedustelun käyttö mahdollistettaisiin myös kotimassa. Työryhmän näkemyksen mukaan toimivaltuuksien käytön tulisi mahdollistaa riittävän tehokas ja kattava tiedonhankinta vakavimmista kansalliseen turvallisuuteen kohdistuvista uhkista riippumatta uhkan maantieteellisestä sijainnista. Vaikka vakavimmat kansalliseen turvallisuuteen kohdistuvat uhat usein liittyvät Suomen ulkopuolisiin tapahtumiin, saattavat uhan seuraukset realisoitua Suomessa. Tiedustelutoimivaltuuksia voidaan pitää sitä tarpeellisempina, mitä lähempänä uhka sijaitsee Suomea. Tiedustelutoimivaltuuksia voidaan pitää välttämättöminä siinä tilanteessa, kun uhka on siirtynyt Suomen rajojen sisälle. Sotilastiedustelulainsäädäntöä valmistellut työryhmä on päätynyt vastaavaan ratkaisuun.

Siviilitiedustelulakityöryhmässä oli neljä erilaista vaihtoehtoa siviilitiedustelulainsäädäntöä koskevaksi lainsäädäntökehikoksi. Ensimmäisen vaihtoehdon mukaan olisi kaikki siviilitiedustelua koskevat säännökset sisällytetty yhteen lakiin siviilitiedustelusta. Toisen vaihtoehdossa henkilötiedustelusta ja tietojärjestelmätiedustelusta olisi säädetty laissa siviilitiedustelusta ja omassa laissaan tietoliikennetiedustelusta siviilitiedustelussa. Kolmannen vaihtoehdon mukaan kaikki siviilitiedustelua koskevat säännökset olisi sisällytetty poliisilain uuteen 5 a lukuun. Neljännen vaihtoehdon, jonka työryhmä valitsi, mukaan henkilö- ja tietojärjestelmätiedustelusta säädettäisiin poliisilain uudessa 5 a luvussa ja tietoliikennetiedustelusta omassa laissa tietoliikennetiedustelusta siviilitiedustelussa.

Viimeksi mainittu vaihtoehto katsottiin tarkoituksenmukaisimmaksi valinnaksi siviilitiedustelulainsäädännön kehikoksi. Tätä puolsi muun muassa se, että suojelupoliisi on poliisiyksikkö ja tämän toimintaan sovelletaan poliisia koskevia säännöksiä. Poliisilain 1 luvussa säädetään poliisin tehtävästä ja poliisin toimintaa ohjaavista periaatteista, kuten perus- ja ihmisoikeuksi-

en kunnioittamisen periaatteesta, suhteellisuusperiaatteesta, vähimmän haitan periaatteesta ja tarkoitussidonnaisuuden periaatteesta sekä toimenpiteestä luopumisesta ja sen siirtämisestä.

Poliisilain 5 luvussa säädetään suojelupoliisin nykyisin käyttämistä tiedonhankintatoimivaltuuksista, salaisista tiedonhankintakeinoista. Henkilötiedustelu ja tietojärjestelmätiedustelu voidaan jakaa toimivaltuuksiksi, joista kyseisessä poliisilain luvussa säädetään. Henkilötiedustelu jakautuu telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tukiasematietojen hankkimiseen, suunnitelmalliseen tarkkailuun, peiteltyyn tiedonhankintaan, tekniseen tarkkailuun (pois lukien tekninen laitetarkkailu ja osin tekninen kuuntelu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimiseen, peitetoimintaan, valeostoon ja tietolähdetoimintaan. Tekninen laitetarkkailu käsittää tietojärjestelmätiedustelun ja teknisen kuuntelun tietyiltä osilta. Näin ollen kokonaan uusista toimivaltuuksista ei suurelta osin olisi tarpeen säätää. Tarpeellista sitä vastoin olisi säännellä toimivaltuuksien käytön perusteista tiedustelutoimintaan soveltuvalla tavalla.

Asiaa voidaan havainnollistaa voimassa olevien toimivaltuuksien kautta. Poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja saa käyttää rikoksen estämiseksi, paljastamiseksi ja vaaran torjumiseksi, kun taas pakkokeinolain 10 luvussa säädettyjä salaisia pakkokeinoja saa käyttää rikoksen selvittämiseksi. Poliisilain uuteen 5 a lukuun säädettäviä tiedustelumenetelmiä ehdotetaan käytettäväksi tiedon hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Edellä kerrottu huomioon ottaen olisi perusteltua, että 5 a luvun keinot menetelmällisesti perustuisivat poliisilain 5 luvussa säädettyihin salaisiin tietohankintakeinoihin.

Suomen rajat ylittävään tietoliikenteeseen kohdistettavasta tiedustelusta säädettäisiin laissa tietoliikennetiedustelusta siviilitiedustelussa. Tietoliikennetiedustelusta ja poliisilain 5 a luvun toimivaltuuksista käytettäisiin nimitystä tiedustelumenetelmät.

3.3 Keskeiset ehdotukset

Poliisilaki

Poliisilain ehdotetussa uudessa 5 a luvussa säädettäisiin siviilitiedustelun tiedustelumenetelmistä. Siviilitiedustelun määritelmästä säädettäisiin luvun 1 §:ssä. Pykälän mukaan siviilitiedustelulla tarkoitettaisiin suojelupoliisin suorittamaa tiedonhankintaa ja tiedon hyödyntämistä kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi sekä muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten. Kyseessä olisi suojelupoliisille säädettävä uusi tehtävä, joka aiheuttaa tarpeen muuttaa myös lain 1 luvun 1 §:n 1 momentissa säädettyjä poliisin tehtäviä sekä poliisin hallinnosta annetun lain 10 §:ssä säädettyä suojelupoliisin tehtäväsäännöstä.

Suojelupoliisin tehtävää määrittelevät säännökset eivät kuitenkaan itsessään perustaisi suojelupoliisille yleistä toimivaltaa ryhtyä tarpeellisiin toimenpiteisiin kansallisen turvallisuuden suojaamiseksi. Tehtävämäärittelyt olisivat kuitenkin lähtökohtana arvioitaessa suojelupoliisin siviilitiedustelussa käyttämien toimenpiteiden sallittavuutta ja muodostaisivat pohjan uusien toimivaltasäännösten tulkinnalle. Jos suojelupoliisin toimivaltuuksia käytettäisiin suojelupoliisin tehtävämäärittelystä poikkeavaan tarkoitukseen, kysymyksessä saattaa olla oikeudenvastainen harkintavallan väärinkäyttö. Tarkoitussidonnaisuuden periaatteesta säädetään nimenomaisesti lain 1 luvun 5 §:ssä.

Poliisilain uudessa 5 a luvussa säädettäisiin muista siviilitiedustelun tiedustelumenetelmistä (2 §) kuin tietoliikennetiedustelusta, josta säädettäisiin omassa laissaan tietoliikennetiedustelusta siviilitiedustelussa. Uuden 5 a luvun tiedustelumenetelmät perustuisivat menetelmällisesti po-

liisilain 5 luvussa säädettyihin salaisiin tiedonhankintakeinoihin, joiden käytön edellytyksistä säädettäisiin jäljempänä tarkemmin esitetyllä tavalla. Kokonaan uusina toimivaltuuksina ehdotetaan säädettäväksi paikkatiedustelusta, jäljentämisestä, lähetyksen pysäyttämisestä jäljentämistä varten ja tietojen saannista yksityiseltä yhteisöltä (2 §:n 2 momentti) sekä tietoliikennetiedustelusta (2 §:n 3 momentti).

Luvun 3 §:ssä säädettäisiin siviilitiedustelun kohteista, joita olisivat 1) terrorismi; 2) ulkomainen tiedustelutoiminta; 3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö; 4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1992) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö; 5) kansanvaltaista yhteiskuntajärjestystä uhkaava toiminta; 6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta; 7) vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille; 8) kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisi; 10) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta; sekä 11) yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus.

Edellä mainittujen siviilitiedustelun kohteiden eli niin sanottujen perusteuhkien katsottaisiin kuuluvan kansallisen turvallisuuden käsitteen alle pääosin siten kuin Euroopan ihmisoikeustuomioistuin on käsitettä tulkinnut. Kohdeluettelo olisi tyhjentävä ja asettaisi toimivallan käytölle rajat suojelupoliisin toimivaltuuksien käytössä.

Tiedustelumenetelmän käytön edellytyksistä säädettäisiin 4 §:ssä. Pykälän 1 momentissa säädettäisiin kaikkia tiedustelumenetelmiä koskevasta perustelua edellyttävästä tuloksellisuusvaatimuksesta. Tiedustelumenetelmän käytön yleisenä edellytyksenä olisi, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Jokaisen tiedustelumenetelmän käytön kohdalla tulisi voida osoittaa kohdeluettelossa mainitun uhkaperusteen olemassaolo sekä se, että kyseinen uhkaperuste myös muodostaisi vakavan uhkan kansalliselle turvallisuudelle. Näin ollen mikä tahansa siviilitiedustelun kohde ei itsessään muodostaisi vakavaa uhkaa kansalliselle turvallisuudelle.

Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitettaisiin viime kädessä valtion oikeudenkäyttöpiirissä olevien ihmisten kollektiiviseen turvallisuuteen välittömästi tai välillisesti kohdistuvaa väkivaltaista ulkoista uhkaa. 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 ”uhkaa” tarkoitettaisiin tilanteita, joissa kansallinen turvallisuus ei ole välittömästi vaarantumassa. Tiedonhankinta voisi siten koskea myös toimintaa, joka jatkuessaan saattaisi vaarantaa kansallista turvallisuutta. Kansallista turvallisuutta vakavasti uhkaavaa olisi tyypillisesti sellainen yleisvaarallinen ja siihen liittyvä toiminta, joka uhkaa suuren ja ennalta arvaamattoman, sattumanvaraisesti määräytyvän ihmisjoukon henkeä tai terveyttä. Kansallisen turvallisuuden kannalta keskeisiä ovat sellaiset yhteiskunnan perustoiminnot, joiden häirintä tai lamauttaminen saattaisi välillisesti johtaa ihmisten hengen tai terveyden vakavaan vaarantumiseen. Kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitettaisiin myös kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa.

Eräiden tiedustelumenetelmien käytön erityisistä edellytyksistä säädettäisiin 4 §:n 2 momentissa. Kyseisiä tiedustelumenetelmiä saataisiin käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitetusta toimin-

nasta. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että menetelmän käyttö on välttämätöntä. Peitetoiminnan käyttäminen edellyttää myös, että tiedonhankintaa on toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena. Pykälän 3 momentissa säädettäisiin matalammasta käyttökynnyksestä niissä tapauksissa, joissa tiedustelumenetelmän käyttö kohdistetaan valtiolliseen toimijaan tai siihen rinnastuvaan tahoon. Pykälän 4 momentissa säädettäisiin kaikkien tiedustelumenetelmien käyttöä koskevasta rajoituksesta, jonka mukaan tiedustelumenetelmää ei saisi kohdistaa vakituiseen asumiseen käytettävään tilaan. Ainoastaan peitetoiminta ja valeosto olisivat poikkeuksia ja niiden käyttö olisi asunnossa sallittua, jos sisäänkäynti tai oleskelu tapahtuu asuntoa käyttävän aktiivisella myötävaikutuksella. Tämä liittyisi kyseisten tiedustelumenetelmien paljastumisriskiin. Pykälän 5 momentissa säädettäisiin vaatimuksesta, jonka mukaan tiedustelumenetelmän käyttö olisi lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Tällä olisi korostunut merkitys tiedustelumenetelmien käyttöä koskevan lupapäätöksen kuuden kuukauden enimmäisajasta sekä erityisesti vähimmän haitan periaatteesta johtuen.

Luvun 5 §:ssä säädettäisiin tiedonhankinnan jatkamisesta eräiden rikosten estämiseksi ja paljastamiseksi 5 a luvun nojalla annetun luvan tai päätöksen voimassaoloajan. Kyse olisi niin sanotusta suojelupoliisin sisäisestä palomuurista. Suojelupoliisin tehtävänä esitettäisiin olevan jatkossakin poliisilain 5 luvun 3 §:ssä tarkoitettujen rikosten estäminen ja paljastaminen. Näin ollen 44 §:ssä säädettäväksi ehdotetun palomuurisääntelyn perusteella suojelupoliisi tekisi 5 luvun 3 §:ssä olevien rikosten kohdalla ilmoituksen itselleen, jos tiedustelumenetelmän käytön aikana ilmenee, että hankkeilla on pykälässä tarkoitettu maanpetos-, vakoilu- tai terroristisessa tarkoituksessa tehtävä rikos ja se olisi vielä estettävissä.

Uudessa 5 a luvussa säädettäisiin edellä kerrotulla tavalla 5 luvussa säädettyjen keinojen tiedusteluperusteisista käyttöedellytyksistä eikä 5 a luvussa ei olisi siksi tarpeen säätää tiedustelumenetelmien määritelmistä, koska salaiset tiedonhankintakeinot ja tiedustelumenetelmät olisivat menetelmällisesti samoja tiedonhankintakeinoja. Ainoastaan uusien tiedustelumenetelmien, paikkatiedustelun ja jäljentämisen määritelmistä säädettäisiin erikseen 5 a luvussa. Siksi 5 a luvussa säädettäisiin useimpien tiedustelumenetelmien kohdalla ainoastaan päätöksenteosta. Esimerkiksi telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättämisestä säädettäisiin luvun 6 §:ssä. Pykälän 1 momentissa todettaisiin, että tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Pykälän 2 momentin mukaan lupa telekuunteluun tai tietojen hankkimiseen telekuuntelun sijasta voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Silloin, kun toimenpiteen kohteena olisi henkilö, lupa voidaan antaa enintään kolmeksi kuukaudeksi kerrallaan. Pykälän 3 momentissa säädettäisiin mitä telekuuntelua ja telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava. Näitä olisivat 1) 3 §:ssä tarkoitettu toiminta, 2) toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite, 3) tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuvat, 4) telekuuntelua koskevan luvan voimassaoloaika kellonajan tarkkuudella, 5) telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies sekä 6) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

Ensinnäkin telekuuntelulle ja sen sijasta toimitettavalle tietojen hankkimiselle, kuten myös muille tiedustelumenetelmille, säädettäisiin kuuden kuukauden lupa-aika, joka ei kuitenkaan automaattisesti tarkoittaisi sitä, että lupa voitaisiin aina hakea kuudeksi kuukaudeksi tai että se tulisi myöntää kuuden kuukauden määräajaksi. Suhteellisuus- ja vähimmän haitan periaatteen

mukaista harkintaa edellyttäisi säännöksessä oleva ilmaisu "enintään kuudeksi kuukaudeksi kerrallaan".

Toiseksi telekuuntelua koskeva lupa voisi kohdistua henkilöön (2 kohta) teleosoitteen ja telepäätelaitteen sijasta. Kun telekuuntelulupa kohdistettaisiin henkilöön, niin tällöin lupa käsittäisi telekuunteluluvan kohteena olevan henkilön hallussa olevat tai hänen oletettavasti muuten käyttämänsä teleosoitteet tai telepäätelaitteet. Telekuuntelulupa ei siten olisi teleosoite- tai telepäälaitekohtainen. Telekuuntelun kohdistuessa henkilöön lupa-aika voisi olla ainoastaan kolmen kuukauden pituinen.

Telekuuntelua koskevaan vaatimukseen ja päätökseen tulee sisällyttää tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuvat (3 kohta). Tosiseikkojen esittäminen tuomioistuimelle velvoittaisi tiedusteluviranomaisen esittämään ja perustelemaan ne tosiseikat, joiden perusteella tuomioistuin voi tehdä tiedustelumenetelmän käytön edellytysten täyttymisestä omat johtopäätöksensä. Edellytyksissä on kyse ensinnäkin 5 a luvun 4 §:ssä säädettävistä tiedustelumenetelmän käytön yleisistä edellytyksistä. Lisäksi vaatimuksessa ja päätöksessä olisi esitettävä riittävät tosiseikat mistä 3 §:ssä tarkoitetusta siviilitiedustelun kohteena olevasta toiminnasta on kyse. Muiden vaatimukseen ja päätökseen sisällytettävien kohtien osalta sääntely vastaisi pääosin 5 luvussa säädettyä.

Televalvonnasta ja suostumusperäisestä televalvonnasta päättämisestä säädettäisiin 5 a luvun 7 §:ssä ja tukiasematietojen hankkimisesta päättämisestä 7 §:ssä.

Suunnitelmallisesta tarkkailusta päättämisestä säädettäisiin luvun 9 §:ssä. Suunnitelmallinen tarkkailu voitaisiin kohdistaa myös henkilöryhmään, kun rikosperusteisesti käytettävässä suunnitelmallisessa tarkkailussa salaisen tiedonhankintakeinon tai salaisen pakkokeinon kohteena voisi olla ainoataan yksittäinen henkilö. Siviilitiedustelussa voi ilmetä tarve seurata tietyn henkilöryhmän toimintaa, jolloin tiedonhankinnan tarve voi koskea tietyn henkilöryhmän organisaatiota, ryhmään kuuluvia henkilöitä ja henkilöryhmän aktiivisuutta tietyllä alueella.

Myös peitelty tiedonhankinta (10 §) voitaisiin kohdistaa henkilöön tai henkilöryhmään. Kuten muidenkin tiedustelumenetelmien osalta, myös peiteltyä tiedonhankintaa koskevassa päätöksessä tulisi kertoa myös muut tiedonhankinnan taustalla olevat tosiseikat, joiden perusteella ulkopuolisen tarkastelijan olisi mahdollista tehdä tiedustelumenetelmän käytön edellytysten olemassaolosta omat johtopäätöksensä. Peitellystä tiedonhankinnasta päättämisessä säädettäisiin poikkeuksesta laatia päätös kiiretapauksessa kirjallisesti. Päätös olisi kuitenkin laadittava kirjallisesti viipymättä toimenpiteen jälkeen.

Tekninen tarkkailu jaoteltaisiin 5 luvun tavoin tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan (myös henkilön tekninen seuranta) ja tekniseen laitetarkkailuun (11–14 §). Teknisen kuuntelun ja teknisen katselun osalta säädettäisiin niin sanotusta kiirepäätösmenettelystä. Myös teleosoitteen ja telepäätelaitteen yksilöintitietojen hankkimisesta säädettäisiin (15 §) 5 a luvussa. Käytettävien laitteiden ei tulisi olla vastaavalla tavalla Viestintäviraston tarkastamia kuin 5 luvussa. Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimiseen käytettävältä laitteelta ei kuitenkaan edellytettäisi, että laitetta voidaan käyttää vain teleosoitteen ja telepäätelaitteen yksilöimiseen. Kyseinen edellytys tekisi telekuuntelun ja -valvonnan tekemisen erittäin vaikeaksi. Teknisen laitteen lokitietojen tallentamisella tiedusteluvaltuutettu sekä sisäasiainhallinnon voisivat valvoa teknisen laitteen lainmukaista käyttöä.

Laitteen, menetelmän tai ohjelmiston asentamista ja poisottamista (16 §) koskevassa pykälässä säädettäisiin 5 lukuun nähden poikkeavalla tavalla, että (poliisimiehen sijaan) suojelupoliisin

palveluksessa olevalla virkamiehellä olisi oikeus tehdä pykälässä tarkoitetut asennuksen ja poisottamisen, koska poliisimiehellä ei välttämättä kaikissa tilanteissa löydy vaadittavaa teknistä osaamista, mitä laitteen, menetelmän tai ohjelmiston asentamisessa ja poisottamisessa vaaditaan.

Peitetoiminnasta ja valeostosta päättämisestä säädettäisiin 17–22 §:ssä. Luvussa ei kuitenkaan säädettäisi järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun osallistumisesta. Luvun 23 §:ssä säädettäisiin poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa, valeostossa ja tietolähdetoiminnassa. Peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttavan poliisimiehen lisäksi myös tietolähdetoimintaa valmisteleva tai toteuttava poliisimies voitaisiin varustaa kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.

Uuteen 5 a lukuun on tarkoitus ottaa säännökset myös ohjatusta tietolähdetoiminnasta päättämisestä (24 §). Tähän liittyvänä uutena toimivaltuutena olisi tietolähteen turvaaminen (25 §). Tietolähteen turvaamisessa olisi kysymys tietolähteen ennakollisesta ja intensiivisemmästä suojaamisesta.

Luvun 26 §:ssä säädettäisiin paikkatiedustelun määritelmästä. Paikkatiedustelulla tarkoitettaisiin muussa kuin vakituiseen asumiseen käytettävässä tilassa tai sellaisessa tilassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi. Paikkatiedustelusta päättämistä koskevat säännökset olisivat 27 §:ssä. Päätöksentekotoimivalta jakautuisi sen mukaan, kohdistuuko paikkatiedustelu kotirauhan suojaamaan paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana vai ei. Ensiksi mainituissa tapauksissa tuomioistuin päättäisi paikkatiedustelusta tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jälkimmäisessä tapauksessa paikkatiedustelusta päättäisi suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Paikkatiedustelu rinnastettaisiin ilmoittamisen osalta suunnitelmallisen tarkkailuun, peiteltyyn tiedonhankintaan, peitetoimintaan, valeostoon ja tietolähteen ohjattuun käyttöön, joista ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa.

Luvun 28 §:ssä säädettäisiin jäljentämisestä, joka olisi paikkatiedustelun lailla tiedustelumenetelmä. Pykälän mukaan suojelupoliisilla olisi siviilitiedustelussa oikeus jäljentää asiakirja tai muu esine tietojen hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Jäljentämiskielloista (29 §) sekä telekuunteluun, televalvontaan ja tukiasematietoihin liittyvistä jäljentämiskielloista (30 §) säädettäisiin pääosin vastaavalla tavalla mitä paikkatiedustelun päättämistä koskevan pykälän 7 momentissa.

Luvun 31 §:ssä ja 32 §:ssä säädettäisiin lähetyksen jäljentämisestä ja lähetyksen pysäyttämisestä jäljentämistä varten. Menetelmällisesti kyse olisi vastaavista keinoista mitä pakkokeinolain 7 luvussa säädetään. Käyttöperusteeltaan ja -tarkoitukseltaan kyse olisi tässä yhteydessä tiedustelumenetelmistä ja näin ollen salassa suoritettavasta tiedonhankinnasta. Jäljentämisestä päättäisi tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies (33 §:n 1 momentti). Suojelupoliisin poliisimiehellä olisi oikeus tehdä kiirepäätös jäljentämisestä, mutta kiirepäätös tulisi saattaa 1 momentissa tarkoitetun poliisimiehen ratkaistavaksi heti, kun tämä olisi mahdollista (33 §:n 1 momentti). Jäljennös on

hävitettävä viipymättä, jos käy ilmi, että jäljentäminen on kohdistunut jäljentämiskiellon alaiseen materiaaliin tai tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi (34 §).

Poliisilain 5 a luvun 35 §:ssä säädettäisiin menettelystä tuomioistuimessa tiedustelumenetelmää koskevan lupa-asian käsittelyssä.

Siviilitiedustelun suojaamisesta säädettäisiin 5 a luvun 36 §:ssä. Suojaaminen kattaisi koko siviilitiedustelutoiminnan, mutta tietolähteelle tai sivulliselle ei voitaisi luoda uutta identiteettiä. Kovin kevyesti suojausta ei saisi muutoinkaan tehdä siihen liittyvien erilaisten ongelmien ja oikeusturvasyiden johdosta. Suojauksen tekemisen tulee siksi olla välttämätöntä. Suojaamisesta päättämisestä säädettäisiin 37 §:ssä.

Tiedustelumenetelmää käytettäessä on mahdollista joutua tilanteeseen, joissa ulkopuolinen apu on tarpeen tai jopa välttämätöntä. Siksi 38 §:ssä säädettäisiin ilmaisukiellosta. Ilmaisukieltoa koskevasta päätös olisi valituskiellon alainen eikä päätökseen saisi hakea muutosta valittamalla. Kiellon saanut saisi kuitenkin ilman määräaikaa kannella päätöksestä. Kantelu olisi käsiteltävä kiireellisenä. Ilmaisukieltoa koskevasta päätöksestä tulisi aina ilmoittaa tiedusteluvaltuutetulle.

Tiedustelumenetelmän käytöstä päättämisestä muualla kuin Suomessa säädettäisiin 39 §:ssä. Päätöksen, esityksen ja suunnitelman sisällön osalta noudettaisiin mitä tiedustelumenetelmiä koskevissa päätöspykälissä säädettäisiin. Ulkomaan tiedustelussa tulisi siten kirjata samat asiat tiedustelumenetelmää koskevaan päätökseen kuin kotimaan tiedustelussa. Eräitä 5 a luvun säännöksiä voitaisiin soveltaa ulkomaan tiedustelussa. Näitä olisivat 4 §:n 4 momentin, 16 §:n 3 momenttia, 41, 44, 46 ja 47 §:n säännökset.

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua ja teknistä katselua ei saisi 41 §:n 1 momentin mukaan kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16, 20 tai 22 §:n 2 momentin nojalla. Säännöksen nojalla suojaa tietoliikennetiedustelulta nauttisivat tiedot, jotka kuuluvat asianajosalaisuuden, terveydenhuollon ammattihenkilön vaitiolovelvollisuuden, papin rippisalaisuuden ja journalistin lähdesuojan piiriin. Jos kyseisen tiedustelumenetelmän aikana tai muulloin ilmenisi, 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 (2 momentti). Kuuntelu- ja katselukiellot eivät kuitenkaan koskisi tapauksia, joissa 1 momentissa tarkoitettu henkilö osallistuu siviilitiedustelun kohteena olevaan toimintaan, joka vakavasti uhkaa kansallista turvallisuutta ja myös hänen osaltaan on tehty päätös telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, teknisestä kuuntelusta tai teknisestä katselusta (3 momentti).

Tallenteiden ja asiakirjojen tarkastamisesta sekä tallenteiden tutkimisesta säädettäisiin 42 ja 43 §:ssä.

Luvun 44 §:ssä säädettäisiin niin sanotusta palomuurista. Kyse olisi poikkeuksesta tiedustelumenetelmillä saadun tiedon käyttötarkoitussidonnaisuudesta. Asiaa koskeva sääntely on laadittu siten, että siinä tasapainoisella tavalla tulisi huomioitua yhtäältä tiedustelun rikostorjunnasta poikkeava käyttötarkoitus sekä toisaalta vakavien rikosten selvittämiseen ja etenkin sellaisten rikosten estämiseen liittyvä huomattava yhteiskunnallinen intressi. Tiedustelussa ilmitulleiden lievien rikosten ilmoittaminen rikostorjuntaan ei saisi olla sillä tavalla automaattista, että tiedustelu tosiasiassa muodostuu tällaisten rikosten estämisen ja selvittämisen keinoksi. Toisaalta verrattain lieviäkin rikoksia on voitava ilmoittaa rikostorjuntaviranomaisille, jos tämä tapauskohtaisesti on välttämätöntä tiedustelun tarkoituksena olevan kansallisen turvalli-

suuden suojaamiseksi. Kaikkein vakavimpien rikosten selvittäminen ja erityisesti ennalta estäminen puolestaan on yhteiskunnan kokonaisedun mukaista, mistä johtuen niiden ilmoittaminen rikostorjuntaan on syytä laajasti sallia. Ilmoittamista perustelee myös oikeudenmukaisuus ja vakavan rikoksen uhrin näkökulman huomioonottaminen.

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

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

Tiedustelumenetelmällä saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi (45 §:n 1 momentti). Kyse olisi tiedustelumenetelmillä saadun tiedon käyttötarkoitussidonnaisuudesta. Tieto voitaisiin kuitenkin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin, jos tämä on tarpeen edellä palomuurisääntelyssä tarkoitetuissa tapauksissa (45 §:n 2 momentti).

Kiiretilanteessa saadun tiedon hävittämisestä säädettäisiin 46 §:ssä. Jos suojelupoliisin päällystöön kuuluva poliisimies olisi 7 §:n 1 momentissa, 8 §:n 1 momentissa, 11 §:n 1 momentissa, 12 §:n 1 momentissa, 13 §:n 1 momentissa, 14 §:n 1 momentissa tai 27 §:n 2 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, teknisen kuuntelun, teknisen katselun, henkilön teknisen seurannan, teknisen laitetarkkailun tai paikkatiedustelun 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. Pykälässä säädettäisiin myös poikkeuksesta hävittämisvelvollisuuteen. Kiirepäätöksellä saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä. 46 §:n 2 momentissa säädettäisiin erikseen jäljentämisestä tehdystä kiirepäätöksestä, jonka mukaan tietoja saataisiin käyttää vastaavin edellytyksin mitä 1 momentin mukaan.

Tiedustelumenetelmän käytön ilmoittamisesta säädettäisiin 47 §:ssä. Kyseisen ehdotuksen pohjana on käytetty poliisilain 5 luvun 58 §:n sääntelyä. Myös 5 luvun 58 §:n 1 momenttia tarkistettaisiin tässä yhteydessä.

Tiedustelumenetelmän käytön lopettamisen jälkeen olisi laadittava ilman aiheetonta viivytystä pöytäkirja (48 §). Pöytäkirjattavista asioista säädettäisiin tarkemmin valtioneuvoston asetuksella. Asianosaisjulkisuuden rajoittamisesta eräissä tapauksissa säädettäisiin 48 §:ssä.

Suojelupoliisin tietojensaantioikeudesta yksityiseltä yhteisöltä siviilitiedustelussa säädettäisiin 50 §:ssä. Sääntely vastaisi tarkoitukseltaan 4 luvun 3 §:ssä säädettyä, mutta olisi käyttöalaltaan ja perusteiltaan täsmällisemmin ja tarkkarajaisemmin määritelty.

Teleyrityksen avustamisvelvollisuudesta ja pääsystä eräisiin tiloihin sekä teleyrityksen oikeudesta korvauksiin säädettäisiin 51 ja 52 §:ssä vastaavalla tavalla, mitä 5 luvussa.

Luvun 53 §:ssä säädettäisiin sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentissa tarkoitettujen tietojen käyttämisestä kansallisen turvallisuuden suojaamiseksi. Ehdotettavan pykälän mukaan tietoja voitaisiin käyttää myös tiedon saamiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, joka on siviilitiedustelun kohteena (3 §). Kyse ei olisi siten uusien tietojen säilyttämisestä, vaan jo olemassa olevien tietojen hyödyntämisestä paitsi rikoksen selvittämiseksi ja syyteharkintaan saattamiseksi, myös kansallisen turvallisuuden suojaamiseksi. Tallennettujen tietojen määrä ei kasvaisi.

Yhteistyöstä sotilastiedusteluviranomaisen ja muiden viranomaisten kanssa (54 §), yhteistyöstä muiden viranomaisten ja yhteisöjen kanssa (55 §) ja salaisen tiedonhankinnan yhteensovittamisesta (56 §) olisivat omat säännöksensä 5 a luvun loppupuolella.

Myös suojelupoliisin kansainvälisestä yhteistyöstä (57 §) säädettäisiin erikseen. Suojelupoliisi voisi tehdä yhteistyötä sekä toteuttaa tiedonhankintaa yhdessä ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa kansallisen turvallisuuden suojaamiseksi ulkomailla sekä Suomessa. Suojelupoliisin päällikkö päättäisi kansainväliseen yhteistyöhön osallistumisesta ja tiedustelumenetelmien käytöstä yhteistyössä.

Siviili- ja sotilastiedustelutoiminnan yhteensovittamisesta tasavallan presidentin, valtioneuvoston kanslian, ulkoasiainministeriön, puolustusministeriön ja sisäministeriön sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken säädettäisiin 58 §:ssä. Jos siviilitiedustelutoiminnalla arvioitaisiin olevan ulko- ja turvallisuuspoliittisia vaikutuksia, asia on valmistelevasti mainittujen viranomaisten kesken.

Siviilitiedustelun valvontaa koskevat säännökset jakautuisivat siviilitiedustelun valvontaan sisäasiainhallinnossa (59 §) siviilitiedustelun ulkoiseen valvontaan (60 §) sekä tiedusteluvaltuutetulle tehtäviin ilmoituksiin (61 §), joka mahdollistaisi tiedusteluvaltuutetun valvonnan reaaliaikaisuuden suojelupoliisin valtuutetulle tekemien ilmoitusten myötä. Suojelupoliisin olisi annettava tieto tiedusteluvaltuutetulle 5 a luvun nojalla annetuista tuomioistuimen päätöksistä ja luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen (1 momentti). Suojelupoliisin olisi myös mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee: 1) muuta kuin 1 momentissa tarkoitettua tiedustelumenetelmää; 2) siviilitiedustelun suojaamista; 3) ilmaisukieltoa; 4) 44 §:n 1 momentissa tarkoitetun ilmoituksen siirtämistä (2 momentti).

Poliisilakiehdotuksen 5 a luvun lopussa säädettäisiin asetuksenantovaltuudesta (62 §), joka olisi jaettu valtioneuvoston asetuksella säädettäviin ja sisäministeriön asetuksella säädettäviin asioihin.

Laki tietoliikennetiedustelusta siviilitiedustelussa

Tietoliikennetiedustelun kohteet

Laissa säädettäisiin tietoliikennetiedustelun käyttämisestä siviilitiedustelussa. Lain tarkoittaman tietoliikennetiedustelun käyttäjänä olisi siviilitiedusteluviranomaisena toimiva suojelupoliisi.

Kansallista turvallisuutta vakavasti uhkaavat toiminnat, joista suojelupoliisi saisi hankkia tietoa tietoliikennetiedustelulla, olisi tyhjentävästi lueteltu laissa. Tietoliikennetiedustelun perus-

teuhkat olisivat samat kuin poliisilain 5 a luvussa säädettävien tiedustelumenetelmien. Tällä varmistettaisiin se, että siviilitiedustelu olisi toimiva ja tehokas eri tiedustelumenetelmistä koostuva kokonaisuus. Koska tietoliiketiedustelulla saadun tiedon olisi ajateltu toimivan syötteenä poliisilain 5 a luvussa tarkoitettujen tiedustelumenetelmien käytölle, mahdollistaisi perusteuhkien samansisältöisyys sen, että muiden tiedustelumenetelmien käyttöön voitaisiin siirtyä riittävän joustavasti ja riittävässä laajuudessa.

Tietoliikennetiedustelun perusteuhkat olisivat samat kuin poliisilakiehdotuksen 5 a luvun 3 §:ssä.

Tietoliikennetiedustelun yleiskuvaus

Tietoliikennetiedustelulla tarkoitettaisiin lain 2 §:n mukaan Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä. Tietoliikennetiedustelu koskisi näin ollen ainoastaan sellaista tietoliikennettä, joka ylittää valtakunnanrajan siirtymällä suomalaisesta viestintäverkosta ulkomaiseen viestintäverkkoon tai päinvastoin. Merkittävä osa suomalaisesta tietoliikenteestä olisi jo tällä perustavanlaatuisella tasolla rajattu tietoliikennetiedustelun ulkopuolelle.

Tietoliikennetiedustelua käytettäisiin viestintäverkossa rajan ylittävään tietoliikenteeseen. Viestintäverkon määritelmään sisältyisi vaatimus tiedonsiirron sähkömagneettisesta toteutustavasta, mutta muuten se olisi luonteeltaan teknologianeutraali. Koska valtaosa Suomen ja ulkomaiden välisestä tietoliikenteestä välittyy valokuituja tiedonsiirtoon käyttävissä kaapeleissa, kohdistuisi tietoliikennetiedustelu käytännössä pääasiassa kaapelivälitteiseen tietoliikenteeseen. Viestintäverkon käsitteen teknologianeutraalisuudella varmistettaisiin kuitenkin lain soveltuvuus myös muissa teknisissä ympäristöissä ja muuttuvien viestintäteknologioiden olosuhteissa.

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 selvitettävänä olevaan uhkaan liittyvän tietoliikenteen voidaan olettaa kulkevan. Tietoliikenteen suodattamiseen perustuva ratkaisu mahdollistaisi uhkaan liittyvän viestinnän havaitsemisen ja sen taustalla olevien tahojen tunnistamisen ja paikallistamisen. Suodattaminen toteutettaisiin vertailemalla valittua tietoliikennevirtaa hakuehdoiksi kutsuttaviin ennakkoon asetettuihin kriteereihin.

Suodattamisen piirissä ei olisi missään yksittäisessä tietoliikennetiedustelun käyttötapauksessa kaikki se tietoliikenne, joka ylittää Suomen rajan viestintäverkossa. Tietoliikennetiedustelun käyttö edellyttäisi, että suojelupoliisilla olisi tieto tai epäilys jonkin perusteuhkan konkreettisesta olemassaolosta ja sen tosiseikoista. Uhkan kulloinenkin luonne ja uhkasta tiedossa olevat tosiseikat vaikuttavat siihen, missä viestintäverkon osassa uhkaviestinnän voidaan olettaa ylittävän Suomen rajan. Vieraiden valtiotoimijoiden tietoliikenteen esimerkiksi voidaan olettaa ylittävän rajan muissa viestintäverkon osissa kuin sellaisen terroristiseen toimintaan liittyvän viestinvaihdon, jota käydään Suomen ja konfliktialueiden välillä.

Se rajan ylittävä viestintäverkon osa, jossa kulkevaan tietoliikenteeseen hakuehtoja saataisiin käyttää, edellytettäisiin mainittavan tietoliikennetiedustelua koskevassa suojelupoliisin lupavaatimuksessa ja tuomioistuimen lupapäätöksessä. Hakuehtoja ei saataisi käyttää muissa kuin

lupapäätöksessä mainituissa viestintäverkon osissa liikkuvaan tietoliikenteeseen. Se, kuinka laajassa osassa rajan ylittävää viestintäverkkoa hakuehtoja olisi kussakin tapauksessa tarpeen käyttää, riippuisi muun muassa uhkan luonteesta ja uhkan taustalla olevien henkilöiden oletettavasti käyttämistä viestintämenetelmistä.

Laissa säädettäisiin välttämättömistä keinoista saada viestintäverkon osan valintaan vaikuttavat tiedot lupavaatimusta varten. Suojelupoliisille säädettäisiin oikeus antaa tätä koskevia selvittämistoimeksiantoja puolustusvoimien tiedustelulaitokselle. Puolustusvoimien tiedustelulaitoksen selvittämistoiminta perustuisi tietoliikennevirtojen tilastolliseen analysointiin. Tilastoanalyysin laadintaa koskevan toimivaltuuden ja sitä varten tarvittavan lupamenettelyn yksityiskohdista säädettäisiin sotilastiedustelulaissa. Toiseksi viestintäverkon omistajille ja haltijoille säädettäisiin velvollisuus antaa viestintäverkon valinnan kannalta tarpeelliset hallussaan olevat tiedot suojelupoliisille.

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. Kun tietoliikennetiedusteluun olisi saatu tuomioistuimen lupa, tehtäisiin luvanmukaiseen viestintäverkon osaan kytkentä. 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, etteivät tiedusteluviranomaiset saa laajempaa pääsyä tietoliikenteeseen kuin tuomioistuimen lupapäätös sallii.

Suomen Erillisverkot Oy:n tekemän kytkennän kohteena oleva tietoliikenne peilattaisiin virtaamaan puolustusvoimien tiedustelulaitoksen hallinnoiman teknisen tiedustelujärjestelmän läpi. Puolustusvoimien tiedustelulaitos olisi määrätty laissa suojelupoliisin tietoliikennetiedustelun tekniseksi toteuttajaksi. Tietoliikennetiedustelun kohdistumisesta viestintäverkon tietoliikenteeseen käsitellään jäljempänä tarkemmin tietoyhteiskuntavaikutusosiossa.

Tiedustelujärjestelmään olisi ennakkoon syötetty tuomioistuimen lupapäätöksessä hyväksytyt hakuehdot, ja järjestelmä vertaisi läpivirtaavaa tietoliikennettä automatisoidusti niihin. Automatisoitu vertailu olisi reaaliaikaista. Hakuehtoja vastaava liikenne ohjattaisiin syrjään jatkokäsittelyä varten, kun taas hakuehtoja vastaamaton tietoliikenne virtaisi vapaasti järjestelmän läpi. Hakuehtoja vastaamaton liikenne ei olisi läpivirtauksen jälkeen palautettavissa tiedusteluviranomaisten tarkasteltavaksi.

Puolustusvoimien tiedustelulaitos toimittaisi hakuehtoja vastaavan tietoliikenteen suojelupoliisille. Tätä tietoliikennetiedustelun perusteuhkan selvittämisen kannalta lähtökohtaisesti relevanttia tietoliikennettä saataisiin käsitellä automaattisesti ja manuaalisesti. Käsittelyssä suojelupoliisi saisi selvittää yksittäisten luottamuksellisten viestien sisällön ja muut tiedot.

Suojelupoliisin oikeus tallentaa tietoliikennetiedustelun avulla hankittuja tietoja toiminnalliseen tietojärjestelmäänsä samoin kuin tallennettujen tietojen poistaminen ja luovuttaminen tietojärjestelmästä määräytyisivät poliisin henkilötietolain säännösten mukaan. Laki tietoliikennetiedustelusta siviilitiedustelussa sisältäisi kuitenkin joukon henkilötietojen käsittelyä koskevia säännöksiä, jotka tulisivat sovellettaviksi jo ennen tiedon tallentamisen edellytysten arviointia. Säännökset koskisivat tietoliikennetiedustelun käyttöä rajoittavia erityisiä ns. tiedustelukieltoja, tietoliikennetiedustelussa kertyneiden tallenteiden ja asiakirjojen tarkastamista ja tutkimista, velvollisuutta hävittää viipymättä eräät tietoliikennetiedustelulla saadut tiedot ja tietoliikennetiedustelulla saadun tiedon luovuttamista rikostorjuntaan. Laissa ehdotetut tiedus-

telukiellot ja hävittämisvelvollisuudet rajoittaisivat merkittävästi sitä, mitä tietoliikennetiedustelutietoja suojelupoliisin toiminnalliseen tietojärjestelmään saataisiin tallentaa.

Tietoliikennetiedustelussa käytettävät hakuehdot

Nykytilan arvioinnista (teletiedustelumenetelmät alla) ilmenee, että tietoliikennetiedusteluksi luonnehdittavassa toiminnassa tietoliikennettä voidaan suodattaa sekä viestin sisältöä kuvaavien hakuehtojen että viestinnän ja tietoliikenteen muihin tietoihin kohdistuvien hakuehtojen avulla. Viestin sisältöä kuvaavan hakuehdon käytön voidaan katsoa sisältävän syvällisemmän puuttumisen sivullisten luottamukselliseen viestintään, 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.

Hakuehtoja koskeva sääntely sisältyisi lain 4 §:ään. Luottamuksellisen viestin sisältöä kuvaavan hakuehdon käyttö olisi tietoliikennetiedustelussa täysin kielletty. Hakuehtoina ei siten saataisi lainkaan käyttää luottamuksellisen viestin semanttiseen sisältöön kuuluvia ilmaisuja tai henkilöiden nimi- tai muita yksilöintitietoja. Kyse olisi tiedustelutoiminnalle asetetusta merkittävästä rajoituksesta, jonka tarkoituksena olisi mahdollisimman pitkälle turvata sivullisen asemassa olevien henkilöiden viestintäsalaisuuden ydinalue. Tietoliikennetiedustelusta säätäneiden vertailuvaltioiden lainsäädännöissä ei ole asetettu vastaavankaltaisia rajoituksia tai esteitä käyttää sisällöllisiä hakuehtoja, vaan niiden käyttö on kyseisissä maissa laajasti sallittu.

Hakuehtoina sallittuja muita kuin luottamuksellisen viestin semanttista sisältöä kuvaavia tietoja olisivat ennen kaikkea tietoliikenteen ohjaus- ja välitystiedot eli sellaiset tietoverkolle taikka lähettävälle tai vastaanottavalle tietojärjestelmälle tarkoitetut ohjeet, komennot ja muut metatiedot, joilla vaikutetaan viestin kuljetukseen ja ohjaamiseen viestintäverkossa ja tietojärjestelmässä. Hakuehtoina sallittuja tietoja olisivat myös esimerkiksi tiedot jonkin salausohjelman tai aakkosmerkistön käytöstä.

Kaikki viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Tästä johtuen lain 4 §:n 2 momentti sallisi viestin semanttista sisältöä kuvaavan hakuehdon käytön kahdessa poikkeustapauksessa. Sisältöä kuvaavaa hakuehtoa saataisiin ensinnäkin käyttää silloin kun tietoliikennetiedustelu voidaan kohdistaa pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen. 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. Ratkaisu olisi tältä osin sekä teknisesti että asiallisesti sama kuin se, josta säädetään sähköisen viestinnän palveluista annetun lain 272 §:ssä.

Tietoliikennetiedustelussa käytettävät hakuehdot eivät olisi suojelupoliisin vapaasti muodostettavissa, vaan ne olisi ennen toiminnan aloittamista tullut yksilöidä ja hyväksyä tuomioistuimen tietoliikennetiedustelua koskevassa lupapäätöksessä (7 §) tai, poikkeuksellisesti, suojelupoliisin päällikön kiirepäätöksessä (9 §).

Lain 7 §:n mukaan tuomioistuin voisi lupapäätöksessään hyväksyä paitsi yksittäisiä hakuehtoja, myös hakuehtojen luokan. Suojelupoliisin sallittaisiin itse muodostaa tietoliikennetiedustelu-

lussa käytettävät hakuehdot tuomioistuimen hyväksymän hakuehtojen luokan puitteissa. Ehdotus perustuu tiedonhankintalakityöryhmän mietintöön, jonka mukaan tietoliikennetiedustelun suuntaamiseen tulisi voida käyttää ennakkoon määrättyjen hakuehtojen ohella myös "sellaisia kansallista turvallisuutta vaarantavan toiminnan sanallisia kuvailuja, jotka mahdollisimman konkreettisesti luonnehtisivat tiedonhankinnan kohdetta". Sanallisen kuvailun kohteena tulisivat kyseeseen viestinnälliset ja muut toimintamallit, joiden tiedetään tai voidaan olettaa liittyvän kansallista turvallisuutta vaarantavaan toimintaan (s. 64).

Tiedonhankintalakityöryhmän mukaan hakuehtojen luokan hyväksymiseen perustuvan lupamenettelyn voidaan katsoa täyttävän Euroopan ihmisoikeussopimuksen asettamat vaatimukset. Ruotsin ja Sveitsin lainsäädännöissä säädetään hakuehtojen luokkien hyväksymisestä tietoliikennetiedustelun perusteeksi vastaavalla tavalla kuin tässä esitetään. Sveitsin tiedustelulakia laadittaessa on voitu ottaa huomioon Euroopan ihmisoikeustuomioistuimen uusin ratkaisukäytäntö.

Ehdotettavassa laissa hakuehtojen luokalla tarkoitettaisiin tarkkarajaista sanallista kuvausta tiedustelukysymyksen kannalta relevanteista hakuehdoista. Hakuehtojen luokkaan voitaisiin hakea lupaa tilanteessa, jossa samaan selkeään kokonaisuuteen kuuluu joukko keskenään samantyyppisiä hakuehtoja, joista vain osa on tietoliikennetiedustelun käynnistyessä tiedossa.

Koska hakuehtojen luokkaa koskevassa tuomioistuimen lupahyväksynnässä olisi kyse siitä, että suojelupoliisille annettaisiin rajattu oikeus muotoilla tietoliikennetiedustelussa käytettävät konkreettiset hakuehdot itse, olisi toimintaan tarve kohdistaa erityistä valvontaa. Valvonnan kohteena olisi se, että konkreettisten hakuehtojen muodostaminen tapahtuu tuomioistuimen lupapäätöksessä mainitun hakuehtojen luokan puitteissa. Valvontaa koskeva sääntely sisältyisi tähän esitykseen liittyvään oikeusministeriön esitykseen tiedustelutoiminnan valvontaa koskevaksi laiksi (/).

Tietoliikennetiedustelun käytön yleiset edellytykset

Tietoliikennetiedustelun yleisistä edellytyksistä säädettäisiin lain 4 §:ssä. Kaiken tietoliikennetiedustelun edellytyksenä olisi perusteltu toiminnan tuloksellisuus. Pelkkä perusteltu tuloksellisuusodotus soveltuisi silloin, kun tietoliikennetiedustelu voidaan kohdistaa pelkästään valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikenteeseen. Valtiolliseen toimijaan rinnastuvalla taholla tarkoitettaisiin valtionomaisen rakenteen omaavaa toimijaa, joka määrätyllä alueella käyttää omintakeista ja pysyvää valtaa. Pelkän perustellun tuloksellisuusodotuksen soveltaminen perustuisi siihen, että valtiot ja niihin rinnastuvat tahot eivät nauti viestintäsalaisuutta.

Muissa tapauksissa tietoliikennetiedustelun yleisenä edellytyksenä olisi tuloksellisuuden lisäksi välttämättömyys, mikä on korkein poliisin toimivaltuuksia koskevan lainsäädännön tuntema edellytyskynnys. 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 luottamuksellisen viestin salaisuutta.

Tietoliikennetiedustelulle asetettaisiin tiukempi edellytys kuin poliisilain 5 a luvussa säädettäväksi ehdotetuille viestintään kohdistuville tiedustelumenetelmille. Ratkaisun taustalla on Euroopan ihmisoikeustuomioistuimen ratkaisu Szabo & Vissy v. Unkari, jonka mukaan tietoliikennetiedustelun käytön tulisi olla yleisellä tasolla ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi, ja yksittäisen tiedusteluoperaation yhteydessä ehdottoman välttämätöntä olennaisen tärkeän tiedon saamiseksi. Lain 3 §:ssä yksilöidyt tietoliikennetiedustelu-

lun kohteet kohdistuvat demokratiaan ja sen keskeisiin instituutioihin, jolloin tietoliikennetiedustelussa voidaan katsoa olevan kyse demokratian suojelemiseksi välttämättömästä toimivaltuuden käytöstä. Säätämällä tietoliikennetiedustelun edellytykseksi välttämättömyys vastattaisiin vaatimukseen, että tietoliikennetiedustelun käytön tulee olla yksittäistapauksessa ehdottoman välttämätöntä. Ihmisoikeustuomioistuimen "ehdottoman välttämättömyyden" ja kansallisen toimivaltuuslainsäädännön korkeimpana kynnyksenä olevan "välttämättömyyden" välillä on vaikea nähdä mitään ratkaisevaa eroa. Myös Ruotsin ja Sveitsin lainsäädännöissä edellytyskynnykseksi on asetettu välttämättömyys.

Tietoliikennetiedustelun välttämättömyydellä tarkoitettaisiin viimesijaisuutta eli sitä, että tietojen hankkiminen muulla keinolla olisi mahdotonta tai kohtuuttoman vaikeaa. Edellytyksen soveltaminen edellyttäisi sekä tietoliikennetiedusteluun lupaa hakevalta suojelupoliisilta että lupavaatimuksen ratkaisijana olevalta tuomioistuimelta vertailua yhtäältä poliisilain 5 a luvussa tarkoitettujen menetelmien sekä toisaalta tietoliikennetiedustelun välillä. Jos muiden tiedustelumenetelmien käyttö ei olisi mahdotonta tai kohtuuttoman vaikeaa, tulisi niitä käyttää ensisijaisina keinoina suhteessa tietoliikennetiedusteluun. Lain 4 §:n 3 momentissa olisi välttämättömyysvaatimusta täsmentävä ja sitä suhteessa teletiedonhankintakeinoihin entisestään tiukentava säännös, jonka mukaan tietoliikennetiedustelun hakuehtona ei saataisi lainkaan käyttää Suomessa olevan telepäätelaitteen tai teleosoitteen yksilöintitietoa. Jos suojelupoliisilla olisi hallussaan tällainen tieto, se ei saisi ylipäätään käyttää tietoliikennetiedustelua, vaan sen tulisi käyttää telekuuntelua, televalvontaa tai muita poliisilain ehdotetussa 5 a luvussa säädettyjä teletiedonhankintatoimivaltuuksia.

Tietoliikennetiedustelua koskeva päätöksenteko

Euroopan ihmisoikeustuomioistuin on katsonut tärkeäksi oikeusturvatakeeksi sen, että luottamuksellisen viestin suojaan puuttuvista toimenpiteistä päättää tuomioistuin tai muu oikeudellista harkintaa suorittava taho. Muodollisen päätösvallan kuuluminen tuomioistuimelle ei kuitenkaan riitä, vaan kansallisen lain on lisäksi sisällettävä riittävät tuomioistuimen lupaharkintaa ohjaavat kriteerit. Laista on riittävällä tarkkuudella käytävä ilmi ne uhkat, joita koskevaa tiedonhankintaa varten tuomioistuin voi myöntää luvan, ja tiedonhankinnan henkilöllisen kohdentamisen perusteet. Lupahakemuksen esittäjän on perusteltava hakemuksensa ja esitettävä riittävät tiedot sitä tukevista tosiseikoista. Lisäksi tuomioistuimen päätöksistä on käytävä yksiselitteisesti ilmi muun muassa tiedonhankintatoimenpiteen voimassaoloaika.

Tiedonhankintalakityöryhmä katsoi, että tietoliikennetiedustelun lupaharkinnan tulisi olla luonteeltaan oikeudellista. Lisäksi työryhmä totesi, että lupamenettelyn järjestämisessä tulisi ottaa huomioon julkisuus- ja salassapitoseikat, asioiden vaatima erityisosaamisen tarve sekä yksilön oikeusturvan varmistaminen (s. 67). Erityisosaamisen tarpeen huomioon ottamista koskevalla toteamuksellaan työryhmä lienee viitannut mahdollisuuteen perustaa tehtävää varten erityistuomioistuin.

Lain 7 §:n mukaan tietoliikennetiedustelua koskevat lupa-asiat ratkaisisi tuomioistuin suojelupoliisin päällikön kirjallisesta vaatimuksesta. Lain 8 §:n mukaan lupa-asian käsittelemisessä ja ratkaisemisessa tuomioistuimessa noudatettaisiin, mitä poliisilain 5 a luvun 35 §:ssä säädetään tiedustelumenetelmää koskevan lupa-asian käsittelemisestä. Viitatun säännöksen perusteella tietoliikennetiedustelua koskevien asioiden oikeuspaikka olisi Helsingin käräjäoikeus. Koska Helsingin käräjäoikeudella muutenkin on maan laajin kokemus salaisten tiedonhankinta- ja pakkokeinoasioiden käsittelemisestä, voidaan tiedonhankintalakityöryhmän edellyttämä erikoisosaamisen tarve saavuttaa keskittämällä tietoliikennetiedustelua koskevat asiat sille.

LUONNOS

Lain 7 § sisältäisi yksityiskohtaisen luettelon niistä seikoista, joiden olisi käytävä ilmi tietoliikennetiedustelun käyttöä koskevasta suojelupoliisin lupavaatimuksesta ja Helsingin käräjäoikeuden päätöksestä. Luettelon esikuvana ovat päätöksentekoa teletiedonhankintakeinojen käyttöä koskevissa asioissa koskevat poliisilain 5 luvun säännökset. Luettelo sisältää Euroopan ihmisoikeustuomioistuimen edellyttämät riittävät tuomioistuimen lupaharkintaa ohjaavat kriteerit. Lupavaatimuksesta ja -päätöksestä edellytetään käyvän ilmi tietoliikennetiedustelun perusteena oleva kohde ja sitä koskevat tosiseikat sekä ne tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset, esimerkiksi vakava uhka kansalliselle turvallisuudelle ja välttämättömyys, perustuvat. Luvan myöntäminen edellyttäisi, että tuomioistuin suojelupoliisin esittämän aineiston perusteella vakuuttuisi edellä mainituista seikoista.

Lupavaatimuksessa ja -päätöksessä olisi tehtävä selkoa lukuisista muistakin asioista, muun muassa toiminnassa käytettävistä hakuehdoista tai niiden luokista perusteluineen, hakuehtojen käytön piirissä olevasta rajan ylittävän viestintäverkon osasta, luvan tarkasta voimassaoloajasta ja tietoliikennetiedustelun valvonnasta vastaavasta virkamiehestä. Tuomioistuimen olisi mahdollista asettaa päätöksessään tietoliikennetiedustelun käytölle rajoituksia ja ehtoja. Tuomioistuimen päätös asettaisi kaiken kaikkiaan täsmälliset rajat sille, millä tavalla ja missä laajuudessa tietoliikennetiedustelua saataisiin suojelupoliisin toimesta kussakin tapauksessa tehdä.

Tietoliikennetiedustelua varten myönnetyn luvan enimmäisvoimassaoloaika olisi 6 kuukautta. Mietinnön kansainvälistä oikeuskäytäntöä kuvaavasta jaksosta ilmenee, että Euroopan ihmisoikeustuomioistuin on katsonut tuon pituisen voimassaoloajan asianmukaiseksi. Ruotsin ja Sveitsin lainsäädännöissä luvan enimmäisvoimassaoloajaksi on määritelty samoin 6 kuukautta.

Tietoliikennetiedustelun käyttö olisi luvassa mainittuun voimassaoloaikaan katsomatta lopetettava, jos tiedonhankinnan tarkoitus olisi saavutettu tai sen edellytyksiä ei enää olisi.

Niin sanottuihin kiiretilateisiin olisi perusteluta liittää kevennetyn päätöksentekomenettelyn mahdollisuus. Euroopan ihmisoikeustuomioistuin on katsonut, että kansallinen laki voi sisältää erityissäännökset kiiretilanteiden päätöksentekomenettelystä edellyttäen, että laista ilmenee sitä voitavan käyttää vain poikkeuksellisesti ja välttämättömistä syistä. Jos poikkeavasta päätösmenettelystä säädetään, tulee myös säätää normaalin päätöksentekijän mahdollisuudesta jälkikäteen arvioida, oliko menettelyn käyttö perusteltua. Samoin on säädettävä perusteettoman kiirepäätöksen nojalla hankittujen tietojen hävittämisestä.

Kiiretilanteen päätösmenettelystä säädettäisiin edellä mainittujen laatuvaatimusten mukaisesti. Kiiretilanteen päätöksentekijänä olisi 8 §:n mukaan suojelupoliisin päällikkö. Menettely tulisi kyseeseen ainoastaan silloin, kun asia ei siedä viivytystä, eli jos normaalin lupamenettelyn käytöstä aiheutuva viivästys vakavasti vaarantaisi kansallisen turvallisuuden. Kyse voisi olla joko välittömän uhkan tilanteesta tai tilanteesta, jossa luvan hakemisesta aiheutuva viivytys johtaisi tiedustelulla saatavissa olevan aineiston peruuttamattomaan menetykseen.

Suojelupoliisin päällikön tekemä kiirepäätös olisi voimassa vain siihen asti, kunnes tuomioistuin olisi ratkaissut luvan myöntämistä koskevan vaatimuksen. Kiirepäätös olisi saatettava tuomioistuimen arvioitavaksi 24 tunnin kuluessa tietoliikennetiedustelun alkamisesta. Perusteettomaksi osoittautuvan kiirepäätöksen avulla hankittujen tietojen hävittämistä käsitellään jäljempänä tiedustelukieltoja ja hävittämisvelvollisuuksia koskevan osuuden yhteydessä. Käytännössä kiirepäätösten tekeminen tulisi jäämään marginaaliseksi.

LUONNOS

Tietoliikennetiedustelun tekninen toteuttaminen

Tietoliikennetiedustelusta säädettäisiin kahdessa eri toimivaltuuslaissa. Suojelupoliisin oikeudesta käyttää tietoliikennetiedustelua tietojen hankkimiseksi tietoliikennetiedustelun kohteista säädettäisiin laissa tietoliikennetiedustelusta siviilitiedustelussa. Puolustusvoimien oikeudesta käyttää tietoliikennetiedustelua tietojen hankkimiseksi sotilaallisesta ja muusta toiminnasta säädettäisiin sotilastiedustelulaissa.

Kun tietoliikennetiedustelun käyttöön oikeutettuja tahoja olisi kaksi, on toiminta mahdollista organisoida molemmilla hallinnonaloilla erikseen tai vaihtoehtoisesti yhteisesti synergiaetujen saavuttamiseksi. Tiedonhankintalakityöryhmän näkemys oli, että tietoliikennetiedustelun teknisen toteuttamisen tulisi perustua keskitettyyn ratkaisuun, jossa yksi viranomainen suorittaa tietoliikennetiedustelun edellyttämät toimet muiden viranomaisten puolesta (s. 66). Ratkaisua perustelevat ennen kaikkea kustannusnäkökohdat. Resurssinäkökulmasta ei ole järkevää, että suojelupoliisi ja puolustusvoimat samaa toimintoa varten rakentavat omat tekniset järjestelmänsä ja ratkaisunsa. Myös toiminnan yhdenmukaisuudelle asetettavat vaatimukset, toiminnan edellyttämä erikoistuminen ja laillisuusvalvontaan liittyvät näkökohdat perustelevat tietoliikennetiedustelun teknisen toteuttamisen osoittamisen yhden viranomaisen tehtäväksi. Tiedonhankintalakityöryhmä arvioi, että teknisestä toteuttamisesta vastaavaksi viranomaiseksi soveltuisi parhaiten puolustusvoimien tiedustelulaitos (s. 66).

Tietoliikennetiedustelun tekniseksi toteuttajaksi osoitettaisiin edellä sanotun mukaisesti puolustusvoimien tiedustelulaitos. Se vastaisi tiedustelun edellyttämän teknisen kyvyn ja teknisten järjestelmien rakentamisesta ja hallinnoimisesta myös siviilitiedustelun tarpeita varten.

Teknisen toteuttamisen keskeisin sisältö olisi se, että puolustusvoimien tiedustelulaitos suorittaisi tietoliikenteen erottelun suojelupoliisin puolesta. Suojelupoliisin oikeudesta antaa tästä koskevia toimeksiantoja säädettäisiin ehdotettavan lain 10 §:n 3 momentissa. Käytännössä toiminta järjestettäisiin siten, että suojelupoliisi toimittaisi tietoliikennetiedustelua koskevan lupapäätöksen tiedustelulaitokselle. Lupapäätöksestä ilmenisivät muun muassa hakuehdot, joita suodatuksessa saadaan käyttää, ja viestintäverkon osa, jota suodatus saa koskea. Tietoliikennetiedustelun edellyttämästä kytkennästä vastaava Suomen Erillisverkot Oy luovuttaisi luvanmukaisessa viestintäverkon osassa liikkuvan tietoliikenteen puolustusvoimien tiedustelulaitokselle, joka peilaisi sen virtaamaan hallinnoimansa teknisen tiedustelujärjestelmän läpi. Puolustusvoimien tiedustelulaitos olisi ennakkoon syöttänyt tiedustelujärjestelmään lupapäätöksestä ilmenevät hakuehdot. Puolustusvoimien tiedustelulaitos toimittaisi hakuehtojen käytön avulla erotellun tietoliikenteen toimeksiantajana olevalle suojelupoliisille. Erotellun tietoliikenteen jatkokäsittely, josta säädettäisiin lain 5 §:ssä, ei olisi osa tietoliikennetiedustelun teknistä toteuttamista, jolloin sen suorittamisesta ja lainmukaisuudesta vastaisi yksin suojelupoliisi.

Tuomioistuin voisi suojelupoliisille myöntämässään luvassa sallia paitsi hakuehtojen, myös hakuehtojen luokan käytön. Konkreettisten hakuehtojen muodostaminen hakuehtojen luokan määrittämissä puitteissa ei olisi osa teknistä toteuttamista, vaan siitä vastaisi yksin suojelupoliisi. Suojelupoliisi toimittaisi puolustusvoimien tiedustelulaitokselle ainoastaan sellaisia hakuehtoja, jotka se sellaisinaan voi syöttää tiedustelujärjestelmään suodatuksessa käytettäväksi.

Tekninen toteuttaminen pitäisi tietoliikenteen suodattamisen lisäksi sisällään myös eräät sellaiset toimenpiteet, joilla mahdollistettaisiin myöhempi tietoliikennetiedustelu. Niiden tarkoituksena olisi hankkia lupavaatimusta varten tieto siitä, missä viestintäverkon osassa tietoliikennetiedustelua tullaan käyttämään. Viestintäverkon osan ennakollinen yksilöinti on aiheellista, jotta hakuehtojen käytön piiriin ei tulisi tarpeettomasti sivullista tietoliikennettä.

LUONNOS

Lakiehdotuksen 10 §:n 2 momentissa säädettäisiin suojelupoliisin oikeudesta antaa puolustusvoimien tiedustelulaitokselle toimeksiantoja sotilastiedustelulain 66 §:ssä tarkoitettua teknisten tietojen käsittelyä varten. Kyseinen sotilastiedustelulain pykälä sallisi tiedustelulaitoksen hetkellisesti kerätä viestintäverkon tietoliikenteestä viestinnän teknisiä tietoja sekä analysoida niitä tilastollisesti sen selvittämiseksi, missä osassa viestintäverkkoa tiettyyn uhkaavaan toimintaan liittyvä tietoliikenne todennäköisimmin liikkuu. Teknisten tietojen käsittely edellyttäisi sotilastiedustelulain 67 §:n mukaan tuomioistuimen lupaa. Puolustusvoimien tiedustelulaitos hakisi luvan silloinkin, kun kyse on suojelupoliisin toimeksiannosta tapahtuvasta toiminnasta. Teknisten tietojen käsittelyä koskevassa lupavaatimuksessa edellytetään esitettävän eräitä sellaisia luvan toimeenpanoon liittyviä seikkoja, joista paras tieto on toimeenpanijalla eli puolustusvoimien tiedustelulaitoksella.

Tilastollisen analyysin valmistuttua puolustusvoimien tiedustelulaitos toimittaisi sen tuloksen suojelupoliisille. Tilastollisen analyysin tulos ei sisältäisi viestintäsalaisuuden piiriin kuuluvaa tietoa. Tuloksen perusteella suojelupoliisi voisi arvioida, mitä viestintäverkon osaa varten sen tulisi hakea lupaa tietoliikennetiedusteluun tuomioistuimelta.

Viestintäverkon osan tunnistaminen lupahakemusta varten edellyttäisi useimmin paitsi puolustusvoimien tiedustelulaitoksen edellä kuvattuja toimenpiteitä myös sitä, että suojelupoliisi saisi viestintäverkon omistajina ja haltijoina olevilta yrityksiltä eräät niiden hallussa olevat tiedot. Yritysten tietojenantovelvollisuutta käsitellään jäljempänä.

Tiedustelukiellot ja hävittämisvelvollisuudet

Tietoliikennetiedustelun muista tiedustelumenetelmistä poikkeavan luonteen vuoksi laissa säädettäisiin erityisistä kielloista kohdistaa tietoliikennetiedustelua tietyn tyyppisiin viesteihin ja tietoihin. Kohdistamiskiellosta huolimatta tietoliikennetiedustelussa saattaa nousta esiin tiedustelukiellon piiriin kuuluvia viestejä ja tietoja. Tiedustelukieltoa vahvistettaisiin tästä johtuen säätämällä suojelupoliisin velvollisuudesta hävittää kiellon piiriin kuuluvat viestit ja tiedot viipymättä, kun niiden luonne on käynyt ilmi. Velvollisuus viipymättä hävittämiseen koskisi myös eräitä muita kuin tiedustelukiellon alaisia viestejä ja tietoja.

Lakiehdotuksessa säädettävät tiedustelukiellot perustuisivat pääosin tiedonhankintalakityöryhmän ehdotuksiin. Työryhmän mietinnön mukaan tietoliikennetiedustelulla ei olisi tarkoitus seurata Suomessa oleskelevien osapuolten välistä tietoliikennettä eikä sellaista Suomesta tapahtuvaa ulkomailla olevaan pilvipalveluun tallentamista, johon ei sisälly viestintää. Tietoliikennetiedustelusta mahdollisesti säädettäessä tulisi riittävästi varmistaa, että tällainen tieto hävitettäisiin välittömästi, kun se havaittaisiin (s. 68).

Ehdotettavassa laissa säädettäisiin kotimaista viestintää koskevasta, mutta ei erillisestä pilvipalveluihin tallentamiseen liittyvästä tiedustelukiellosta ja hävittämisvelvollisuudesta. Syitä tiedonhankintalakityöryhmän kannanotosta eroavaan ratkaisuun käsitellään tämän osuuden päätteeksi.

Kotimaista viestintää koskeva tiedustelukielto ilmenisi lakiehdotuksen 12 §:stä, jonka mukaan tietoliikennetiedustelua ei saisi kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa. Tietoliikennetiedustelua ei käytettäisi Suomen sisäisessä viestintäverkossa vaan ainoastaan rajan ylittävässä viestintäverkossa tiedon hankkimiseksi ulkoisista uhkista. Kotimaassa olevien osapuolten välinen viestintä usein reitittyy lähettäjältä vastaanottajalle rajan ylittävän viestintäverkon kautta. Tiedustelukiellosta esitetään säädettäväksi siksi, että kaiken kotimaiseksi tarkoitetun viestinnän tulisi olla samassa asemassa katsomatta siihen, kuinka tuo viestintä sattumanvaraisten tekijöiden vuoksi reitittyy.

Lakiehdotuksen 12 §:n mukaan tiedustelua ei myöskään saisi kohdistaa tietoon, josta viestinnän jommallakummalla osapuolella tai tiedon tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla. Säännöksen nojalla suojaa tietoliikennetiedustelulta nauttisivat tiedot, jotka kuuluvat asianajosalaisuuden, terveydenhuollon ammattihenkilön vaitiolovelvollisuuden, papin rippisalaisuuden ja journalistin lähdesuojan piiriin. Tiedustelukielto ei koskisi oikeudenkäymiskaaressa tarkoitettujen ammattihenkilöiden viestiyhteyksiä yleensä, vaan ainoastaan niitä nimenomaisia tietoja, joista henkilöillä oikeudenkäymiskaaren asianomaisten säännösten mukaan on velvollisuus tai oikeus olla todistamatta.

Tiedustelukieltojen noudattaminen siten, että tietoliikenteestä ei lainkaan kerättäisi kieltojen piiriin kuuluvia tietoja, ei ole teknisesti mahdollista. Tietoliikennetiedustelun hakuehtoja ei yleensä voida muodostaa siten, että ne tunnistaisivat tiedustelukiellon alaisen viestin tai tiedon ja estäisivät sen pääsyn jatkokäsittelyyn ohjautuvaan aineistoon. Lain 15 §:ssä säädettäisiin tästä johtuen suojelupoliisin velvollisuudesta hävittää tiedustelukiellon alaiset viestit ja tiedot viipymättä, kun niiden luonne on käynyt ilmi. Hävittämisvelvollisuus olisi ehdoton eikä siitä olisi säädetty poikkeuksia. Hävittämisvelvollisuudesta seuraisi myös ehdoton kielto hyödyntää tai käyttää tällaisia viestejä tai tietoja mitään tarkoitusta varten.

Lakiehdotuksen 15 §:n säädettäisiin lisäksi suojelupoliisin velvollisuudesta hävittää viipymättä kaikki sellaiset tietoliikennetiedustelulla saadut tiedot, joilla ei ole merkitystä kansallisen turvallisuuden suojaamiseksi. Velvollisuus kansallisen turvallisuuden suojaamisen kannalta epäolennaisten tietojen hävittämiseen ei kuitenkaan olisi yhtä absoluuttinen kuin velvollisuus tiedustelukiellon alaisten viestien ja tietojen hävittämiseen, vaan ne saataisiin erikseen säädetyin edellytyksin luovuttaa rikostorjuntaan sekä tallettaa poliisin henkilörekistereihin. Esimerkiksi tallettamistoimivalta olisi olemassa ainoastaan silloin, kun tiedot olisivat tarpeen sellaisen rikoksen, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, selvittämistä tai estämistä varten taikka syyttömyyttä tukevana selvityksenä.

Hävittämisvelvollisuuksien toteutumista tuettaisiin säätämällä velvollisuudesta tarkastaa tietoliikennetiedustelun käytössä kertyneet tallenteet ilman aiheetonta viivytystä (13 §). Tallenteita saisivat tutkia ainoastaan laissa nimetyt tai erikseen tähän tehtävään määrätyt tai osoitetut virkamiehet tai muut tahot (14 §).

Perusteettoman tai virheellisen kiirepäätöksen avulla hankittujen tietojen hävittämistä koskisi erityssääntely, jota laadittaessa on huomioitu Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntö. Lakiehdotuksen 9 §:n 2 momentin mukaan, jos tuomioistuin arvioidessaan kiirepäätöstä katsoisi, että tietoliikennetiedustelulle säädetty perusteltu tuloksellisuus- ja välttämättömyysedellytys ei ole täyttynyt, olisi tietoliikennetiedustelulla saatu aineisto kokonaisuudessaan heti hävitettävä. Jos tuomioistuin katsoisi kiirepäätöksen joltain vähäisemmältä osin virheelliseksi, olisi tiedot hävitettävä siinä laajuudessa kuin tuomioistuimen päätös edellyttää. Vähäisempi virheellisyys voisi koskea esimerkiksi jotain väärin muodostettua hakuehtoa, jonka käytön avulla hankitut tiedot näin muodoin tulisi hävittää. Perusteettomalla tai virheellisellä kiirepäätöksellä hankittujen tietojen hävittämisestä saataisiin poiketa vain siinä tapauksessa, että tiedot olisivat tarpeen sellaisen rikoksen, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, selvittämistä tai estämistä varten taikka syyttömyyttä tukevana selvityksenä. Tällaisten tietojen tallentamiseen ja käyttöön voidaan katsoa olevan erityisen painava yhteiskunnallinen intressi.

Tiedonhankintalakityöryhmä esitti mietinnössään, että tiedustelukiellon ja hävittämisvelvollisuuden tulisi koskea sellaista Suomesta ulkomaille tapahtuvaa pilvipalveluun tallentamista, johon ei sisälly viestintää. Kannanottoa ei perustella mietinnössä eikä sen motiivi ole tiedossa.

Tällaisesta tiedustelukiellosta ei ole säädetty minkään muun tässä esityksessä käsitellyn vertailuvaltion lainsäädännössä eikä sellaista ehdoteta otettavan Suomenkaan lainsäädäntöön.

Tietoliikennetiedustelun keskeisenä käyttötarkoituksena on havaita kansalliseen turvallisuuteen kohdistuvia vakavia uhkia ja tunnistaa niiden taustalla olevia henkilöitä. Pilvipalveluun tallentamiseen kohdistettavalla tietoliikennetiedustelulla on samankaltainen merkitys kuin muullakin tietoliikennetiedustelulla tämän tarkoituksen toteutumisen kannalta. Pilvipalveluihin tallentamista käytetään tosiasiassa laajasti hyväksi erilaisessa terrorismiin ja vakoiluun liittyvässä toiminnassa.

Tietoliikennetiedustelun käyttö on tarpeen esimerkiksi tilanteessa, jossa tiedetään terrori-iskun suunnittelun ja valmistelun tapahtuvan pilvipalveluun luodussa rajatussa ryhmätyötilassa, mutta valmisteluun osallistuvat henkilöt ovat tuntemattomia. Ryhmätyötilaan Suomesta tapahtuva liikenne voidaan havaita ja sen taustalla olevat henkilöt tunnistaa tietoliikennetiedustelun avulla käyttäen ryhmätyötilan sijaintia hakuehtona. Valtiollinen kybervakoilu toteutetaan yleensä siten, että vakoilussa käytettävä haittaohjelma tallentaa anastamansa tiedot ulkomailla sijaitsevaan pilveen. Jos pilvipalveluliikenteeseen liitettäisiin tiedustelukielto ja hävittämisvelvollisuus, ei tietoliikennetiedustelua voitaisi käyttää tällaisen toiminnan havaitsemiseen ja estämiseen.

Pilvipalveluihin tallentamiseen liittyvää tiedustelukieltoa vastaan puhuvat myös muut seikat, ennen kaikkea tiedustelukiellon alan järkevän rajaamisen ja täsmällisen määrittelemisen mahdottomuus. Tiedustelukiellosta säätäminen edellyttäisi pilvipalveluun tallentamisen määrittelemistä. Määritelmä voitaisiin periaatteessa laatia joko teknologialähtöisesti tai vaihtoehtoisesti pilvipalveluun tallentamisen toiminnalliseen luonteeseen perustuen. Ensimmäinen vaihtoehto olisi ristiriidassa laissa muuten omaksutun teknologianeutraalisuutta painottavan lähtökohdan kanssa. Tieto- ja viestintätekniikan alati kiihtyvän kehityksen johdosta on myös todennäköistä, että teknologialähtöinen pilvipalveluun tallentamisen määritelmä hyvin nopeasti vanhenisi, jolloin siihen sidottu tiedustelukielto menettäisi merkityksensä.

Toiminnan luonteeseen tukeutuva teknologianeutraali määritelmä taas olisi epätäsmällinen ja epätarkoituksenmukainen. Pilvipalveluun tallentamisessa on kyse datan tallentamisesta verkon yli palvelimelle. Tällainen määritelmä kattaisi datan varmuuskopioinnin ohella esimerkiksi suuren osan www-palvelun päivityksistä ja sosiaalisen median palveluiden käytöstä, joihin kohdistuvalla tiedustelulla voi tapauskohtaisesti olla suuri merkitys kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitsemiseksi. Toiminnan luonteeseen perustuvaan määritelmään sidottua tiedustelukieltoa olisi myös vaikea soveltaa käytännössä, koska se edellyttäisi jokaisen tietoliikennetapahtuman teknistä analysointia sen selvittämiseksi, onko tapahtumassa ollut kyse määritelmänmukaisesta verkon yli tapahtuvasta tiedon tallentamisesta. Ei myöskään ole asiallista perustetta sille, että sellaista esimerkiksi sosiaalisen median käyttöä, joka perustuu verkon yli tapahtuvaan datan tallentamiseen, kohdeltaisiin muusta sosiaalisen median käytöstä poikkeavasti.

Tiedonhankintalakityöryhmän ehdotuksen mukaan viestintää sisältävä pilvipalveluun tallentaminen ei olisi kuulunut työryhmän esittämän tiedustelukiellon piiriin. Koska tällaisen toiminnan erottaminen muusta pilvipalveluun tallentamisesta lienee monessa tapauksessa mahdotonta, seuraisi kiellosta ja siitä tehtävästä poikkeuksesta säätämisestä, että kiellon ala muodostuisi epämääräiseksi. Esimerkkinä viestintää sisältävästä pilvipalveluliikenteestä voidaan mainita tilanne, jossa Suomessa oleva henkilö tallentaa ulkomailla olevaan pilveen asiakirjan, jonka ulkomailla oleva henkilö käy sieltä myöhemmässä vaiheessa lukemassa. Koska jälkimmäinen ulkomailta ulkomaille tapahtuva tietoliikennetapahtuma kuitenkaan ei ylitä Suomen rajaa viestintäverkossa, ei siitä voida saada havaintoa tietoliikennetiedustelussa. Tällöin jää

pysyvästi epäselväksi, onko pilvipalveluun tallentaminen sisältänyt viestintää vai ei, ja soveltuuko tiedustelukielto vai ei. Mahdollisen tiedustelukiellon soveltumiseen liittyvillä epävarmuustekijöillä voitaisiin arvioida olevan oikeusvarmuutta heikentävä vaikutus.

Edellä sanotusta johtuen on perusteltua, että tietoliikennetiedustelua saadaan kohdistaa pilvipalveluihin tallentamiseen samojen reunaehtojen puitteissa kuin muuhunkin tietoliikenteeseen. Pilvipalveluun tallentamista koskevaa hakuehtoa saataisiin käyttää, jos tuomioistuin hyväksyisi sen käytön 7 §:ssä tarkoitetussa päätöksessään. Pilvipalveluun tallentamista koskevan hakuehdon käytön tulisi aina perustua johonkin riittävän konkreettiseen tietoliikennetiedustelun kohteena olevaan kansallista turvallisuutta vakavasti uhkaavaan toimintaan, jota koskevat tosiseikat suojelupoliisi olisi velvoitettu antamaan tuomioistuimelle esittämässään lupavaatimuksessa. Jos pilvipalveluun tallentamista koskevan hakuehdon käyttöä ei voitaisi kohdistaa pelkästään vieraan valtion tietoliikenteeseen vaan suodattamisen piiriin saattaisi tulla muutakin tietoliikennettä, olisi hakuehdon käytön edellytyksenä 6 §:n 2 momentin mukaisesti välttämättömyys.

Pilvipalveluun tallentamista koskevana hakuehtona voisi lähinnä tulla kyseeseen pilvipalvelun sijaintipaikkaa kuvaava tieto. Sen sijaan hakuehtona ei tässäkään tapauksessa voitaisi käyttää Suomessa olevan henkilön teleosoitteen tai telepäätelaitteen yksilöintitietoa, koska lain 4 §:n 3 momentti nimenomaisesti kieltäisi sen. Tietoliikennetiedustelun avulla ei näin ollen voitaisi hankkia tietoa siitä, mitä kaikkea dataa yksittäisestä tiedossa olevasta laitteesta on ulkomailla olevaan pilvipalveluun tallennettu.

Pilvipalveluun tallentamiseen nimenomaisesti kohdistettavan tietoliikennetiedustelun sallimisesta osittain erillinen kysymys on se, voiko ja missä laajuudessa sivullisten henkilöiden pilvipalvelukäyttöön liittyvää tietoliikennettä suodattua 5 §:ssä tarkoitettuun jatkokäsittelyyn silloin kun suodatuksessa käytettävät hakuehdot eivät millään tavalla liity pilvipalveluliikenteeseen. Konkreettisemmin voidaan esimerkiksi kysyä, kuinka todennäköistä on, että mobiililaitteen varmuuskopiointiin liittyvä sivullinen tietoliikenne vastaa jonkin terroristisen uhkan selvittämisessä käytettävää ohjaus- ja välitystietoihin perustuvaa hakuehtoa. Arvion mukaan sivullinen pilvipalveluliikenne voi vastata tietoliikennetiedustelussa käytettäviä hakuehtoja vain varsin poikkeuksellisesti. Riskiä pienentää valittu sääntelymalli, jossa tietoliikennetiedustelun hakuehdot eivät voisi kuvata viestin sisältöä.

Sikäli kuin sivullista pilvipalveluliikennettä kuitenkin ohjautuu jatkokäsittelyyn, sovellettaisiin siihen samoja tietojen viipymättä hävittämistä koskevia säännöksiä kuin muuhunkin tietoliikenteeseen. Lakiehdotuksen 13 §:ssä säädettäisiin suojelupoliisin velvollisuudesta ilman aiheetonta viivästystä tarkastaa tietoliikennetiedustelun käytössä kertyneet tallenteet. Jos tallenteiden tarkastamisessa tai 14 §:ssä tarkoitetussa tallenteiden tutkimisessa havaittaisiin kansallisen turvallisuuden suojaamisen kannalta vailla merkitystä olevaa tietoa, tulisi se 15 § mukaan viipymättä hävittää. Lisäksi, jos pilvipalveluun tallentamiseen liittyvä tieto kuuluisi esimerkiksi asianajosalaisuuden tai lähdesuojan piiriin, olisi se hävitettävä viipymättä katsomatta siihen, onko se ollut kansallisen turvallisuuden suojaamisen kannalta merkityksellistä vai ei.

Yksityisten yritysten velvollisuudet

Suomen rajan ylittävä viestintäverkko on yksityisessä omistuksessa. Tietoliikennetiedustelun käytännön toteuttaminen edellyttää tästä johtuen, että viestintäverkon omistajille säädetään riittävä velvollisuus myötävaikuttaa tietoliikennetiedustelun toteuttamiseen. Tiedustelua ei esimerkiksi voida toteuttaa ilman, että viestintäverkossa kulkeva tietoliikenne saadaan ohjattua yksityisen hallusta puolustusvoimien tiedustelulaitoksen hallinnoiman tiedustelujärjestelmän läpi.

Velvollisuuksien kohteena olevista tahoista käytettäisiin laissa käsitettä tiedonsiirtäjä. Tiedonsiirtäjällä tarkoitettaisiin lain 2 §:n mukaan tahoa, joka omistaa tai hallitsee viestintäverkon sitä osaa, joka ylittää Suomen rajan. Laissa ei osoitettaisi velvoitteita muille yksityisille kuin tiedonsiirtäjille. On syytä korostaa, että laki ei asettaisi yrityksille velvollisuutta luovuttaa salausavaimia suojelupoliisille tai asentaa ns. takaportteja ohjelmistoihinsa tai laitteistoihinsa suojelupoliisin tarpeita varten. Sellaisia velvoitteita ei asetettaisi myöskään sotilastiedustelulaissa, joka sisältää tietoliikennetiedustelun teknistä toteuttamista koskevia täydentäviä säännöksiä.

Tiedonsiirtäjälle tässä laissa ja sotilastiedustelulaissa säädettävät velvollisuudet olisivat kahdenlaatuisia. Ensinnäkin tiedonsiirtäjällä olisi velvollisuus myötävaikuttaa tietoliikennetiedustelun edellyttämän liitynnän rakentamiseen omistamaansa tai hallitsemaansa viestintäverkon rajan ylittävään osaan. Liitynnän olemassaolo on edellytys sille, että Suomen Erillisverkot Oy voisi tehdä tuomioistuimen luvan mukaisen kytkennän ja ohjata luvan tarkoittaman tietoliikenteen puolustusvoimien tiedustelulaitokselle hakuehtojen käyttöä varten. Velvollisuus myötävaikuttaa liitynnän rakentamiseen liittyy läheisesti tietoliikennetiedustelun tekniseen toteuttamiseen, mistä johtuen siitä säädettäisiin sotilastiedustelulaissa.

Edellä mainitun myötävaikutusvelvollisuuden lisäksi viestintäverkon omistajille ja haltijoille säädettäisiin velvollisuus antaa suojelupoliisille eräät sellaiset tiedot, jotka ovat välttämättömiä tuomioistuimelle esitettävää lupavaatimusta varten. Lakiehdotuksen 7 §:n mukaan lupavaatimuksessa olisi esitettävä tieto siitä rajan ylittävän viestintäverkon osasta, jossa tietoliikennetiedustelua tehtäisiin, sekä perustelut viestintäverkon osan valinnalle. Viestintäverkon osan yksilöinti lupavaatimuksessa ja -päätöksessä on perusteltua, jotta tietoliikennetiedustelun hakuehtoperusteista vertailua ei voitaisi kohdistaa tietoliikenteeseen laajemmin kuin on välttämätöntä tietoliikennetiedustelun kohteena olevan kansallista turvallisuutta vakavasti uhkaavan toiminnan selvittämiseksi. Lain 22 § velvoittaisi näin ollen tiedonsiirtäjät antamaan suojelupoliisille viestintäverkon osan valinnan kannalta tarpeelliset hallussaan olevat tiedot. Tällaiset tiedot koskisivat ennen kaikkea tiedonsiirtäjältä tehtyjä siirtokapasiteetin varauksia, mutta myös muita seikkoja, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen viestintäverkon rajan ylittävässä osassa. Sen sijaan pykälä ei perustaisi tiedonsiirtäjillä velvollisuutta antaa suojelupoliisille tietoa yksittäisistä viestintätapahtumista tai tällaisten tapahtumien osapuolista.

Tiedonsiirtäjien tiedonantovelvollisuus palvelisi samaa tarkoitusta kuin puolustusvoimien tiedustelulaitoksen suojelupoliisin puolesta suorittama teknisten tietojen käsittely. Se, kummalla menetelmällä tai millaisella menetelmien yhdistelmällä tietoliikennetiedustelun kannalta relevantti viestintäverkon osa tunnistettaisiin lupavaatimusta varten, vaihtelisi tapauskohtaisesti. Tavoitteena molemmissa olisi minimoida sivullisen tietoliikenteen tuleminen tietoliikennetiedustelun piiriin.

Tiedonsiirtäjällä olisi lain 23 §:n mukaan oikeus saada korvaus tietojen antamisesta sille aiheutuneista välittömistä kustannuksista. Oikeus korvaukseen, jonka maksamisesta päättäisi suojelupoliisi, olisi laajempi kuin perinteisten teletiedonhankintakeinojen osalta, sillä välittöminä kustannuksina korvattavaksi tulisivat myös henkilöstökustannukset.

Tietoliikennetiedustelusta ilmoittaminen

Tietoliikennetiedustelusta ilmoittamista koskevan sääntelyn laadinnassa on huomioitu Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntö. Ihmisoikeustuomioistuin on korostanut tiedonhankinnan kohdehenkilön oikeutta tehokkaisiin oikeusturvakeinoihin lainvastaista viranomaistiedonhankintaa vastaan. Oikeusturvakeinojen käytön edellytyksenä on yleensä, että

henkilö saa tiedon hänen oikeuksiaan mahdollisesti loukkaavasta viranomaisten toiminnasta. Viranomaisella tulisi näin ollen olla velvollisuus oma-aloitteisesti ilmoittaa henkilölle tähän kohdistetusta tiedonhankinnasta sitten kun yksilöllinen este ilmoittamiselle on poistunut. Jos oikeus kannella viranomaisen tiedonhankinnasta kuitenkin on kansallisesti säädetty sillä tavalla yleiseksi, että kuka hyvänsä voi kannella viranomaisten toiminnasta pelkän yksilöimättömän lainvastaisuutta koskevan epäilyn perusteella, on velvollisuus ilmoittamiseen voitu säätää rajatummaksi.

Suojelupoliisin velvollisuus ilmoittaa kohdehenkilölle tietoliikennetiedustelusta olisi tässä laissa säädetty verrattain rajatuksi. Tätä kompensoitaisiin säätämällä tiedustelun oikeudellista valvontaa koskevassa laissa (/) jokaiselle oikeus tehdä tietoliikennetiedustelua koskeva tutkimispyyntö tiedusteluvaltuutetulle.

Ilmoittamisvelvollisuuden rajaaminen on perusteltua siksi, että tietoliikennetiedustelu saattaa puuttua eri vaiheissaan eri laajuudessa eri henkilöiden luottamuksellisen viestin salaisuuden suojaan. Silloin kun puuttuminen on ollut lievää tai ohimenevää tai sitä koskevat tiedot on hävitetty tiedusteluviranomaisen hallusta, ei ilmoittamiseen voida katsoa olevan syytä. Lisäksi on huomioitava, että ihmisoikeustuomioistuimen ratkaisukäytäntö edellyttää ilmoittamista sille nimenomaiselle henkilölle, joka on ollut tiedonhankinnan kohteena. Tietoliikennetiedustelun piiriin hetkellisesti tuleva henkilö, jonka tiedot hävitetään heti kun hänet on todettu sivulliseksi, ei ole tietoliikennetiedustelun kohde. Jakoa kohdehenkilöihin ja sivullisiin sovelletaan myös teletiedonhankintakeinoista ilmoittamista koskevassa sääntelyssä. Telekuuntelusta ja -valvonnasta edellytetään ilmoitettavan vain sille henkilölle, jonka rikoksen estämiseksi, paljastamiseksi tai selvittämiseksi tiedonhankintakeinoa on käytetty. Tiedonhankinnasta ei ilmoiteta niille ehkä lukuisillekin sivullisille henkilöille, joihin kohdehenkilö telekuuntelun tai -valvonnan aikana on ollut viestiyhteydessä ja joiden viestintäsalaisuuteen keinon käytöllä siten myös on puututtu. Vastaavasti esimerkiksi peitetoiminnasta tai suunnitelmallisesta tarkkailusta ei ilmoiteta sellaisille henkilöille, jotka sattumalta ja hetkellisesti ovat tulleet keinon käytön piiriin. Tietoliikennetiedustelusta ilmoittamista koskevan sääntelyn ei ole perusteltua merkittävästi poiketa muiden tiedonhankintakeinojen tai tiedustelumenetelmien ilmoittamista koskevasta sääntelystä.

Tietoliikennetiedustelusta edellytettäisiin lakiehdotuksen 20 §:n mukaan ilmoitettavan Suomessa olevalle henkilölle, jonka luottamuksellisen viestin sisältö tai tallentama tieto on selvitetty manuaalisesti. Ilmoitusvelvollisuutta ei olisi, jos tietoliikennetiedustelulla olisi selvitetty ainoastaan viestinnän muu tieto kuin sen sisältö, tai jos viestin sisältö olisi selvitetty automaattisesti. Viestin sisällön automaattinen selvittämisen tarkoituksena on supistaa manuaalisen käsittelyn kohteeksi otettavan tiedon määrää. Jos viesti hävitetään tällaisen karsimistarkoituksessa tehdyn toimenpiteen jälkeen ilman, että sen sisältö on tullut kenenkään suojelupoliisin virkamiehen tietoon, ei ilmoittamista voida katsoa perustelluksi. Velvollisuutta ilmoittaa tietoliikennetiedustelun käytöstä ei olisi myöskään sellaiselle henkilölle, joka on ulkomailla. Edelleen, koska ilmoitusvelvollisuus olisi ainoastaan henkilölle, jonka luottamuksellisen viestin sisältö on selvitetty, rajautuisivat vieraan valtion viranomaisviestinnän osapuolet ilmoittamisen ulkopuolelle sen perusteella, että viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Asiaa koskevan erityissäännöksen johdosta ilmoittamisen ulkopuolelle rajattaisiin myös henkilöt, joiden luottamuksellisen viestin sisältö on selvitetty manuaalisesti, mutta joiden viestintää koskevat tiedot lain sisältämien hävittämisvelvoitteiden mukaisesti on hävitetty viipymättä. Ilmoittaminen ei ole perusteltua, sillä sen henkilön tiedot, jolle ilmoitus olisi muuten tehtävä, olisi hävitetty tiedusteluviranomaisen hallusta lukuun ottamatta hävittämistä koskevaa lokitietomerkintää.

Silloin kun velvollisuus ilmoittaa tietoliikennetiedustelusta olisi olemassa, sovellettaisiin ilmoittamiseen, mitä poliisilain 5 a luvussa säädetään telekuuntelusta ilmoittamisesta. Ratkaisua voidaan perustella sillä, että tietoliikennetiedustelu, jossa on manuaalisesti selvitetty luottamuksellisen viestin sisältö, rinnastuu perusoikeuspuuttumisen syvyyden puolesta telekuunteluun. Telekuuntelua koskevan ilmoittamissäännöksen soveltamisesta seuraisi, että tiedonhankinnasta olisi viipymättä ilmoitettava tiedonhankinnan kohteelle sen jälkeen, kun tiedonhankinnan tarkoitus olisi saavutettu. Tuomioistuimen päätöksellä ilmoitusta voitaisiin kuitenkin siirtää tai jättää se kokonaan tekemättä, jos siirtäminen olisi perusteltua ja kokonaan ilmoittamatta jättäminen välttämätöntä laissa erikseen tyhjentävästi lueteltujen etujen suojaamiseksi. Siirtämisen ja kokonaan ilmoittamatta jättämisen yksilöllisistä syistä mahdollistava sääntely on sopusoinnussa Euroopan ihmisoikeustuomioistuimen ratkaisukäytännön kanssa.

Jokaisella olisi oikeus edellä todetusti kannella tietoliikennetiedustelusta tiedusteluvaltuutetulle täysin katsomatta siihen, onko hänelle tullut ilmoittaa siitä. Tiedusteluvaltuutettu myös valvoisi sitä, että suojelupoliisi soveltaa ilmoittamista koskevia säännöksiä oikein.

Tietojen luovuttaminen rikostorjuntaan

Tietojen luovuttamisesta rikostorjuntaan säädettäisiin yhdenmukaisesti poliisilain 5 a luvun 44 §:ssä ehdotetun kanssa.

4 Esityksen vaikutukset

4.1 Taloudelliset vaikutukset

Ehdotuksella tulisi olemaan vaikutusta valtion talousarvioon. Osa vaikutuksista olisi pysyviä, osa kertaluonteisia lähinnä investoinneista aiheutuvia. Osa valtiolle aiheutuvista menoista aiheutuisi suoraan nyt ehdotettavista säädösmuutoksista, osa siitä, että toiminnan volyymia olisi tarkoituksenmukaista laajentaa. Menojen tuleva ajoitus edellyttää vielä lisäselvityksiä muun muassa perustuslain tarkistamista koskevan lainsäädäntöhankkeen etenemisestä johtuen. Taloudellisten vaikutusten selvittämistä jatkettaisiin lähtökohtaisesti niin, että tehtävien rahoituksesta ja resursseista päätettäisiin julkisen talouden suunnitelman ja valtion talousarviovalmistelun yhteydessä.

Esityksellä on taloudellisia vaikutuksia sisäministeriön hallinnonalalla erityisesti suojelupoliisiin, mutta myös muuhun poliisiin sekä sisäministeriöön ja oikeusministeriön hallinnonalalla tuomioistuimiin, syyttäjiin ja Rikosseuraamusvirastoon sekä elinkeinoelämän osalta teleyrityksiin. Tarkemmat vaikutusarviot on esitetty osioissa 4.1.1 - 4.1.4. Taloudellisia vaikutuksia aiheutuu ensisijaisesti henkilöstön lisäystarpeesta, mutta myös kertaluonteisista investoinneista ja muun muassa operatiivisen toiminnan, koulutuksen ja tietojärjestelmien ylläpidon vuosittaisista menoista.

Taloudellisten vaikutusten arvioinnissa on otettu lähtökohdaksi, että siviilitiedustelua koskeva lainsäädäntö tulee voimaan vuoden 2019 alussa. Arvioidut taloudelliset vaikutukset konkretisoituvat lain voimaantulovuonna, pois lukien eräät suojelupoliisin menot, jotka toteutuvat etupainotteisesti jo vuosi ennen lainvoimaan tuloa. Jos lain voimaantulo aikaistuu tai myöhentyy lähtökohdaksi otetusta vuoden 2019 alusta, aikaistuvat tai myöhentyvät esitetyt taloudelliset vaikutukset vastaavasti.

LUONNOS

Suojelupoliisi

Suurin osa esityksessä ehdotettujen muutosten aiheuttamista taloudellisista vaikutuksista kohdistuisi suojelupoliisiin. Uuden lainsäädännön myötä suojelupoliisin tehtävät lisääntyvät merkittävästi tehtäväkentän laajetessa ja toimivaltuuksien lisääntyessä. Koska kyseessä on nykyistä laajempi tehtäväkenttä ja kokonaan uudet toimivaltuudet, ei suojelupoliisin nykyisiä taloudellisia tai henkilöstöresursseja ole mahdollista kohdentaa uusiin tehtäviin. Näin ollen kaikki tässä esitetyt lisäresursointitarpeet tulisivat päätettäväksi julkisen talouden suunnitelman yhteydessä ja talousarvioprosesseissa.

Suojelupoliisin nykyinen tehtävä on rikostorjunnallinen. Käytännössä se vastaa rikoslain 12 ja 13 luvuissa tarkoitettujen maan- ja valtiopetosrikosten estämisestä, paljastamisesta ja selvittämisestä sekä rikoslain 34 a luvussa tarkoitettujen terrorismirikosten estämisestä ja paljastamisesta. Terrorismirikosten selvittäminen kuuluu jo nykyisin pääsääntöisesti keskusrikospoliisille.

Esityksessä suojelupoliisin tehtäväksi säädettäisiin kansallisen turvallisuuden suojaaminen. Lainsäädännön voimaantulon myötä suojelupoliisin asema muuttuisi yhdistetyksi kotimaan turvallisuuspalveluksi ja ulkomaan tiedustelupalveluksi, jonka tehtävänä olisi hankkia tietoa kansalliseen turvallisuuteen kohdistuvista uhkista siihen katsomatta, onko uhkissa kyse rikoksista vai ei. Tiedonhankinnan perusteet sekä toiminnan ajallinen ja alueellinen ulottuvuus muuttuisivat ja laajenisivat nykyisestä.

Siviilitiedustelua koskevan lainsäädäntökokonaisuuden yhteydessä suojelupoliisilta ehdotetaan poistettavaksi sille nykyisin kuuluvat esitutkintatehtävät. Suojelupoliisi on käyttänyt henkilöresurssejaan ja suunnannut rahoituksestaan erittäin vähän näihin tehtäviin viime vuosina. Näin ollen ehdotuksella ei ole tähän liittyen henkilöstövaikutuksia eikä tarvetta suunnata nykyresursseja uudelleen.

Valtion turvallisuutta vaarantavien rikosten estämis- ja paljastamistehtävä säilyy suojelupoliisilla entiseen tapaan. Uusien koti- ja ulkomaantehtävien ja -toimivaltuuksien osoittamisesta suojelupoliisille ja samanaikaisesta olemassa olevien tehtävien ja toimivaltuuksien laajasta säilymisestä suojelupoliisilla seuraa, että viraston tehtäväkenttä ja sen velvoitteet muodostuvat kansainvälisessäkin vertailussa ainutlaatuisen laajoiksi.

Suojelupoliisin tehtäväkentän laajetessa ja sen toimivaltuuksien lisääntyessä viraston tiedonhankinnan volyymin arvioidaan kasvavan siinä suhteessa kuin tiedonhankintaa resursoidaan. Uuden lainsäädännön toimeenpano tulee asettamaan yhä korkeammat laadulliset, koulutukselliset, oikeudelliset ja rakenteelliset vaatimukset viraston kaikkien yksiköiden toiminnalle. Tiedonhankinnan volyymin kasvattaminen ja edellä mainittujen vaatimusten täyttäminen siten, että siviilitiedustelulainsäädännön vaikuttavuudelle asetetut tavoitteet saavutetaan, edellyttävät suojelupoliisin toiminnan perusresursoinnin uudelleenarviointia sekä kertaluonteisia ICT-investointeja. Operatiivisten resurssien ja valmiuksien vahvistaminen edellyttää myös niitä tukevien toimintojen, kuten henkilöstö- ja taloushallinnon, vahvistamista.

Uusien tiedustelutoimivaltuuksien riittävä hyödyntäminen ja sitä kautta saavutettava yhteiskunnallinen vaikuttavuus ulko- ja turvallisuuspoliittisessa päätöksenteossa, oikea-aikaisessa turvallisuustilannekuvassa viranomaisille ja kansantaloudellisten etujen suojaamisessa edellyttää resursoinnin oikea-aikaisuutta. Resursointi, koulutus ja toiminnan suunnittelu tulisi siksi käynnistää riittävän aikaisessa vaiheessa jo ennen lainsäädännön voimaantuloa.

LUONNOS

Siviilitiedustelun volyymi on verrannollinen siihen osoitettavien taloudellisten resurssien kanssa. Seuraavassa esitetyt määrärahalisäykset perustuvat siihen, että suojelupoliisi pystyisi suoriutumaan sille säädettävästä uudesta tehtävästä riittävän tehokkaasti ja laadukkaasti. Virastolle aiheutuvan henkilöresurssitarpeen arvioidaan jakautuvan siten, että perustettavista uusista viroista noin 30 % olisi poliisivirkoja ja 70 % siviilivirkoja.

Taloudellisten vaikutusten arvioinnissa on otettu tässä vaiheessa lähtökohdaksi, että siviilitiedustelua koskeva lainsäädäntö tulisi voimaan vuoden 2019 alussa. Jos jonkin rahoitustarpeen realisoitumisajankohdaksi esimerkiksi mainitaan jäljempänä vuosi 2018, tarkoitetaan tällä sitä, että etupainotteinen rahoitustarve on olemassa jo vuotta ennen lain voimaantuloa. Jos lain voimaantulo aikaistuu tai myöhentyy lähtökohdaksi otetusta vuoden 2019 alusta, aikaistuvat tai myöhentyvät etupainotteiset rahoitustarpeet vastaavasti. Siviilitiedustelulainsäädännöstä aiheutuvat kustannusvaikutukset on eritelty vuosittain jäljempänä tässä osiossa.

Suojelupoliisissa käynnissä oleva suojelupoliisin suorituskyvyn kehittämishanke (SSK), ei kata siviilitiedustelulaista ja tietoliikennetiedustelulaista aiheutuvia tarpeita.

Koulutus ja henkilöstö- ja taloushallinto. Suojelupoliisi ei voisi jatkossa nojautua yksinomaan Poliisiammattikorkeakoulun ja keskusrikospoliisin suunnittelemiin ja järjestämiin koulutuksiin salaisen tiedonhankinnan osalta, koska siviilitiedustelussa käytettävien toimivaltuuksien käyttöperuste, käyttöön liittyvät taktiset näkökohdat, kokonaan uudet toimivaltuudet ja menetelmien henkilöllinen kohdentaminen eroavat perinteisistä rikostorjuntamenetelmistä. Lisäksi menetelmiä on määrä käyttää uudessa toimintaympäristössä eli ulkomailla. Uusien siviilitiedustelutoimivaltuuksien koulutusrakenteet olisi siten luotava ja vakiinnutettava viraston sisälle. Tarkoitus on perustaa suojelupoliisiin koulutusyksikkö, joka vastaisi viraston henkilöstön erikois- ja jatkokoulutuksesta ja siviilitiedustelulain edellyttämästä päällystön erikoiskoulutuksesta sekä osallistuisi sotilastiedusteluviranomaisen, tuomioistuimien ja laillisuusvalvonnan kanssa tehtävään koulutusyhteistyöhön. Tässä vaiheessa suojelupoliisi arvioi, että suojelupoliisin koulutustoiminto sisältäisi perehdytysvaiheessa 6 henkilötyövuotta, joista 2 määräaikaista ja ylläpitovaiheessa 4 pysyvää henkilötyövuotta. Osa taktisesta koulutuksesta olisi hankittava sellaisilta kansainvälisiltä yhteistyötahoilta, joilla on pitkäaikainen kokemus tiedustelutoimivaltuuksien käytöstä. Lainsäädäntömuutoksista aiheutuva organisaation henkilömäärän kasvu edellyttäisi myös henkilöstöhallintoon sekä viraston talous- ja yleishallintoon liittyvien resurssien pysyvää vahvistamista.

Laillisuusvalvonta ja oikeudellinen tuki. Suojelupoliisissa ei ole nykyisin päätoimista sisäistä laillisuusvalvontatoimintoa, vaan sisäistä laillisuusvalvontaa suoritetaan samoin kuin muussakin poliisissa sivutoimisesti ja pääasiassa määräaikaisten tarkastusten muodossa.

Uusien tiedustelutoimivaltuuksien myötä viraston sisäisen laillisuusvalvonnan merkitys korostuu. Sisäinen laillisuusvalvonta olisi järjestettävä entistä reaaliaikaisemmaksi, tehokkaammaksi ja kattavammaksi, mikä edellyttäisi eriyttämistä omaksi toiminnokseen ja siten lisäresursseja (4htv). Samalla olisi järjestettävä sisäisen laillisuusvalvonnan suhde ulkoisiin laillisuusvalvontaelimiin, ennen kaikkea tähän esitykseen liittyvässä oikeusministeriön esityksessä ehdotettavaan valvontaviranomaiseen. Laillisuusvalvonta tekisi tiivistä yhteistyötä koulutusyksikön kanssa oikeiden soveltamiskäytäntöjen jakamiseksi tiedustelutoimivaltuuksia käyttäville virkamiehille. Sisäisen laillisuusvalvonnan järjestäminen edellyttäisi osin rahoitusta jo ennen lain voimaantuloa siten, että toimintoa varten suojelupoliisin tarvitsemasta arvioidusta kokonaishenkilöresurssista 3 henkilötyövuotta saataisiin käyttöön vuosi ennen lain voimaantuloa. Tämä mahdollistaisi sen, että oikeisiin soveltamiskäytäntöihin perustuva riittävästi koulutettu siviilitiedustelumenetelmien käyttö voitaisiin aloittaa täysimittaisesti heti lain voimaantullessa.

Lisäksi operatiivisiin yksiköihin perustetaan kaksi uutta operatiivisen lakimiehen miehen virkaa, joilla tuetaan uusien kotimaan, ulkomaan ja tietoliikenne-tiedustelutoimivaltuuksien operatiivista tiedonhankintaa. Nämä virat sisältyvät sisäisen laillisuusvalvonnan kokonaisresurssitarpeeseen 4 henkilötyövuotta. Edellä kuvatulla jaolla varmistetaan, että laillisuusvalvonta ja operatiivinen päätöksenteko pidetään jatkossakin erillään.

Menetelmäkehitys, analyysi ja operatiivinen tiedonhankinta. Siviilitiedustelulainsäädännön myötä suojelupoliisin tehtävät lisääntyisivät ja viraston tehtäväkenttä laajenisi. Tiedonhankinta tulisi vastaisuudessa perustumaan kansallisen turvallisuuden suojaamiseen eikä yksinomaan rikosten estämiseksi ja paljastamiseksi. Uusien toimivaltuuksien tehokas hyödyntäminen edellyttäisi operatiivisen tiedonhankinnan vahvistamista sekä henkilöresurssien että laitteiston ja menetelmäkehityksen muodossa. Kun viraston hankkiman raakatiedon määrä välttämättömien panostusten johdosta kasvaisi, olisi tiedon hyödynnettävyys varmistettava panostamalla sisään virtaavan tiedon tekniseen ja operatiiviseen analysointiin sekä sen esikäsittelyyn, uhkien jatkoselvittämiseen ja kohdehenkilöiden valvontaan. Tiedonhankinnan tehostaminen ja hankitun tiedon hyödyntäminen Suomen kansallisen turvallisuuden suojaamiseksi edellyttää myös, että suojelupoliisi laajentaa yhteistyöverkostoaan luomalla uusia kumppanuuksia sekä kotimaisiin että ulkomaisiin viranomaistahoihin ja muihin toimijoihin. Tämän johdosta operatiivisen yhteistyön määrä tulisi kasvamaan merkittävästi.

Arvioitu henkilöresurssitarve operatiivisen toiminnan ja yhteistyörakenteiden vahvistamiselle on 48 henkilötyövuotta. Kyse olisi uusien pysyvien virkojen perustamisesta. Tehokas ja täysimittainen tiedustelutoimivaltuuksien hyödyntäminen edellyttää, että taktinen ja tekninen menetelmäkehitys aloitettaisiin hyvissä ajoin ennen lain voimaantuloa ja että operatiivinen henkilöstö olisi riittävissä määrin koulutettu toimivaltuuksien käyttöön ennen lain voimaantuloa. Tästä johtuen uusia virkoja tulisi perustaa ja laitteistoa hankkia jo osin ennen lain voimaantuloa.

Raportointi valtiojohdolle, viranomaisille ja muille sidosryhmille. Suojelupoliisin hankkiman tiedon määrän arvioidaan kasvavan tiedonhankinnan perusteiden laajentuessa ja uusien tiedustelumenetelmien sekä lisäresursoinnin myötä. Yksi siviilitiedustelulainsäädännön keskeisiä tavoitteita on lisätä ja parantaa ylimmän valtiojohdon tiedonsaantia Suomen turvallisuustoimintaympäristön muutoksista ja kehittymisestä oikea-aikaisen ja riittäviin tosiseikkoihin perustuvan ulko- ja turvallisuuspoliittisen päätöksenteon tukemiseksi. Tämän tehtävän täyttäminen edellyttää, että suojelupoliisin hankkima tiedustelutieto saatettaisiin monipuolisesti ja perusteellisesti analysoituna valtiojohdon ja viranomaisten käyttöön, jotta suojelupoliisi voisi optimaalisella tavalla tukea niiden toimintaa. Lainsäädännön uudistuessa myös odotukset analysoidun tiedustelutiedon tuottamiseksi yksityisen sektorin toimijoiden käyttöön yhteiskunnan tärkeiden taloudellisten etujen turvaamiseksi kasvaisivat. Uusien toimivaltuuksien avulla hankitun tiedustelutiedon strategiseen analysointiin ja yhdistelemiseen sekä sen raportointiin asiaankuuluville tahoille olisi välttämätöntä resursoida, arviolta 8 henkilötyövuotta.

Tietoliikennetiedustelu. Esityksestä ilmenevällä tavalla puolustusvoimien tiedustelulaitos toimisi siviilitiedustelutarkoituksessa tapahtuvan tietoliikennetiedustelun teknisenä toteuttajana. Suojelupoliisi olisi vastuussa sille välitettyjen tietojen analysoinnista ja muista jatkotoimenpiteistä. Ratkaisusta seuraa, että tietoliikennetiedustelun teknisestä toteuttamisesta aiheutuvat kustannukset kohdistuisivat ensi sijassa puolustusvoimien tiedustelulaitokseen. Taloudellisten vaikutusten arviointi tältä osin on sisällytetty tähän esitykseen liittyvään sotilastiedustelulainsäädäntöä koskevaan esitykseen. Siviilitiedustelutarkoituksessa tapahtuvaan tietoliikennetiedusteluun liittyviä kustannuksia käsitellään jäljempänä olevassa taulukossa vain siltä osin kuin ne kohdistuvat suojelupoliisin. Sekä siviilitiedustelussa että sotilastiedustelussa käytettävien teletiedustelumenetelmien kustannusvaikutukset on sisällytetty suojelupoliisin taloudel-

listen vaikutusten arviointiin. Mahdolliset viranomaisten väliset kustannusten jaot tarkastellaan vielä erikseen.

Ulkomaan tiedustelu. Ulkomaan tiedustelutoimivaltuudet edellyttäisivät kokonaan uuden toiminnon perustamista. Tämä tarkoittaisi erikoiskoulutettua henkilöstöä, tiedonhankinnan ja henkilöstön suojaamisrakenteita ja -prosesseja, tarpeen mukaan ympärivuorokautista operatiivista vasteaikaa sekä kansainvälisiä yhteistyörakenteita. Ulkomaan tiedustelun toteuttaminen edellyttää myös siihen liittyvän tukitoiminnon ylläpitoa (muun muassa talouspalvelut sekä hallinnollisten suojaamisrakenteiden ja peitteiden tuki). Ympärivuorokautinen tukitoiminta sisältää myös henkilöstöturvallisuustoiminnan laajentamisen ja vahvistamisen, kuten ympärivuorokautisen vartioinnin sekä virastopalveluiden ja kiinteistöpalveluiden ylläpidon operatiivisen toiminnan edellyttämällä tavalla.

Toimitilakulut. Uuteen siviilitiedustelulainsäädäntöön liittyvät resurssilisäykset tulevat merkitsemään viraston henkilöstömäärän kasvua, mikä puolestaan tulee kasvattamaan myös viraston toimitilakustannuksia. Suojelupoliisi on arvioinut tässä vaiheessa, että jokainen henkilötyövuoden lisäys aiheuttaa vuosittaisten toimitilakustannusten kasvamisen 7.500 eurolla.

Samanaikaisesti tämän lainsäädäntöhankkeen kanssa on meneillään suojelupoliisin toimitilahanke, jossa kartoitettavana ovat vaihtoehdot toimitilakysymyksen järjestämiseksi viraston nykyisten toimitilojen vuokrasopimuksen päättyessä vuosien 2019 ja 2020 vaihteessa. Toimitilojen mahdollisista uudelleenjärjestelyistä aiheutuvia kustannuksia ei ole huomioitu esityksessä eikä tiedustelulainsäädännöstä aiheutuvia kustannuksia ole toistaiseksi huomioitu toimitilahankkeessa.

Yhteenveto esityksen suojelupoliisin taloudellisista vaikutuksista (suojelupoliisin arvio)

Yhteenveto lakiesityksen taloudellisista vaikutuksista koskien suojelupoliisia	**TAE2018**	**S2019** ***(lain ehdotettu voimaantulo)***	**S2020**	**S2021 ->**
Suojelupoliisin toimintamenot 26.10.02				
Kertaluonteiset investoinnit	**9 700 000**	**-**	**-**	**-**
- josta tietojärjestelmämuutoskustannukset	*700 000*			
- josta tietoliikennetiedustelun investoinnit	*9 000 000*			
Henkilöstökulut (htv)	**1 911 000 (27 htv)**	**6 764 000 (94 htv)**	**6 764 000 (94 htv)**	**6 614 000 (92 htv)**
Muut vuotuiset kulut yhteensä	**895 000**	**4 405 000**	**4 405 000**	**4 390 000**
- josta toimitila-, turvallisuus-, vartiointi- ja kiinteistöpalvelut	*195 000*	*1 105 000*	*1 105 000*	*1 090 000*
- josta ajoneuvohankinnat	*-*	*200 000*	*200 000*	*200 000*
- josta operatiiviset kehityskustannukset	*400 000*	*1 500 000*	*1 500 000*	*1 500 000*
- josta linja-, ylläpito- ja lisenssikustannukset, tietojärjestelmien elinkaarikustannukset sekä korvaukset operaattoreille	*-*	*1 300 000*	*1 300 000*	*1 300 000*
- josta ulkopuolinen koulutus	*300 000*	*300 000*	*300 000*	*300 000*
Suojelupoliisi yhteensä	**12 506 000**	**11 169 000**	**11 169 000**	**11 004 000**

Suojelupoliisin sisäinen valvonta on eduskunnan oikeusasiamiehen tekemien laillisuusvalvonnan havaintojen mukaan hyvällä tasolla. Suojelupoliisi siirtyi vuoden 2016 alusta sisäministeriön alaisuuteen eikä ole enää Poliisihallituksen laillisuusvalvonnan piirissä. Sisäministeriön laillisuusvalvonnan henkilöresurssit ovat oikeusasiamiehen mukaan varsin vähäiset ja henkilöstöllä on runsaasti muitakin tehtäviä. Oikeusasiamiehen mukaan tulee varmistaa, ettei suojelupoliisin valvonnan taso laske (Eduskunnan oikeusasiamiehen kertomus vuodelta 2015, s. 181).

Siviilitiedustelulainsäädäntökokonaisuus kasvattaisi suojelupoliisin tiedonhankintatoimivaltuuksia sekä henkilöresurssien määrää tavalla, joka edellyttäisi vahvistamaan sen sisäistä laillisuusvalvontaa reaaliaikaisemman valvonnan muodossa. Tämä toiminta- ja valvontalisä edellyttäisi myös sisäministeriön hallinnollisia ja oikeudellisia tehtäviä suojelupoliisiin liittyen. Sisäministeriön on arvioinut, että henkilöresurssitarve sisäministeriön valvontamekanismin vahvistamiselle on vähintään kaksi henkilötyövuotta eli euromääräisesti arvioituna noin 175.000 euroa.

Edellä suojelupoliisia koskevassa osiossa siviilitiedustelukyvyn luominen tulisi kasvattamaan suojelupoliisin resursseja 92 henkilötyövuodella. Ottaen huomioon siviilitiedustelutoimintaan ja tiedustelutoimivaltuuksien käyttöön liittyvä ohjaustarve sekä toiminnan henkilöstöresurssit, sisäministeriön ohjauksen merkityksen arvioidaan korostuvan. Jotta sisäministeriö pystyisi toteuttamaan edellä esitetyssä normeissa sille säädetyt tehtävät, henkilöresurssitarve sisäministeriön ohjausmekanismin vahvistamiselle olisi vähintään kaksi henkilötyövuotta eli euromääräisesti arvioituna on 175.000 euroa.

Sisäministeriö on 12.10.2016 tekemällään päätöksellä (SMDno-2016-1478) asettanut hankkeen valmistelemaan ehdotukset siviilitiedustelun sekä suojelupoliisin ohjauksen kehittämiseksi sisäministeriön hallinnonalalla. Kyseisen hankkeen loppuraportissa ja tämän esityksen taloudellisia vaikutuksia koskevassa jaksossa arvioidaan tarkemmin suojelupoliisin ohjauksen ja valvonnan aiheuttamia työmäärän lisäyksiä sisäministeriössä edellä arvioidun minimivaatimuksen ylittäviltä osin.

Yhteenveto lakiesityksen taloudellisista vaikutuksista koskien sisäministeriötä	**TAE2018**	**S2019** ***(lain ehdotettu voimaantulo)***	**S2020**	**S2021 ->**
Sisäministeriön toimintamenot 26.01.01				
Henkilöstökulut (htv)		**350 000 (4 htv)**	**350 000 (4 htv)**	**350 000 (4 htv)**

Muu poliisihallinto

Kaikkein vakavimpien rikosten selvittäminen ja erityisesti ennalta estäminen on puolestaan yhteiskunnan kokonaisedun mukaista, mistä johtuen niiden ilmoittaminen rikostorjuntaan on syytä laajasti sallia. Ilmoittamista perustelee myös oikeudenmukaisuus ja vakavan rikoksen uhrin näkökulman huomioonottaminen. Suojelupoliisin oikeudesta ja velvollisuudesta ilmoittaa muulle poliisiviranomaiselle tiedustelumenetelmän aikana havaitusta rikoksesta ehdotetaan säädettäväksi poliisi-lain 5 a luvun 43 §:ssä ja tietoliikennetiedustelulain 17 §:ssä. Suojelupoliisilla olisi mainittujen säännösten mukaan velvollisuus ilmoittaa toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenisi jokin rikoslain 15 luvun 10 §:ssä tarkoitettu jo tapahtunut tai vielä estettävissä oleva ylitörkeä rikos. Tiedustelussa havaitun jo tapahtuneen rikoksen osalta laissa säädettäisiin välttämättömiin syihin perustuvasta mahdollisuudesta lykätä ilmoituksen tekemistä. Lisäksi suojelupoliisilla olisi oikeus ilmoittaa toimivaltaiselle viranomaiselle tiedustelumenetelmän käytön aikana ilmenneestä jo tapahtuneesta tai

vielä estettävissä olevasta lievemmästä rikoksesta, jonka seuraamusuhka ylittää tietyn alarajan. Jo tapahtuneiden rikosten osalta vähimmäisseuraamusuhkana olisi kolme vuotta vankeutta ja vielä estettävissä olevien rikosten osalta kaksi vuotta vankeutta.

Ilmoittamisvelvollisuus ja -oikeus koskisivat sellaisia rikoksia, joista suojelupoliisi saa tiedon tiedustelumenetelmän käytön yhteydessä. Tiedustelumenetelmät vastaisivat, paikkatiedustelu ja tietoliikennetiedustelu pois lukien, niitä salaisia tiedonhankintakeinoja, joiden käytöstä nykyisin säädetään poliisilain 5 luvussa ja joita suojelupoliisi käyttää rikoksen estämiseksi ja paljastamiseksi. Tiedonhankintamenetelmien lukumäärän lisääntyminen olisi näin ollen varsin rajallista.

Siviilitiedustelun tiedonhankinnan kohteista säädettäisiin poliisilain 5 a luvun 3 §:ssä ja tietoliikennetiedustelulain 3 §:ssä. Kyseiset tiedustelumenetelmien käytön perusteuhkat laajentaisivat suojelupoliisin tiedonhankintatoimivaltuuksia pääasiassa kahdella tapaa. Yhtäältä tietoa voitaisiin hankkia eräistä sellaisista kansallista turvallisuutta vakavasti uhkaavista ilmiöistä, jotka eivät ole rikoksia ja joiden ei myöskään voida olettaa muodostuvan sellaisiksi. Toisaalta tietoa voitaisiin hankkia nykyistä varhaisemmassa vaiheessa, sillä tiedustelumenetelmiä olisi mahdollista käyttää jo silloin, kun tiedonhankinnan kohteena oleva teko ei ole konkretisoitunut estettävän rikoksen eli niin sanotusti konkreettisen ja yksilöidyn rikosepäilyn asteelle.

Edellä mainittujen laajennusten luonne vaikuttaa siihen, kuinka paljon rikoslain 15 luvun 10 §:n mukaisia jo tapahtuneita tai vielä estettävissä olevia rikoksia voidaan olettaa vuosittain ilmoitettavan muille poliisiyksiköille. Siltä osin kuin tiedustelumenetelmän käyttö kohdistuu ilmiöön, jonka ei edes voida olettaa muodostuvan rikokseksi olisi harvinaista, että käytön yhteydessä paljastuisi rikoksia. Siltä osin kuin tiedustelussa on kyse rikoksen estämistä edeltävästä varhaisvaiheen tiedonhankinnasta, voidaan arvioida, että sama tiedonhankinta saattaisi joka tapauksessa myöhemmin tulla toteutetuksi poliisilain 5 luvun mukaisena salaisena tiedonhankintana.

Ne rikokset, joista suojelupoliisi olisi velvoitettu tai oikeutettu ilmoittamaan, voidaan karkeasti jakaa yhtäältä rikoksiin, jotka suoraan kytkeytyvät tiedustelun perusteena olevaan uhkaan, ja toisaalta rikoksiin, jotka tiedustelun näkökulmasta rinnastuvat ylimääräisen tiedon luonteiseen tietoon. Esimerkkinä ensimmäiseen ryhmään kuuluvasta rikoksesta voidaan mainita terrorismin rahoittamisrikos, joka voi tulla ilmi silloin, kun tiedustelun perusteuhkana on terrorismi. Esimerkkinä jälkimmäiseen ryhmään kuuluvasta rikoksesta voidaan mainita törkeä varkaus, joka sattumalta tulee ilmi tiedusteltaessa joukkotuhoaseiden leviämistä.

Ensimmäiseen ryhmään kuuluvia rikoksia voidaan olettaa tulevan tiedustelussa ilmi jossain laajuudessa, kun taas jälkimmäiseen ryhmään kuuluvia rikoksia voidaan arvioida tulevan ilmi harvemmin. Voidaan myös arvioida, että ensimmäiseen ryhmään kuuluvia rikoksia, erityisesti valmistelu- ja edistämistyyppisiä rikoksia, tulisi ilmi nimenomaan silloin, kun tiedustelumenetelmän käytön perusteuhkana on terrorismi. Vaikka esitutkintaviranomaiselle ilmoitettavien terrorismirikosten määrä todennäköisesti tulisi uuden lainsäädännön voimaantulon myötä lisääntymään, on myös huomioitava, että lainsäädäntö sisältää lisääntymistä hillitseviä tekijöitä. Terrorismia koskeva tiedonhankinta tapahtuisi aiempaa varhaisemmassa vaiheessa. Ainakin osassa tapauksia tiedustelu mahdollistaisi sellaisiin varhaisvaiheen torjuntatoimiin ryhtymisen, joiden johdosta tiedonhankinnan kohteena oleva toiminta ei lainkaan pääsisi etenemään rangaistavan ja siten ilmoitettavan menettelyn asteelle. Edellä kerrotun perusteella tiedustelu voisi osaksi olla omiaan vähentämään toteutuneiden ja sitä kautta rikosoikeudellisen menettelyn piiriin tulevien rikosten määrää. Tiedonhankinnan siirtymisestä aiempaa varhaisempaan vaiheeseen seuraisi myös, että rikoksen havaitseminen ja rikoksesta esitutkintaviranomaiselle tehtävä ilmoitus aikaistuisi nykyisestä. Suojelupoliisi siirtää nykyisin esitutkintaviranomaisille

varsin laajasti sellaisia terrorismirikoksia, jotka ovat tulleet ilmi sen käyttäessä poliisilain 5 luvussa säädettyjä salaisia tiedonhankintatoimivaltuuksia. On ilmeistä, että joistain näistä rikoksista saataisiin havainto ja ilmoitettaisiin jo tiedustelumenetelmää käytettäessä. Kyse ei tältä osin ole ilmoitusten lisääntymisestä, vaan niiden aikaistumisesta.

Silloin kun tiedustelun perusteuhkana on vieraan valtion tiedustelutoiminta, voidaan olettaa, että ilmi saattaisi tulla rikoslain 12 luvussa tarkoitettuja maanpetoksellisia rikoksia. Harkittaessa näiden rikosten rikostutkintaan siirtämistä on huomioitava, että niitä esimerkiksi diplomaattiseen koskemattomuuteen liittyvistä syistä ei useinkaan voida käsitellä rikosprosessissa. Reagointi rikokseen tapahtuu diplomaattisin eikä rikosoikeudellisin keinoin.

Edellä on todettu, että poliisilain 5 a luvussa säädettäväksi ehdotettavat tiedustelumenetelmät ovat valtaosiltaan samat kuin ne, joista nykyisin säädetään salaisina tiedonhankintakeinoina poliisilain 5 luvussa. Merkittävin täysin uusi tiedustelumenetelmä olisi tietoliikennetiedustelu, josta säädettäisiin erillisessä laissa. Tietoliikennetiedustelun avulla saatavan tiedon voidaan arvioida olevan luonteeltaan sellaista, että se ei sellaisenaan useinkaan johda rikoksen havaitsemiseen ja siitä ilmoittamiseen. Puolustusministeriön asettaman tiedonhankintalakityöryhmän mietinnössä todetaan, että tietoliikennetiedustelun avulla saatavat tiedot ovat pääasiassa muita viestintään liittyviä tietoja kuin viestinnän sisältöä kuvaavia tietoja. Tämä johtuu muun muassa viestinnän yleistyvästä salauksesta Viestinnän ohjaus- ja välitystiedot ovat tiedustelun kannalta erittäin hyödyllisiä, mutta niiden perusteella ei yleensä voida tehdä johtopäätöstä, että jokin tietty rikos on tapahtunut, mikä puolestaan laukaisisi velvollisuuden tai oikeuden ilmoittaa siitä esitutkintaviranomaiselle.

Edellä sanottujen seikkojen perusteella voidaan suuntaa-antavasti arvioida, että niin sanotun palomuurisääntelyn (5 a luvun 44 §) puitteissa esitutkintaviranomaiselle tehtävistä ilmoituksista itsenäisen esitutkinnan käynnistäviä tiedonluovutuksia arvioidaan olevan kaksi. Osa palomuurisääntelyn puitteissa tehtävistä ilmoituksista saattaa tämän lisäksi liittyä jo käynnissä oleviin tutkintoihin tai olla sellaisia, ettei esitutkintaviranomainen katso esitutkintakynnyksen ylittyneen. Palomuurisääntelyä soveltaessaan suojelupoliisi ei arvioi esitutkintakynnyksen ylittymistä ainakaan sillä tavalla kuin esitutkintalaissa säädetään, vaan arvion tekeminen kuuluu ilmoituksen vastaanottajalle. Esitutkintaviranomainen saattaa arvioida, että luovutettu tieto soveltuu ainoastaan rikostiedustelukäyttöön. Myös tällainen tieto aiheuttaa toimenpiteitä, josta syntyy henkilötyövuosivaikutuksia.

Edellä kerrotun perusteella poliisilain 5 a luvun 44 §:n mukaisien ilmoitusten voidaan arvioida johtavan muun poliisihallinnon osalta 20 henkilötyövuoden lisäystarpeeseen mistä aiheutuisi vuosittain 1 180 000 euron meno, jota ei ole mahdollista uudelleen kohdentaa poliisihallinnon muista nykyisistä tehtävistä. Tässä vaiheessa kyse olisi resurssitarpeiden suuntaa-antavasta vähimmäisarviosta.

Yhteenveto lakiesityksen taloudellisista vaikutuksista koskien muuta poliisihallintoa	**TAE2018**	**S2019** ***(lain ehdotettu voimaantulo)***	**S2020**	**S2021 ->**
Poliisin toimintamenot 26.10.01				
Henkilöstökulut (htv)		**1 180 000 (20 htv)**	**1 180 000 (20 htv)**	**1 180 000 (20 htv)**
Muut vuotuiset kulut		**140 000**	**140 000**	**140 000**
Poliisin htv -määrän noston vaikutus muihin vuotuisiin kuluihin (7 000€/htv)		*140 000*	*140 000*	*140 000*
Muu poliisi yhteensä		**1 320 000**	**1 320 000**	**1 320 000**

Oikeushallinto

Tietojen luovuttaminen rikostorjuntaan johtaisi poliisin osalta 20 henkilötyövuoden lisäykseen, mistä aiheutuisi vuosittain 1 180 000 euron menot. Oikeusministeriön hallinnonalalla lisämäärärahan tarve on tällä ja Helsingin käräjäoikeuden käsiteltäviksi tulevien lupa-asioiden perusteella oikeusavun osalta 141 600 euroa, syyttäjälaitoksen osalta 153 400 euroa, tuomioistuinten osalta 473 800 euroa ja rangaistusten täytäntöönpanon osalta 944 000 euroa.

Oikeusministeriön arvio perustuu eri viranomaisten osuuksiin rikostorjunnan kustannuksista. Poliisin rikostorjunnan osuus rikosprosessin kustannuksista on noin 42 prosenttia. Vuonna 2013 poliisin rikostorjunnan kustannukset olivat 345 miljoonaa euroa, syyttäjälaitoksen 46 miljoonaa euroa, oikeusavun 41 miljoonaa euroa, tuomioistuinten 107 miljoonaa euroa ja rangaistusten täytäntöönpanon 278 miljoonaa euroa. Jokaista poliisin rikostorjuntaan käyttämää euroa kohden aiheutuu siten oikeusministeriön hallinnonalalle kustannuksia keskimäärin 1,36 euroa, josta syyttäjien osuus on 0,13 euroa, oikeusavun 0,12 euroa, tuomioistuinten 0,31 euroa ja rangaistusten täytäntöönpanon 0,8 euroa. Luvut on laskettu tiedoista, jotka sisältyvät Oikeuspoliittisen tutkimuslaitoksen julkaisuun ”Rikollisuustilanne 2013” (Ville Hinkkanen: Rikollisuuden kustannukset, s. 412). Edellä kerrotun laskentakaavan perusteella saatujen arvojen lisäksi tuomioistuinlaitoksen kustannuksiin on sisällytetty arvio suojelupoliisin lupavaatimusten käsittelystä aiheutuvista kuluista.

Oikeusministeriön hallinnonalan arvioitujen vaikutusten osalta on syytä korostaa erityisesti rangaistusten täytäntöönpanoon liittyvien vaikutusten arvioinnin vaikeutta. Vaikutukset riippuvat siltäkin osin rikosprosessiin päätyvien asioiden määrästä ja laadusta, joita on vaikea ennakoida. Sama koskee sitä, minkälaisia ja minkä pituisia rangaistuksia tuomitaan. Toisaalta rikostorjuntaan luovutettavat tiedot koskevat vakavia rikoksia, mikä voi johtaa vuosittain useidenkin pitkien ehdottomien vankeusrangaistusten tuomitsemiseen. Vaikutusten selvittämistä jatketaan.

Yhteenveto lakiesityksen taloudellisista vaikutuksista koskien oikeushallintoa	**TAE2018**	**S2019** ***(lain ehdotettu voimaantulo)***	**S2020**	**S2021 ->**
Oikeusministeriön hallinnonala 25.				
Muiden tuomioistuinten toimintamenot 25.10.03				
Henkilöstökulut, ml. lupakustannukset		**473 800**	**473 800**	**473 800**
Oikeusaputoimistojen ja kuluttajariitalautakunnan toimintamenot 25.10.04				
Henkilöstökulut		**141 600**	**141 600**	**141 600**
Syyttäjälaitoksen toimintamenot 25.30.01				
Henkilöstökulut		**153 400**	**153 400**	**153 400**
Rikosseuraamuslaitoksen toimintamenot 25.40.01				
Henkilöstökulut		**944 000**	**944 000**	**944 000**

Yhteenveto lakiehdotusten taloudellisista vaikutuksista

Yhteenveto lakiesityksen taloudellisista vaikutuksista	**TAE2018**	**S2019** ***(lain ehdotettu voimaantulo)***	**S2020**	**S2021 ->**
Sisäministeriön hallinnonala 26.				
Suojelupoliisin toimintamenot 26.10.02				

Kertaluonteiset investoinnit	**9 700 000**	**-**	**-**	**-**
- josta tietojärjestelmä-muutoskustannukset	*700 000*			
- josta tietoliikennetiedustelun investoinnit	*9 000 000*			
Henkilöstökulut (htv)	**1 911 000 (27 htv)**	**6 764 000 (94 htv)**	**6 764 000 (94 htv)**	**6 614 000 (92 htv)**
Muut vuotuiset kulut yhteensä	**895 000**	**4 405 000**	**4 405 000**	**4 390 000**
- josta toimitila-, turvallisuus-, vartiointi- ja kiinteistöpalvelut	*195 000*	*1 105 000*	*1 105 000*	*1 090 000*
- josta ajoneuvohankinnat	*-*	*200 000*	*200 000*	*200 000*
- josta operatiiviset kehityskustannukset	*400 000*	*1 500 000*	*1 500 000*	*1 500 000*
- josta linja-, ylläpito- ja lisenssikustannukset, tietojärjestelmien elinkaarikustannukset sekä korvaukset operaattoreille	*-*	*1 300 000*	*1 300 000*	*1 300 000*
- josta ulkopuolinen koulutus	*300 000*	*300 000*	*300 000*	*300 000*
Suojelupoliisi yhteensä	**12 506 000**	**11 169 000**	**11 169 000**	**11 004 000**
Poliisin toimintamenot 26.10.01				
Henkilöstökulut (htv)		**1 180 000 (20 htv)**	**1 180 000 (20 htv)**	**1 180 000 (20 htv)**
Muut vuotuiset kulut		**140 000**	**140 000**	**140 000**
Poliisin htv -määrän noston vaikutus muihin vuotuisiin kuluihin (7 000€/htv)		*140 000*	*140 000*	*140 000*
Muu poliisi yhteensä		**1 320 000**	**1 320 000**	**1 320 000**
Sisäministeriön toimintamenot 26.01.01				
Henkilöstökulut (htv)		**350 000 (4 htv)**	**350 000 (4 htv)**	**350 000 (4 htv)**
Oikeusministeriön hallinnonala 25.				
Muiden tuomioistuinten toimintamenot 25.10.03				
Henkilöstökulut, ml. lupakustannukset		**473 800**	**473 800**	**473 800**
Oikeusaputoimistojen ja kuluttajariitalautakunnan toimintamenot 25.10.04				
Henkilöstökulut		**141 600**	**141 600**	**141 600**
Syyttäjälaitoksen toimintamenot 25.30.01				
Henkilöstökulut		**153 400**	**153 400**	**153 400**
Rikosseuraamuslaitoksen toimintamenot 25.40.01				
Henkilöstökulut		**944 000**	**944 000**	**944 000**

4.2 Vaikutukset kansantalouteen ja yrityksiin

Tiedustelulainsäädännön vaikutuksia kansantalouteen, yrityksiin ja elinkeinoelämään on arvioitava kokonaisuutena. Lainsäädännön seurauksia arvioitaessa 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.

Siviilitiedustelulainsäädännön tarkoituksena on suojata Suomen kansallista turvallisuutta ja siihen kuuluvaa kansantaloutta. Siviilitiedustelulainsäädännön 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 täydentävät 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 ennakoitavuutta yritysten toiminnan suunnittelun ja investointipäätösten kannalta. 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 kriteereitä vastaaviksi.

Yhteiskuntaan kohdistuvien uhkien tunnistaminen ja torjunta sekä 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 suojelupoliisi voisi luovuttaa tietoa yrityksille näiden merkittävien etujen suojaamiseksi. Tiedustelun tuottamaa tietoa voitaisiin tarvittaessa luovuttaa yksityisille yhteisöille vakavien uhkien torjunnan mahdollistamiseksi tai merkittävien taloudellisten tappioiden estämiseksi. Asiaa koskevaa sääntelyä sisältyisi muun muassa ehdotettavaan siviilitietoliikennetiedustelulakiin.

Vaikutukset elinkeinoelämän kilpailukykyyn ja investointeihin

Elinkeinoelämä toimii globaalissa, kansainvälisen talouden ja arvoverkostojen toimintaympäristössä. Globaalissa kilpailussa pienetkin tekijät ovat vaikutuksellisia. Yritykset sijoittavat toimintonsa maakohtaisesti optimoiden koko yritystoimintansa omien yrityskohtaisten kilpailuetujen perusteella. Sijoittautumispäätökset ovat kokonaisarviointeja yritysten liiketoiminnan kannalta, joissa 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.

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. Vaikutukset yritystoiminnalle ovat erilaiset riippuen muun muassa yrityksen toimialasta, koosta ja sen harjoittamasta kansainvälisestä toiminnasta.

Täsmällinen, tasapuolinen ja oikeasuhtainen tiedustelusääntely vahvistaa Suomen mainetta ennustettavana ja luotettavana toimintaympäristönä. Tämä koskee jo Suomessa olevia ja Suomeen mahdollisesti investoivia toimijoita.

Lainsäädäntötyössä on arvioitu sääntelyn vaikutuksia Suomen kansainväliseen kilpailukykyyn sekä Suomen houkuttelevuuteen investointikohteena. Valtioiden ylimitoitetun verkkovalvonnan- ja tiedustelutoiminnan on kansainvälisissä tutkimuksissa katsottu vaikuttavan negatiivisesti kansalaisten digitaalisia palveluita kohtaan tuntemaan luottamukseen ja ICT-alan yritysten edellytyksiin saada kansainvälisiä asiakkaita tai tehdä investointeja kyseisiin valtioihin. Olennaista ICT-alan yritysten kilpailukyvyn kannalta on, että ehdotettava 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. Uskottava valvontajärjestelmä ja viranomaistoiminnan kontrolli ovat myös olennaisia sääntely-ympäristöä selvittävien ja Suomea liiketoimintaympäristönä arvioivien kansainvälisten ICT-yritysten kannalta. Yrityssalaisuuden suojaa tukevat puolestaan lakiin kirjatut käsittelykiellot ja hävittämisvelvollisuudet sekä tiedusteluviranomaisten kansainväliseen tiedonvaihtoon liittyvät kirjaukset.

Kaikkien Suomessa toimivien yritysten, ja erityisesti tiedonsiirtäjiksi määriteltävien yritysten kannalta on huomioitu, että sääntelystä aiheutuvat velvoitteet ovat selkeitä, läpinäkyviä ja ennakoitavissa. Tietoliikennetiedustelua koskevalla sääntelyllä ei siirretä tiedonsiirtäjinä pidettäville yrityksille tai muillekaan yrityksille sellaisia velvoitteita, jotka kuuluvat viranomaiselle. Tiedonsiirtäjiin kohdistuva avustamisvelvollisuus määriteltäisiin tarkasti ehdotettavassa sääntelyssä.

Lainsäädäntötyötä edeltäneen tiedonhankintalakimietinnön yhteydessä selvitettiin tietoliikenteeseen kohdistuvan tiedustelun mahdollisia kielteisiä vaikutuksia Suomeen kohdistuviin investointeihin. Vaikutuksia todettiin olevan vaikea arvioida, mutta vertailukohteena käytettiin tietoliikennetiedustelusta varsin yksityiskohtaisesti ja julkisesti säätänyttä Ruotsia. Selvityksessä ei havaittu sellaista poikkeamaa ulkomaisten investointien yleisessä kehityksessä, joka voitaisiin selittää Ruotsin tietoliikennetiedustelua koskevan lainsäädännön vaikutuksella. Selvityksen mukaan lain voimaantulolla ei ole selkeää merkitystä Ruotsiin suuntautuneiden ulkomaalaisten investointien kehitykselle verrattuna Suomeen ja Tanskaan. Ruotsi on menestynyt esimerkiksi Data Center Risk Index -vertailussa Suomea paremmin. Samoin Suomeen kohdistuu edelleen lainsäädäntötyön ollessa meneillään uusia datakeskusinvestointeja.

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.

Vaikutukset tutkimus- ja kehitystoimintaan sekä uuden yritystoiminnan syntyyn

Tehokkaasti ja luotettavasti toimiva tiedustelujärjestelmä edellyttää viranomaisilta investointeja tiedustelussa käytettävään teknologiaan ja osaamiseen. Tiedonhankintatoimivaltuudet edel-

lyttävät teknologiainvestointeja ja panostamista turvalliseen tuotekehitykseen. Toiminnan luonteen vuoksi investoinneissa on huomioitava erityisesti hankittavan teknologian turvallisuus sekä järjestelmien toiminnan kannalta olennaiset huoltovarmuuskysymykset. Samoin on tarpeen huomioida mahdollisuudet sopimusperusteisen palvelutuotannon hyödyntämiseen, sillä teknologista osaamista ja resursseja on väistämättä tarpeen hankkia myös yksityiseltä sektorilta. Tämä voi tarkoittaa nopeasti kehittyvän digitaalisen teknologian oloissa uusien liiketoimintamallien, työpaikkojen ja osaamisen syntymistä Suomeen.

4.3 Vaikutukset viranomaisten toimintaan

Siviilitiedustelulainsäädäntö parantaisi mahdollisuuksia hankkia tietoja kansallisen turvallisuuden suojaamiseksi ja parantaisi tätä kautta ylimmän valtionjohdon mahdollisuuksia saada tietoa turvallisuusympäristössä tapahtuvista muutoksista ja kansallista turvallisuutta uhkaavista toiminnoista. Suojelupoliisin ohella paranisi muiden kansallista turvallisuutta ylläpitävien viranomaisten sekä muiden suojelupoliisin yhteistyöviranomaisten tiedonsaanti tarpeellisista tiedoista niiden tehtävien suorittamiseksi. Muutos ei kuitenkaan merkittävästi muuttaisi olemassa olevaa viranomaisyhteistyötä tai menettelytapoja.

Suojelupoliisin ja sotilastiedusteluviranomaisten yhteistyö kuitenkin tiivistyisi nykyisestä, kun niille säädettäisiin samansisältöisistä tiedustelutoimivaltuuksista ja yhteistyöstä tiedustelutoiminnassa säädettäisiin myös laintasolla. Suojelupoliisin ja sotilastiedusteluviranomaisten yhteistyö edellyttäisi käytännön operatiivisen yhteistyön lisäksi myös esimerkiksi yhteistä koulutustoimintaa ja operatiivisten menettelytapojen yhtenäistämistä. Yhteistyö olisi tiivistä erityisesti tietoliikennetiedustelussa, koska sen tekninen toteutus olisi ehdotettu tehtäväksi puolustusvoimien tiedustelulaitoksessa.

Lisäksi sekä suojelupoliisin että sotilastiedusteluviranomaisen suorittamaa tiedustelua varten perustettaisiin oikeusministeriön tähän esitykseen liittyvässä esityksessä ehdotettavalla tavalla uusi laillisuusvalvonnan viranomainen. Oikeusministeriön esityksessä käsitellään tarkemmin tiedustelun valvonnan vaikutuksia viranomaisten toimintaan. Eduskunnan pääsihteerin asettamassa työryhmässä valmistellaan esitys tiedustelutoiminnan parlamentaarisen valvonnan järjestämisestä.

Ehdotuksen laajimmat viranomaisvaikutukset kohdistuisivat suojelupoliisin tehtäviin ja menettelytapoihin. Suojelupoliisista tulisi ehdotuksen myötä siviilitiedusteluviranomainen eli viranomainen, jolle säädettäisiin oikeus käyttää tiedustelumenetelmiä tiedon hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta sekä kotimaassa että ulkomailla. Tästä tehtävämuutoksesta aiheutuvia toiminnallisia, koulutuksellisia, järjestelmä- ja menetelmäkehityksellisiä ja laillisuusvalvonnallisia vaikutuksia suojelupoliisin työhön sekä siitä suoriutumiseksi tarvittavaa henkilöstömäärää ja muita voimavaratekijöitä arvioidaan tarkemmin taloudellisia vaikutuksia koskevassa jaksossa.

Poliisilain 5 a luvun mukaisia tiedustelumenetelmiä ja tietoliikennetiedustelua koskevat lupaasiat ratkaistaisiin Helsingin käräjäoikeudessa. Tiedustelusta säätäminen tulisi lisäämään tuomioistuimelle osoitettavien lupavaatimusten määrää. Tiedonhankinnan alan laajentumisen ohella lupavaatimusten määrää on omiaan lisäämään se, että tuomioistuimen päätösvaltaan kuuluisi täysin uusia tiedustelumenetelmiä (paikkatiedustelu ja tietoliikennetiedustelu).

Ehdotettava lainsäädäntö sisältää toisaalta useita sellaisia ratkaisuja, jotka ovat omiaan rajoittamaan lupavaatimusten määrän lisääntymistä. Yksi tällainen tekijä on se, että uhkat, joista tiedustelumenetelmillä saataisiin hankkia tietoa, on ehdotettu määriteltävän tyhjentävästi ja sangen tiukasti. Perusteuhkien ala on joiltain osin merkittävästikin suppeampi kuin suojelupo-

liisin lakisääteinen toimiala. Suojelupoliisi esimerkiksi estää ja paljastaa kotimaisten ääriliikkeiden rikoksia, mutta tiedustelulla ei ole tarkoitus hankkia tietoja tällaisten tahojen toiminnassa. Toinen lupavaatimusten määrän suhteellista kasvua vaimentava tekijä on se, että lupien enimmäisvoimassaoloajat olisivat merkittävästi pidempiä kuin poliisilain 5 luvun nojalla myönnettävien vastaavien lupien. Sekä poliisilain 5 a luvussa säädettäviä tiedustelumenetelmiä että tietoliikennetiedustelua koskevien lupien enimmäisvoimassaoloaikana olisi kuusi kuukautta poliisilain 5 luvun salaisille tiedonhankintakeinoille säätämän yhden kuukauden sijaan. Pitkäaikaisessa tiedusteluoperaatiossa saattaa näin ollen tulla vuoden aikana esitettäväksi vain kaksi lupavaatimusta sen sijaan, että niitä esitettäisiin - jos luvan enimmäisvoimassaoloaika olisi sama kuin 5 luvussa - kaksitoista. Kolmas lupamäärän kasvua hillitsevä tekijä on se, että telekuuntelu- ja televalvontalupia voitaisiin hakea paitsi yksittäiseen teleosoitteeseen tai telepäätelaitteeseen, myös henkilöön. Jos luvan voimassaoloaikana tulisi tietoon luvan kohdehenkilön käyttämiä uusia teleosoitteita tai -päätelaitteita, ei niitä varten olisi tarpeen hakea uutta lupaa tuomioistuimelta.

Edellä sanotun lisäksi on syytä huomioida, että poliisilain 5 a luvun nojalla tulevaisuudessa suoritettava tiedustelu saattaa jossain määrin vähentää tarvetta 5 luvun mukaisten salaisten tiedonhankintatoimivaltuuksien käyttöön tai ainakin hillitä niiden käytön kasvua. Kyse ei ole siirtymästä siinä mielessä, että sellainen vaatimus, joka nykyisin esitetään 5 luvun perusteella, esitettäisiin tulevaisuudessa 5 a luvun perusteella. Ennemmin kyse on siitä, että varhaisvaiheen tiedonhankinta ja sen mahdollistamat torjuntatoimet saattavat vähentää vaaraa, että tiedonhankinnan kohdetoiminta ylipäätään konkretisoituu sellaiseksi estettäväksi rikokseksi, johon olisi tarpeen kohdistaa 5 luvun mukaisia menetelmiä. Myös ulkomaan tiedustelusta säätäminen on omiaan vähentämään vaaraa siitä, että tiedustelun kohteena oleva toiminta siirtyy Suomeen ja konkretisoituu estettäväksi rikokseksi. Tiedustelusta säätämisen ja siitä riippumattoman toimintaympäristön muuttumisen vaikutuksia tosin on vaikea erottaa toisistaan.

Ehdotukseen sisältyy säännös tiedustelumenetelmien käytön valvonnasta ja delegointisäännös valtioneuvoston asetuksella annettavista tarkemmista säännöksistä. Asetuksella asetettaisiin tiedustelumenetelmiä koskevat tarkemmat kirjaamis-, pöytäkirjaamis-, raportointi- ja valvontavelvoitteet. Tältä osin ei olisi nähtävissä mainittavaa muutosta nykyisiin menettelytapoihin, koska tiedustelumenetelmiä koskien esitettäisiin asetustasolla säädettäväksi vastaavalla tavalla kuin salaisia tiedonhankinta- ja pakkokeinoja koskien.

4.4 Yhteiskunnalliset vaikutukset

Kansalaisten asema yhteiskunnassa ja kansalaisyhteiskunnan toiminta

Siviilitiedustelulainsäädännöllä puututtaisiin perustuslaissa ja kansainvälisissä ihmisoikeusvelvoitteissa suojattuihin oikeushyviin, erityisesti yksityiselämän suojaan ja luottamuksellisen viestin salaisuuteen. EIT on katsonut ratkaisukäytännössään, että luottamukselliseen viestintään puuttumisen mahdollistava sääntely jo itsessään rajoittaa jokaiselle EIS 8(2) artiklan nojalla kuuluvaa oikeutta siitä riippumatta, onko tiedonhankintatoimenpiteitä tosiasiassa käytetty vai ei (Liberty and others, kohta 56 ja Weber and Saravia, kohta 78). Ehdotus rajoittaisi näin ollen yksittäisen kansalaisen perustuslain 10 §:ssä ja EIS 8(2) artiklassa turvattua yksityiselämän suojaa ja luottamuksellisen viestin salaisuutta.

Ehdotuksessa esitetty toimivaltuussääntely on edellä mainituista syistä laadittu tarkkarajaiseksi ja täsmälliseksi, mikä merkitsee sitä, että sen soveltaminen on kansalaisten näkökulmasta ennakoitavaa. Sääntelyn tarkoituksena on suojata kansallista turvallisuutta, millä on myönteisiä vaikutuksia yksittäisten kansalaisten turvallisuuteen. Ehdotus on laadittu suhteellisuusperi-

aate, vähimmän haitan periaate ja tehokkaita oikeusturvajärjestelyjä koskevat vaatimukset huomioiden.

Ehdotuksella ei olisi vaikutuksia kansalaisten osallistumis- tai vaikuttamismahdollisuuksiin yhteiskunnassa, kuten poliittiseen puoluetoimintaan tai ammatilliseen tai muuhun järjestö- ja yhdistystoimintaan.

Perus- ja ihmisoikeuksiin liittyviä kysymyksiä käsitellään tarkemmin jäljempänä suhdetta perustuslakiin ja säätämisjärjestystä koskevassa jaksossa.

Rikostorjunta ja turvallisuus

Tiedustelun ja rikostorjunnan, erityisesti rikosten selvittämisen, tarkoitukset eroavat toisistaan. Tiedustelun tarkoituksena ei ole toteuttaa rikosvastuuta vaan tukea ylimmän valtiojohdon päätöksentekoa sellaisten tietojen avulla, jotka eivät ole saatavissa muulla tavalla. Lisäksi tiedustelun tarkoituksena on mahdollistaa kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitseminen ja torjunta mahdollisimman varhaisessa vaiheessa.

Tiedustelutoiminnalla voidaan olettaa saatavan tietoa paitsi uhkista niin myös sellaisista rikoksista, jotka vaarantavat kansallista turvallisuutta, kuten esimerkiksi terrorismirikoksista. Silloin kun tiedonhankinnassa ilmenisi kansallista turvallisuutta uhkaavia tai muita vakavia rikoksia, suojelupoliisin olisi ilmoitettava niistä toimivaltaiselle viranomaiselle tai esitutkintaviranomaiselle. Suojelupoliisi saisi lisäksi luovuttaa esitutkintaviranomaiselle tietoa erikseen säädettäväksi ehdotetulla tavalla rikosten estämiseksi ja selvittämiseksi.

Ehdotuksen voidaan olettaa edistävän esitutkintaviranomaisten mahdollisuuksia saada tietoa ainakin kaikkein vakavimmista rikoksista. Ehdotuksen rikostorjunnallinen vaikutus ilmenisi myös toimivaltaisen viranomaisen parantuneina mahdollisuuksina estää niitä. Uudella lainsäädännöllä pystyttäisiin yksittäistapauksissa paremmin estämään tilanteen kehittyminen vakavan rikoksen valmistelusta sen täytäntöön panemiseen.

Tietoyhteiskuntavaikutukset

Siviilitiedustelulainsäädännöllä on nähtävissä sekä suoria että välillisiä tietoyhteiskuntavaikutuksia, jotka aiheutuvat ennen muuta ehdotetusta uudesta tietoliikennetiedustelutoimivaltuudesta. Poliisilakiin ehdotetuista uusista tiedustelutoimivaltuuksista aiheutuva vaikutus on vähäisempi, sillä digitaaliseltaluonteeltaan ne ovat samoja keinoja, joista säädetään poliisilain 5 luvussa salaisina tiedonhankintakeinoina (telekuuntelu, tietojen hankkiminen telekuuntelu 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 lainsäädäntöhankeen johdosta aiheutunut julkinen keskustelu.

Tieto- ja viestintäteknologian yritysten kilpailukykyyn aiheutuvat vaikutukset sivuavat tietoyhteiskuntavaikutuksia. Niistä on tässä luvussa käsitelty vain suorat vaikutukset. Epäsuorat yritysvaikutukset on käsitelty kansantaloudellisten vaikutusten yhteydessä.

Tietoliikennetiedustelun vaikutukset tietoyhteiskunnan palveluiden käyttäjiin

Tietoliikennetiedustelulla arvioidaan olevan vaikutuksia tiedustelun kohteen kannalta sivullisten henkilöiden luottamuksellisen viestinnän suojaan. Puuttumisen intensiteettiä on lainsäädäntöteknisillä valinnoilla pyritty rajaamaan niin, ettei kenenkään oikeuksiin puututtaisi enempää kuin on välttämätöntä.

Tietoliikennetiedustelu olisi toteutettava liikenteen solmukohdassa tapahtuvana tietoliikenteen suodatuksena. Tehokkaan tietoliikennetiedustelun edellytyksenä on, että suodatusjärjestelmä näkee mahdollisimman suuren osan tiedustelun kohteen kannalta olennaisesta tietoliikenteestä. Tästä toisaalta seuraa, että suodatusjärjestelmän läpi virtaa myös sivullista tietoliikennettä.

Vaikka tietoliikennetiedustelua käytetään ainoastaan valtakunnan rajat ylittävään tietoliikenteeseen, tietoliikennetiedustelun suodatuksen piiriin voi internetin toimintatavan vuoksi päätyä myös maan sisäistä tietoliikennettä. Esimerkiksi ruuhka- tai vikatilanteessa yhteys kahden Suomessa olevan osapuolen välillä saattaa reitittyä ulkomailla sijaitsevan reitittimen kautta. On mahdollista, että automaattisesti erotellun tietoliikenteen jatkokäsittelyssä selviää tietoliikenteen kotimainen luonne. Ehdotukseen on edellä sanotusta johtuen otettu kotimaista viestintää koskeva tiedustelukielto ja velvollisuus hävittää tällainen viestintä heti, kun se on havaittu.

Vaikutukset tietoturvallisuuteen sekä kriittisen tietoinfrastruktuurin suojaan

Tietoliikennetiedustelulla arvioidaan olevan positiivinen vaikutus tietoturvallisuuteen sekä kriittisen infrastruktuurin suojaan Suomessa.

Tiedon turvaaminen sekä tietoturvapoikkeamien havainnointi on yleisesti tehokkainta toteuttaa mahdollisimman lähellä suojattavaa tietoa. Sähköisen viestinnän palveluista annetun lain 272 § säädetään teleyrityksen, yhteisötilaajan ja lisäarvopalvelun oikeuksista ryhtyä toimenpiteisiin viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi. Suuressa osassa tietoturvallisuutta loukkaavista tapahtumista sähköisen viestinnän palveluista annetun lain mahdollistamat torjuntatoimenpiteet toimivat hyvin, sillä määrällisesti suurin osa tietoturvapoikkeamista toteutetaan automatisoituina hyökkäyksinä, jolloin myös torjuntatoimet voidaan tehokkaasti automatisoida. Tilanne on kuitenkin kokonaan toinen sellaisen valtiotaustaisen kybervakoilun osalta, jota ei toteuteta massana automatisoidusti, vaan kohdentaen hyökkäykset tarkasti käsin.

Kybervakoilun havaitseminen sähköisen viestinnän palveluista annetun lain 272 § säädetyin toimenpitein on osoittautunut epätodennäköiseksi. Nykytilanteen ongelmallisuus on tunnistettu selkeästi tuoreessa tutkimusjulkaisussa, jossa todetaan, että kybervakoilun havaitseminen on kansallinen sokea piste. Tietoriskien hallinta on kokonaisuudessaan muuttunut aiempaa monimutkaisemmaksi. Organisaation toiminnan kannalta kriittinen tieto on usein pitkien alihankintaketjujen kautta useiden eri toimijoiden hallussa. Vaikka kukin palvelutuottaja sinänsä hoitaisi tiedon teknisen suojauksen huolellisesti ja vaikka palvelusopimukset olisi laadittu taiten, tietohallintonsa ulkoistaneiden organisaatioiden ei ole enää teknisesti mahdollista itse havaita tietonsa käsittelyyn liittyviä poikkeamia. Ammattitaitoinenkaan palveluntarjoaja taas ei pysty tunnistamaan poikkeamaksi sellaista tapahtumaa, jonka merkityksen voi ymmärtää vain tuntemalla syvällisesti asiakasorganisaation toimintaa. Kokonaisvastuu tiedon turvaamisesta säilyy silti organisaatiolla itsellään, eikä kansallista turvallisuutta uhkaavien tietoriskien havaitsemiskyvyn parantaminen muuta tilannetta.

LUONNOS

Samaan aikaan, kun poikkeamien havaitsemisen edellytykset ovat jopa heikentyneet, on tiedon merkitys tietoyhteiskunnan keskeisimpänä tuotantotekijänä kasvanut. Tiedon eheys, luottamuksellisuus sekä saatavuus ovat nykyään niin olennaisia turvattavia intressejä, että koko yhteiskunnan on osallistuttava niiden suojaamiseen omalla sektorillaan. Tiedon omistavien organisaatioiden, ICT-palveluntarjoajien sekä tietoturvapalveluita tuottavien yritysten tietoturvatoiminnan lisäksi tarvitaan tehokkaasti toimivia viranomaisia, joilla on edellytykset havaita ja torjua Suomeen kohdistuvia uhkia. Viestintäviraston kyberturvallisuuskeskus tekee arvokasta tietoturvatyötä yritysten ja julkishallinnon tukena. Se ei kuitenkaan vielä riitä, vaan sen lisäksi tarvitaan parempi kyky tunnistaa myös tarkasti kohdennettuja valtiotaustaisia kyberuhkia jo ennen kuin niiden toteutus on käynnistynyt. Tietoliikennetiedustelu parantaisi toimivaltaisten viranomaisten edellytyksiä havaita sekä kriittiseen infrastruktuuriin kohdistuvaa kyberkartoitusta että valtiollista kybervakoilua, joka kohdistuu ulkomailta korkean teknologian tutkimus- sekä tuotekehitystietoon Suomessa.

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

Poliisilain 5 a lukuun esitetyt tiedustelumenetelmillä (telekuuntelu, tietojen hankkiminen telekuuntelun sijasta ja televalvonta) olisi vaikutuksia tietoyhteiskunnan palveluntarjoajista ainakin teleyrityksiin, joilla on velvoite avustaa viranomaista teletiedustelumenetelmiä koskevien kytkentöjen toteuttamiseksi. Teleyritysten työmäärä lisääntyisi, mutta työmäärän kasvua olisi omiaan hillitsemään lupa-aikojen pidentyminen. Teletiedustelumenetelmiä koskeva lupa voitaisiin myöntää kuudeksi kuukaudeksi kerrallaan. Tämä vähentäisi pidempikestoisessa tiedusteluoperaatiossa teleyrityksille aiheutuvaa henkilöresurssikuormitusta suhteessa siihen, että luvat olisivat ajalliselta kestoltaan 5 luvun mukaisia. Siinä missä 5 luvun mukaisella luvalla toteutettu telekuuntelu edellyttää teleyritykseltä kytkentätoimenpiteitä kuukauden välein, ehdotettujen toimivaltuuksien myötä teleyritykseltä tarvittaisiin toimenpiteitä kuuden kuukauden välein.

Uuden tietoliikennetiedustelun vaikutus tietoyhteiskuntapalveluiden tarjoajiin on suurempi, sillä vastaavaa sääntelyä ei tällä hetkellä ole. Vaikutukset kohdistuisivat yksinomaan niin sanottuihin tiedonsiirtäjiin, joilla tarkoitettaisiin tahoja, jotka omistavat tai hallitsevat viestintäverkon sitä osaa, joka ylittää Suomen rajan. Tällaisia yrityksiä arvioidaan nykyisin olevan kymmenkunta. Tietoliikennetiedustelulainsäädännöllä asetettaisiin velvoitteita, joista aiheutuvat välittömät kustannukset mukaan lukien henkilöstökustannukset kuitenkin korvattaisiin valtion varoista.

Tietoliikennetiedustelua koskevassa sääntelyssä ei ehdoteta edellä mainituille tiedonsiirtäjille eikä muillekaan yrityksille velvoitteita heikentää ohjelmistotuotteidensa tai tietoyhteiskunnan palveluidensa asiakaslupausta esimerkiksi salausavaimien luovuttamisen, takaporttien asentamisen tai salaustuotteiden käyttöön liittyvien rajoitteiden muodossa.

Tietoliikennetiedustelun kohdistuminen viestintäverkon tietoliikenteeseen

Viestintäverkoissa liikkuvan tietoliikenteen määrästä on vaikea saada tarkkaa kuvaa. Kulloisenakin hetkenä viestintäverkoissa liikkuvaan tiedon määrään vaikuttaa muun muassa se, mi-

LUONNOS

ten tietoliikenne liikkuu muissa osissa globaalia viestintäverkkoa, esimerkiksi internet-verkossa tietoliikenne ohjautuu sitä kautta, mistä se pääsee nopeimmin määränpäähänsä.

Kulloisenakin hetkenä tarkin kuva viestintäverkon osassa liikkuvasta tietoliikenteen määrästä on viestintäverkon osaa hallinnoivalla taholla, käytännössä viestintäverkon osan omistajalla tai esimerkiksi yksittäisen kuidun vuokranneella taholla. Näitä tietoja ei kuitenkaan ole saatavilla niiden ollessa yrityssalaisuuden piirissä.

Tietoliikennemääriä voidaan kuitenkin arvioida lähialueiden internet-verkon tietoliikenteen yhdyspisteitä (internet exchange, IX) ylläpitävien tahojen julkaisemista tilastoista. Keskeisten yhdyspisteiden kautta kulkee vain osa tietoliikenteestä, mutta tilastojen perusteella voidaan arvioida Suomesta lähtevän ja Suomeen saapuvan tietoliikenteen määräksi 1 terabittiä sekunnissa ja Suomen kautta kulkevaksi tietoliikenteen määräksi tilanteesta riippuen 5-10 terabittiä sekunnissa.

Tietoliikennetiedustelussa tiedustelu kohdennettaisiin tuomioistuimen luvassa määrättyihin viestintäverkon osiin, kuten Suomen rajan ylittävän valokaapelin sisältämään yksittäiseen kuituun, kuituparin tai aallonpituuteen. Suomen rajat ylittävissä valokuitukaapeleissa kuituparien määrä tyypillisesti vaihtelevat alle kymmenestä kuituparista jopa satoihin kuitupareihin. Yksittäisen kuituparin sisällä voidaan aallonpituusteknologialla välittää nykyisin yleisesti käytössä olevalla tekniikalla noin 90 aallonpituutta eli kanavaa. Yksittäisellä kanavalla voidaan välittää 100-400 gigabittiä sekunnissa (Gbit/s) liikennettä riippuen käytettävissä olevasta teknologiasta ja siirtoyhteyden pituudesta. Yhden kuituparin osalta maksimivälityskyky vaihtelee, mutta voi olla tyypillisesti nykyisin käytössä olevalla tekniikalla noin 18 terabittiä sekunnissa (Tbit/s) kansainvälisissä yhteyksissä. Yksittäisen valokaapelin maksimivälityskyky riippuu siinä käytössä olevien kuituparien määrästä.

Edellä sanotusti Suomeen tulevasta ja sieltä lähtevästä sekä Suomen kautta kulkevasta tietoliikenteestä voidaan huomata, että tietoliikennemäärät ovat verraten suuria, vaikka tietoliikennetiedustelu kohdistettaisiinkin aallonpituuteen. Esimerkiksi aallonpituudessa kulkevaan tietoliikennevirrasta voidaan kuitenkin sivuuttaa tiedustelun kannalta epärelevantti tietoliikenne. Suurimpien tietoliikenneverkkoteknologiaa kehittävien yritysten arvioiden mukaan tietoliikenteestä vuonna 2016 noin 66 prosenttia oli videopalveluihin (kuten Netflix, HBO, Youtube) ja musiikkipalveluihin (kuten Spotify) liittyvää tietoliikennettä. Yritysten arvioiden mukaan videokuvan siirto kattaa vuonna 2021 noin 80 prosenttia kaikesta tietoliikenteestä. Lisäksi tietoliikennevirrasta voidaan pois sulkea esimerkiksi verkkokauppojen aiheuttama tietoliikenne, joka kattaa arvioiden mukaan noin 6,5 prosenttia tietoliikenteestä.

Tietoliikennetiedustelu voisi edellä kuvatun pois suljennan jälkeen kattaa noin 15 prosenttia kaikesta tietoliikenteestä, eli käytännössä 15 prosenttia esimerkiksi tietyssä aallonpituudessa liikkuvasta tietoliikenteestä. Tähän osuuteen kohdistettaisiin tuomioistuimen luvassa tarkoitettuja hakuehtoja. Hakuehtojen perusteella voidaan arvioida tapauskohtaisesti valikoituvan noin 0,5 prosenttia tietoliikenteestä, eli noin 0,75 gigabittiä sekunnissa kaikesta tietoliikenteestä.

Hakuehtojen perusteella valikoitunut tietoliikenne analysoitaisiin ja siitä poistettaisiin hetihävittämisvelvollisuuden perusteella tarpeeton tieto. Näin ollen vain pieni osa hakuehtojen mukaisesti tietoliikenteestä loppujen lopuksi tallentuu tiedustelutehtävän perusteella laadittaviin raportteihin ja koosteisiin. Lisäksi tallennettaisiin hakuehtojen mukaisesti tietoliikenteestä edelleen tunnistetietoja ja muita tiedustelutehtävään liittyviä tietoja, joiden perusteella voidaan edelleen kohdentaa tietoliikennetiedustelua ja muuta tiedustelutoimintaa.

4.5 Siviilitiedustelulainsäädännön hyötyjen ja haittojen arviointia

Tiedustelulainsäädännön varaan rakentuvan tiedustelujärjestelmän oikeutus riippuu osin siitä, kuinka hyvin ja millaisin kustannuksin järjestelmä selviytyy sille asetetuista tavoitteista. Tämän oikeutuksen arvioinnissa nousee keskeiseen asemaan tiedustelulainsäädäntöön liittyvien mahdollisten hyötyjen ja haittojen punninta. Kysymys on leimallisesti tilannekohtainen, mutta sen ydinsisältö on muuttumaton: tiedustelujärjestelmän käytöstä aiheutuvia hyötyjä ja haittoja on vertailtava keskenään ja saavutettavien hyötyjen on oltava aiheutuvia haittoja suurempia.

Uhkantorjunta

Tiedustelulainsäädännöllä mahdollistettaisiin ajantasaisen turvallisuustilannekuvan muodostaminen, kansallisen turvallisuuden vakaviin uhkatilanteisiin varautuminen ja uhkien torjunta. Koska tiedustelun perustehtävä liittyy kansanvaltaisen valtio- ja yhteiskuntajärjestyksen, yhteiskunnan perustoimintojen, suuren ihmismäärän hengen tai terveyden sekä kansainvälisen rauhan ja turvallisuuden suojaamiseen niihin kohdistuvilta uhkilta, ensimmäinen ja merkittävin tiedustelusääntelyllä tavoiteltava käytännöllinen hyöty on tällaisten uhkien torjunta. Uhkarealisaation välttämisellä pyritään poistamaan tai ainakin vähentämään toteutuneen uhkan välittömiä ja välillisiä seurauksia. Välittömiä, heti ilmeneviä seurauksia ovat esimerkiksi ihmisten hengen ja terveyden menetykset ja aineelliset vahingot. Esimerkiksi Norjassa heinäkuussa 2011 tehdyn terroristihyökkäyksen seurauksena vaurioituneen hallituskorttelin välittömiksi siivous- ja korjauskuluiksi sekä väistötilojen hankkimisesta ja lisääntyneestä turvallisuusvartioinnista johtuviksi kustannuksiksi on arvioitu 1,45 miljardia Norjan kruunua, mikä vastaa noin 150 miljoonaa euroa (Ministeri Aasrud, Rigmor: haastattelu Aftenpostenissa). Välillisiä, viiveellä kypsyviä seurauksia ovat esimerkiksi vahingot kansainväliselle kaupalle, turismille ja vakuutusalalle, markkinahäiriöt ja kiristävät toimet kriminaali- ja turvallisuuspolitiikassa ja menopuolen lisäykset valtion budjetissa. Esimerkiksi niin sanotun pronssisoturikiistan yhteydessä vuonna 2007 kaatui niin pankkien verkkopalveluita kuin medioiden ja valtion verkkosivuja Viroon kohdistetussa laajamittaisessa verkkohyökkäyksessä. Vaikka kyseisen hyökkäyksen kustannuksista on saatavissa vain vähän tietoa, ilmoitti yksi virolainen pankki noin 1 miljoonan Yhdysvaltain dollarin taloudellisista vahingoista (Herzog, Stephen: Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses).

Rikostorjunta

Tiedustelulainsäädännön oletetaan edistävän esitutkintaviranomaisten ja muiden toimivaltaisten viranomaisten mahdollisuuksia saada tietoa kaikkein vakavimmista rikoksista. Ehdotettavalla sääntelyllä pystyttäisiin yksittäistapauksessa paremmin estämään tilanteen kehittyminen vakavan rikoksen valmistelusta sen täytäntöön panemiseen. Siviilitiedustelulakityöryhmän mietinnössä on arvioitu, että suojelupoliisin tiedustelun yhteydessä ilmenisi joka vuosi kaksi törkeää esitutkintaan johtavaa rikosta ja useampia vielä estettävissä olevia vakavia rikoksia. Toinen, mutta niin ikään tärkeä tiedustelusääntelyn hyöty liittyy näin ollen rikostorjuntaan eli tavoitteeseen estää rikoksia ennalta tai saattaa siihen syylliset rikosvastuuseen. Rikostorjunnalla pyritään vähentämään rangaistavan käyttäytymisen kielteisiä seurauksia, kuten rikoksen uhrin henkilövahinkoja, kärsimystä, esinevahinkoja ja taloudellisia vahinkoja ja valtion kontrollijärjestelmän kustannuksia. Yhden terroristisessa tarkoituksessa tehdyn rikoksen kokonaiskustannukset voivat muodostua kansantaloudellisesti merkittäviksi jopa useisiin miljooniin euroihin.

Yhden terroristisessa tarkoituksessa tehdyn rikoksen kokonaiskustannukset voivat muodostua kansantaloudellisesti merkittäviksi jopa useisiin miljooniin euroihin. Esimerkiksi Ranskassa tapahtuneet terroristi-iskut ovat Ranskan viranomaisten mukaan aiheuttaneet Ranskalle arviol-

ta 750 miljoonan euron menetykset turismin vähentymisenä (Reuters in Paris 23.8.2016). Brysselin terroristi-iskujen arvioitiin maksaneen Belgian taloudelle lähes miljardin verran (Politico 26.7.2016). International Air Transport Association (IATA) toukokuussa 2017 julkaisemassa raportissa esitetyn arvion mukaan Länsi-Euroopassa vuoden 2015 loppupuolella ja vuoden 2016 alkupuolella tehdyt terroristi-iskut heikensivät Euroopan lentoyhtiöiden kansainvälistä matkustajaliikennettä ja heikensivät eurooppalaisten lentoyhtiöiden vuoden 2016 liikevaihtoa noin 2,5 miljardilla dollarilla.

Välittömät kustannusvaikutukset

Tiedustelusääntelyllä tulisi olemaan vaikutuksia valtion talousarvioon. Suojelupoliisin etupainotteisiksi - ennen siviilitiedustelua koskevan lainsäädännön voimaantulovuotta - toimintamenoiksi on arvioitu 12,5 miljoonaa euroa, josta määrästä 9,7 miljoonaa euroa menisi kertaluonteisiin investointeihin. Tätä seuraavina vuosina suojelupoliisin siviilitiedustelusääntelystä ja -kyvystä aiheutuvan lisätoimintamenon on arvioitu asettuvan noin 11 miljoonan euron tasolle. Tällöin menoja selittäisivät ennen kaikkea henkilöstökulut, operatiiviset kehityskustannukset ja tietojärjestelmien ylläpitokulut. Muun poliisin, sisäministeriön ja oikeushallinnon siviilitiedustelusta johtuviksi vuosittaisiksi toimintamenoiksi on arvioitu yhteensä noin 2,6 miljoonaa euroa lain ehdotetusta voimaantulovuodesta alkaen. Ensiksi mainitun toimintamenokokonaisuuden perustana olisi uhkantorjunta ja viimeksi mainitun perustana taas rikostorjunta.

Kokoavia huomioita

Tiedustelulainsäädännön hyödyt on edellä jaoteltu uhkan- ja rikostorjuntaan ja haitat taas toiminnallisiin rajoituksiin ja kärsimyksiin sekä välittömiin kustannusvaikutuksiin. Kun uhkat ovat moninaisia ja ajassa muuttuvia, ovat myös niiden realisoitumisesta aiheutuvat välittömät ja välilliset kustannusvaikutukset laajasti vaihtelevat ja vaikeasti ennakoitavat. Rikostorjunnan hyöty vaihtelee sen mukaan, kuinka monta ja minkä laatuista rikosasiaa tiedustelusta kunakin vuonna erottuisi esitutkintaviranomaisille ja muille toimivaltaisille viranomaisille ilmoitettavaksi. Selvää kuitenkin on, että todennäköisyys torjua kansalliseen turvallisuuteen kohdistuvia vakavia uhkia ja siviilitiedustelun yhteydessä ilmeneviä rikoksia on sitä suurempi, mitä merkittävämmin näitä torjuntakykyjä resursoidaan. Selvää on edeltävien esimerkkien valossa myös, että jo yhdenkin uhan onnistuneella torjumisella säästetyt vahinkokustannukset voivat olla moninkertaiset tiedustelukyvyn vuosittaisiin toimintamenoihin nähden. Tiedustelusääntelyllä ja -kyvyllä saavutettavien hyötyjen voidaan näin ollen ennakoida ylittävän siitä johtuvat haitat paitsi rahamääräisesti hankalasti arvostettavien suojeluintressien ja toiminnallisten rajoitusten välisessä vertailussa, myös taloudellisesti.

5 Asian valmistelu

5.1 Valmisteluvaiheet ja -aineisto

Kyberturvallisuus on ollut esillä jo vuoden 2010 yhteiskunnan turvallisuusstrategiassa (Valtioneuvoston periaatepäätös 16.12.2010). Kyberuhat tunnistettiin yhdeksi mahdolliseksi uhaksi ja tietojärjestelmiin tunkeutumisen todettiin tietyissä olosuhteissa voivan täyttää jopa sotilaallisen voimankäytön tunnusmerkit. Suomen kyberturvallisuusstrategiassa (Valtioneuvoston periaatepäätös 24.1.2013) määritellään keskeiset tavoitteet ja toimintalinjat, joiden avulla vastataan kybertoimintaympäristöön kohdistuviin haasteisiin ja varmistetaan sen toimivuus.

Kyberturvallisuusstrategian linjausten 5 kohdan mukaan sotilaallinen kyberpuolustuskyky muodostuu tiedustelun, vaikuttamisen ja suojautumisen suorituskyvyistä. Suorituskyvyn var-

mistamiseksi kehitetään tiedustelu- ja vaikuttamiskykyä kybertoimintaympäristössä osana muun sotilaallisen voimankäytön kehittämistä.

Tasavallan presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta keskustelivat kokouksessaan 7.11.2013 valtionhallinnon tietoturvallisuudesta sekä laajemmin kyberturvallisuuteen liittyvistä kysymyksistä sekä kansallisen kyberturvallisuuden kehittämistarpeista. Asiaa käsiteltiin aiemmin muun muassa vuoden 2013 toukokuun kokouksessa. Tuolloin käydyn keskustelun ja valtioneuvoston periaatepäätöksenä 24.1.2013 julkaistun Suomen kyberturvallisuusstrategian mukaisesti puolustushallinto on tarkastellut kansainvälisen oikeuden ja kansallisen lainsäädännön soveltuvuutta ja riittävyyttä ja myös eräiden muiden maiden kyberturvallisuuteen vaikuttavaa lainsäädäntöä.

Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi. Tavoitteena oli selvittää turvallisuusviranomaisten tiedonhankintaa koskevat toimintaedellytykset erityisesti kybertoimintaympäristön kautta Suomeen kohdistuvat uhkat huomioon ottaen sekä tiedonhankintaa koskevat nykyiset toimivaltuudet ja niiden kehittämistarpeet. Työryhmän työssä tarkasteltiin sekä siviili- että sotilastiedusteluun liittyviä toimivaltuustarpeita. Siviiliviranomaisten osalta työryhmän työ painottui suojelupoliisin tehtäviin ja toimivaltuuksiin. Työryhmä luovutti mietintönsä puolustusministeriölle 14.1.2015 (Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö). Mietinnössä arvioidaan erityisesti tiedustelua koskevan lainsäädännön kehittämistarpeita.

Tiedonhankintalakityöryhmä esitti, että tiedustelua koskevan säädösperustan luomiseksi käynnistettäisiin yksi tai useampia lainsäädäntöhankkeita, jotka voitaisiin valmistella toimialakohtaisesti. Tulisi myös harkita esimerkiksi parlamentaarista tai muuta poliittisessa ohjauksessa tapahtuvaa valmistelua.

Tiedonhankintalakityöryhmän mietintö lähetettiin lausuntokierrokselle 9.2.2015 ja lausuntoa pyydettiin 150 eri taholta. Lausuntopyyntö oli myös julkisesti saatavilla puolustusministeriön internet-sivuilla. Lisäksi erikseen pyydettiin lausunnot professori Martin Scheininiltä European University Inistitutesta, apulaisprofessori Juha Lavapurolta, Tampereen yliopistosta ja professori Tomi Voutilaiselta Itä-Suomen yliopistosta. Lausunnon antoi 74 tahoa. Näistä on laadittu lausuntotiivistelmä (puolustusministeriön julkaisu FI.PLM.2015-3439). Lausuntopalautteessa 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.

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 sisäministeriö johtaa siviilitiedustelua koskevaa hanketta, puolustusministeriö sotilastiedustelua koskevaa ja oikeusministeriö perustuslain mahdollista muuttamista

koskevaa hanketta. Sotilastiedustelun ja samanaikaisesti sisäministeriössä valmisteltavana olevien siviilitiedustelua koskevien säännösten tulee olla keskenään yhteen sovitettuja.

Sisäministeriö asetti 1.10.2015 hankkeen, jonka tehtävänä on valmistella ehdotukset siviilitiedustelua koskevaksi lainsäädännöksi, jolla luotaisiin säädösperusta ulkomaan henkilötiedustelulle, tietojärjestelmätiedustelulle ja tietoliikennetiedustelulle. Lisäksi tehtävänä on selvittää ja arvioida suojelupoliisin salaisten tiedonhankintakeinojen toimivuutta ja riittävyyttä sekä erilaisia tiedustelutiedon hankintakeinoja vaihtoehtoineen. Samassa yhteydessä valmistellaan muut tarvittavat ehdotukset hankkeeseen liittyvän lainsäädännön muutoksiksi.

Hankkeen keskeisin tavoite on kansallisen turvallisuuden parantaminen. Tavoitteena on valmistella siviilitiedustelua koskevat keskeiset säännökset ja näin parantaa suojelupoliisin tiedonhankintaa poliisin tehtäviin liittyvistä vakavista kansainvälisistä uhista siten, että suojelupoliisilla olisi toimivaltuudet ulkomaan henkilötiedusteluun ja tietojärjestelmätiedusteluun sekä tietoliikennetiedusteluun.

Siviilitiedustelulakityöryhmässä edustettuina olivat jäsenet tasavallan presidentin kansliasta, oikeusministeriöstä, puolustusministeriöstä, sisäasianministeriöstä, suojelupoliisista, poliisihallituksesta, keskusrikospoliisista sekä asiantuntijoina edustajat Elinkeinoelämän keskusliitosta, valtioneuvoston kansliasta, ulkoasianministeriöstä, liikenne- ja viestintäministeriöstä sekä Pääesikunnan tiedusteluosastolta. Työryhmä jätti ehdotuksensa yksimielisenä.

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän 24.9.2014 julkaistussa loppuraportissa (Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportti, Sisäministeriön julkaisu 28/2014) todetaan, että jos suojelupoliisin tehtäviä ja toimivaltuuksia kehitetään merkittävästi tiedustelullisempaan suuntaan, syntyy tarve ulkoisen laillisuusvalvonnan ja parlamentaarisen valvonnan muotojen uudistamiselle. Kyse voisi olla esimerkiksi uusien tuomioistuinlupien edellyttämisestä ja erityisen parlamentaarisen valvontaelimen perustamisesta. Jos suojelupoliisin toiminnan ulkomaantiedustelullisten elementtien merkitys edelleen kasvaa, tulisi siviilitiedustelun ja sotilastiedustelun tehtävien ja toimivaltuuksien sääntelyn, ohjauksen ja valvonnan kehittämisen olla toisensa huomioon ottavaa. Edelleen työryhmän loppuraportissa todetaan, että jos suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, tulisi oikeudenmukaisen oikeudenkäynnin turvaamiseksi harkita suojelupoliisin esitutkintatehtävien ja -toimivaltuuksien rajoittamista. Suojelupoliisi voisi osallistua edelleenkin tarpeen mukaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa.

Oikeusministeriön asettaman asiantuntijatyöryhmän tehtävänä oli selvittää ja valmistella perustuslain tarkistamista siten, että lailla voidaan säätää tarpeelliseksi katsottavien edellytysten täyttyessä kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin suoraan. Valmistelussa oli otettava huomioon Suomen kansainväliset ihmisoikeusvelvoitteet. Työryhmä julkaisi mietintönsä 11.10.2016. Työryhmä ehdotti mietinnössä 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.

Sisäministeriö muodollisesti asetti parlamentaarisen seurantaryhmän tiedustelulainsäädännön uudistamiseen liittyville hankkeille. Ryhmä toimi linkkinä lainsäädäntöhankkeiden ja edus-

kunnan välillä, jotta eduskunta on jatkuvasti tietoinen hankkeiden etenemisestä. Seurantaryhmän toimikausi oli 11.12.2015 - 31.12.2016. Seurantaryhmän toimikautta jatkettiin ja vuoden 2017 loppuun ja sen toimeksiantoa tarkistettiin.

Tiedustelulainsäädännön aiemmissa vaiheissa on havaittu, että tiedustelu vaatii asianmukaista kattavaa, riippumaton ulkopuolista valvontaa. Tämä ilmenee myös EIT:n ratkaisukäytännöstä. Turvallisuusviranomaisten tiedustelun valvonnan järjestämistä varten oikeusministeriö asetti 17.10.2016 työryhmän, jonka tehtävänä on valmistella lainsäädäntö siviili- ja sotilastiedusteluviranomaisten tiedustelutoiminnan valvontaa varten.

5.2 Lausunnot ja niiden huomioon ottaminen

Siviilitiedustelulakityöryhmä luovutti mietintönsä (Siviilitiedustelulainsäädäntö, Siviilitiedustelulakityöryhmän mietintö, Sisäministeriön julkaisu 8/2017) sisäministeri Paula Risikolle 19.4.2017. Työryhmä ehdotti, että säädettäisiin uusi laki tietoliikennetiedustelusta siviilitiedustelussa sekä muutettaisiin poliisilakia niin, että siihen lisättäisiin uusi 5 a luku, jossa säädettäisiin tiedustelumenetelmistä ja niiden käytöstä siviilitiedustelussa. Lisäksi työryhmä ehdottaa muutettavaksi lakia poliisin hallinnosta, lakia henkilötietojen käsittelystä poliisitoimessa, esitutkintalakia, pakkokeinolakia ja lakia oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa.

Ehdotus lähetettiin lausunnolle 24.4.2017. Lausuntoaika oli kahdeksan viikkoa (24.4.–16.6.2017). Lausuntoa pyydettiin seuraavilta tahoilta: Ahvenanmaan hallintotuomioistuin, Ahvenanmaan maakuntahallitus, American Chamber of Commerce in Finland (AmCham Finland), Amnesty International – Suomen osasto, Auktorisoidut lakimiehet, BaseN Oy, Cinia Oy, CSC-Tieteen tietotekniikan Keskus Oy, Oikeuspoliittinen yhdistys Demla ry, DNA Oyj, eduskunnan oikeus-asiamiehen kanslia, Electronic Frontier Finland ry Effi, Elinkeinoelämän keskusliitto EK, Elisa Oyj, Enfo Oyj, Ericsson, FiCix ry, Finnet-liitto ry, Finnvera, FISC, F-Secure Oyj, Fujitsu Finland Oy, Google, Helsingin hallinto-oikeus, Helsingin käräjäoikeus, Huoltovarmuuskeskus, Hämeenlinnan hallinto-oikeus, Ihmisoikeusliitto, Internet-käyttäjät ikuisesti - IKI ry, Invest in Finland, Finpro ry, Itä-Suomen hallinto-oikeus, Julkisalan koulutettujen neuvottelujärjestö JUKO ry, Julkisen sanan neuvosto, Julkisten ja hyvinvointialojen liitto JHL ry, Juridiska Föreningen i Finland, kansalaisyhteiskunnan neuvottelukunta, Kansallinen Kokoomus r.p., Keskuskauppakamari, Keskusrikospoliisi, Korkein hallinto-oikeus, korkein oikeus, liikenne- ja viestintäministeriö, maa- ja metsätalousministeriö, Maahanmuuttovirasto, Microsoft Oy, Nixu Oy, Nokia Oyj, Ohjelmistoyrittäjät ry, oikeuskanslerinvirasto, oikeusministeriö, opetus- ja kulttuuriministeriö, Palkansaajajärjestö Pardia ry, Patria Oyj, Perussuomalaiset r.p, Piraattipuolue r.p., Pohjois-Suomen hallinto-oikeus, Poliisiammattikorkeakoulu, Poliisihallitus, puolustusministeriö, pääesikunta, Rajavartiolaitoksen esikunta, sosiaali- ja terveysministeriö, SSH Secure Communications Oyj, Suojelupoliisi, Suomen Asianajajaliitto, Suomen Erillisverkot Oy, Suomen Internet-yhdistys, Suomen Journalistiliitto, Suomen Keskusta r.p., Suomen Kristillisdemokraatit (KD) r.p., Suomen Lakimiesliitto, Suomen ruotsalainen kansanpuolue r.p., Suomen Sadankomitea ry, Suomen Sosialidemokraattinen Puolue r.p., tasavallan presidentin kanslia, Teknologiateollisuus ry, Telia Finland Oyj, Tieto Finland Oyj, Tieto- ja viestintätekniikan ammattilaiset TIVIA ry, Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry, Tietosuojavaltuutetun toimisto, Tietoyhteiskunnan kehittämiskeskus ry TIEKE, Tulli, Turun hallinto-oikeus, Turvallisuuskomitean sihteeristö, työ- ja elinkeinoministeriö, ulkoasiainministeriö, Vaasan hallinto-oikeus, Valtakunnansyyttäjänvirasto, valtioneuvoston kanslia, valtiovarainministeriö, Vasemmistoliitto r.p., Viestinnän Keskusliitto, Viestintävirasto, Vihreä liitto r.p. (eduskuntaryhmä), ympäristöministeriö.

Pääosa lausunnoista on saatavilla osoitteessa http://valtioneuvosto.fi/hankkeet (hankerekisterinumero SM047:00/2015). Lausuntotiivistelmä julkaistiin 7.9.2017 (Siviilitiedustelulainsäädäntö, Lausuntotiivistelmä, Sisäministeriön julkaisu 21/2017).

Lausuntopyyntö lähetettiin 96 taholle, joista lausunnon antoivat 59 tahoa. Lausuntopyynnön vastaanottajien lisäksi lausuntonsa antoi seitsemän tahoa, joten mietinnöstä saatiin lausunnot yhteensä 66 taholta.

Lausunnoissa työryhmän mietintöä kommentoitiin laajasti. Suurin osa lausunnonantajista piti uutta siviilitiedustelulainsäädäntöä ja siitä säätämistä tarpeellisena ja kannatettavana. Varsin useassa lausunnossa ei niinkään kritisoitu pykäliä, vaan toivottiin täsmentämään niiden perusteluita. Vähemmistö lausunnonantajista suhtautui ehdotukseen kriittisesti.

Lausunnoissa annettu palaute huomioitiin lakien jatkovalmistelussa laajalti. Erityisesti pykälien perusteluja täsmennettiin ja laajennettiin. Tietoliikennetiedustelun kohdistamiseen kiinnitettiin huomiota useissa lausunnoissa ja toivottiin tarkempaa rajausta tai rajatumpaa tekniikkaa. Lausuntojen perusteella tietoyhteiskuntavaikutuksiin laadittiin seikkaperäinen selostus tietoliikennetiedustelun kohdistumisesta viestintäverkon tietoliikenteeseen.

Siviilitiedustelulakityöryhmä ehdotti, että 5 a luvun 3 §:ssä säädettäisiin siviilitiedustelun kohteista. Tietoliikennetiedustelusta siviilitiedustelussa ehdotetun lain 3 § sisältäisi saman kymmenkohtaisen uhkaluettelon. Pykälä on erittäin tärkeä, koska se määrittäisi tyhjentävästi, mistä kansallista turvallisuutta vakavasti uhkaavasta toiminnasta tiedustelumenetelmillä saataisiin hankkia tietoa. Varsin usea taho, kuten oikeusministeriö, Asianajajaliitto, Demla, Suomen journalistiliitto ja Amnesty International Suomen osasto katsoi palautteessaan, että uhkien määrittelyyn ja tarkkarajaisuuteen on edelleen panostettava.

Lausuntopalautteen perusteella tiedustelumenetelmien käytön perusteita täsmällistettiin ja tarkkarajaistettiin niin, että kohteiden muotoiluihin tehtiin täsmentäviä, osin teknisiä, muutoksia. Kritiikkiä saanut pykälän 3 kohta (valtio- ja yhteiskuntajärjestystä uhkaava toiminta) muutettiin kansanvaltaista yhteiskuntajärjestystä uhkaavaksi toiminnaksi. Lisäksi pykälään lisättiin uusi 10 kohta, Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaavasta toiminnasta.

Merkittävin muutos oli se, että pykälässä tarkoitettuja kohtia ei itsessään pidettäisi tiedustelumenetelmän käyttöön oikeuttavina, vaan jokaisen siivilätiedustelun kohteen kohdalla tulisi siviilitiedusteluviranomaisen yksittäistapauksellisesti pystyä osoittamaan, että kyseisessä kohdassa tarkoitettu toiminta muodostaan vakavan uhkan kansalliselle turvallisuudelle. Tämä edellytys ilmenisi 5 a luvun 4 §:n 1 momentista, jonka mukaan: "Tiedustelumenetelmän käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta." Kyse olisi selkeästä käyttöedellytyksestä, joka edellyttäisi myös em. seikkojen olemassaolon perustelemista. Toimivaltuuksien käyttöedellytyksiä muutoinkin täsmällistettiin ja tarkkarajaistettiin annetun palautteen perusteella kirjoittamalla yksityiskohtaisiin perusteluihin siviilitiedusteluviranomaisen harkintavaltaa rajoittavia seikkoja, jotka liittyvät tiedustelutoimivaltuuksien käyttöä ohjaaviin poliisilain alussa säädettyihin poliisioikeudellisiin yleisiin periaatteisiin.

Siviilitiedustelutoimintaan kohdistettavan laillisuusvalvonnan (ja parlamentaarisen valvonnan) osalta useassa lausunnossa käsiteltiin valvonnan tärkeää roolia. Laillisuusvalvonnan ja parlamentaarisen valvonnan tulee olla tehokasta, uskottavaa ja asianmukaisesti järjestettyä. Siviilitiedustelulakityöryhmän ehdotuksessa suojelupoliisin olisi tullut antaa tieto tiedustelun val-

vontaviranomaiselle tuomioistuimen luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen. Kyseinen velvollisuus laajennettiin koskemaan jokaista tiedustelumenetelmän käyttöä koskevaa päätöstä sekä päätöksestä, joka koskee siviilitiedustelun suojaamista, ilmaisukieltoa tai 44 §:n 1 momentissa tarkoitetun ilmoituksen siirtämistä. Myös tarkemmissa säännöksissä esitettyä asetuksenantotoimivaltaa laajennettiin valtioneuvoston osalta koskemaan rikostorjuntaan luovutettavan tiedon siirtämistä koskevaa menettelyä ja siinä yhteydessä annettavia tarpeellisia tietoja, suojelupoliisin ja sotilastiedusteluviranomaisen välisen yhteistyön järjestämisestä, suojelupoliisin ja muiden viranomaisten välisen yhteistyön järjestämisestä, salaisen tiedonhankinnan yhteensovittamisen järjestämisestä, tiedustelutoiminnan yhteensovittamisen järjestämisestä. Sisäministeriön asetuksella voitaisiin säätää siviilitiedustelun valvonnan järjestämisestä sisäasiainhallinnossa, suojelupoliisin ja muun sisäasiainhallinnon välisen yhteistyön järjestämisestä sekä suojelupoliisin kansainvälisen yhteistyön järjestämisestä.

Palautteessa käsiteltiin työryhmän ehdotusta tiedon luovuttamisesta rikostorjuntaan (Poliisilain 5 a luvun 43 §) melko laajasti. Lausuntopalaute pyrittiin ottamaan huomioon ennen kaikkea perustelulausumin, mutta myös pykälään tehtiin muutoksia, jotka liittyvät pykälässä tarkoitettujen ilmoitusten tekemiseen liittyvää harkintaa.

Kysymykset perus- ja ihmisoikeuksien toteutumisesta herätti lausuntopalautetta kokonaisuutena arvioiden jonkin verran keskustelua. Tältä osin erityisesti esityksen jaksoa "Suhde perustuslakiin ja säätämisjärjestys" kiinnitettiin valmistelussa erityistä huomiota, mutta perustuslaillisia kysymyksiä käsitellään laajemmin myös toimivaltuuspykälien yksityiskohtaisissa perusteluissa.

Eräissä lausunnoissa pohdittiin siviilitiedustelun tehokkuutta. Lisäksi esityksen jatkovalmistelun aikana esityksen vaikutuksia koskeva osio esteltiin valtioneuvoston kanslian yhteydessä toimivalle riippumattomalle ja itsenäiselle lainsäädännön arviointineuvostolle. Saadun palautteen perusteella erityisesti tietoyhteiskuntavaikutuksia koskevaa osioon laadittiin arvio tietoliikennetiedustelun kohdistuminen viestintäverkon tietoliikenteeseen. Lisäksi esityksen vaikutuksiin laadittiin uusi jakso, jossa punnitaan siviilitiedustelunlainsäädännön hyötyjä ja haittoja.

Esityksen taloudellisia vaikutuksia koskevaa jaksoa kommentoitiin useassa lausunnossa. Siihen ei kuitenkaan tehty jatkovalmistelun aikana muutoksia.

Siviilitiedustelulainsäädäntöä koskevan ehdotuksen jatkovalmistelussa kiinnitettiin huomiota siviilitiedustelu ja sotilastiedustelua koskevien lakiehdotusten yhdenmukaisuuteen ja niitä yhdenmukaistettiin sisäministeriön ja puolustusministeriön välisessä yhteistyössä kaikilta niiltä osin, joissa tällainen yhteensovittaminen on perusteltua ja sääntelyn selkeyden kannalta toivottavaa.

Annetun palautteen perusteella sekä pykäliin että perusteluihin tehtiin runsaasti teknisiä tarkistuksia, esityksen perusteluja syvennettiin ja laajennettiin esimerkiksi perustuslainmukaisuuden arvioinnissa. Lakiehdotuksiin perusteluteksteihin tehtiin monin paikoin kielellisiä viimeistelyjä.

6 Riippuvuus muista esityksistä

Puolustusministeriössä on vireillä lainsäädäntöhanke, jossa ehdotetaan säädettäväksi laki sotilastiedustelusta. Kyseinen esitys annetaan samaan aikaan tämän esityksen kanssa. Sotilastiedustelua koskeva hallituksen esitys ja tämä esitys liittyvät yhteen erityisesti tiedustelumenetelmiä koskevan sekä niihin liittyvän sääntelyn osalta.

Oikeusministeriössä on valmisteltu esitys perustuslain muuttamisesta koskien luottamuksellisen viestin suojan rajoittamista tiedon hankkimiseksi sotilaallisesta toiminnasta ja muusta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Toteutuessaan kyseinen perustuslain muutos mahdollistaisi siviili- ja sotilastiedustelulainsäädännössä välttämättömistä luottamuksellisen viestin salaisuuden suojaan puuttuvista tiedustelumenetelmistä säätämisen.

Oikeusministeriössä on edellä mainitun lisäksi valmisteltu tähän esitykseen liittyvä esitys tiedustelutoiminnan valvonnasta. Tähän esitykseen sisältyvän poliisilakiehdotuksen 5 a luvun 60 §:ssä säädettäisiin siviilitiedustelun ulkoisesta valvonnasta ja 61 §:ssä tiedusteluvaltuutetulle tehtävistä ilmoituksista sekä tietoliikennetiedustelua siviilitiedustelussa koskevan lakiehdotuksen 25 §:ssä tietoliikennetiedustelun ulkoisesta valvonnasta ja 26 §:ssä tiedusteluvaltuutetulle tehtävistä ilmoituksista. Tiedustelutoiminnan valvonnasta annettavassa lakiehdotuksessa säädettäisiin puolestaan tiedusteluvaltuutetun oikeudesta olla läsnä poliisilakiehdotuksen 5 a luvun 35 §:ssä tarkoitetussa tuomioistuinmenettelyssä.

Sisäministeriö on 28.1.2016 asettanut hankkeen, jonka tavoitteena on uudistaa poliisin henkilötietojen käsittelyä koskeva lainsäädäntö. Poliisin henkilötietolain kokonaisuudistusta koskeva hallituksen esitys on tarkoitus antaa kevätistuntokaudella 2018. Koska uusilla tiedustelutoimivaltuuksilla saataisiin muiden tietojen ohella myös henkilötietoja, ja koska tiedustelutoimivaltuuksia koskeva sääntely tulisi mahdollisesti voimaan ennen uudistettavaa poliisin henkilötietolakia, viimeksi mainittua lakia ehdotetaan tässä esityksessä muutettavaksi.

Esitys liittyy valtion vuoden 2018 lisätalousarvioesitykseen ja on tarkoitettu käsiteltäväksi sen yhteydessä.

LUONNOS

YKSITYISKOHTAISET PERUSTELUT

1 Lakiehdotusten perustelut

1.1 Laki poliisilain muuttamisesta

1 luku **Yleiset säännökset**

1 §. *Poliisin tehtävät.* Pykälän 1 momenttia muutettaisiin niin, että siihen lisättäisiin poliisin tehtäväksi kansallisen turvallisuuden suojaaminen. Näin pykälän 1 momentin ensimmäisen virkkeen mukaan poliisin tehtävänä olisi oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen.

Kansallisen turvallisuuden käsitettä käytetään useissa kansainvälisissä sopimusasiakirjoissa. Kansallinen turvallisuus on yksi niistä perusteista, joka ihmisoikeussopimuksen 8 artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. Valtioilla on varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat uhkaavan kansallista turvallisuuttaan. Myös Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan mukaan kansallinen turvallisuus säilyy yksinomaan kunkin jäsenvaltion vastuulla, vaikka tämä ei aina ole yksiselitteistä.

Kansallisen turvallisuuden käsitteen sisältö on laaja ja osaksi jäsentymätön eikä sen merkityssisältöä ole juuri täsmennetty ylikansallisissa sopimuksissa. Kansallisen turvallisuuden voidaan katsoa tarkoittavan ainakin sitä, ettei sitä uhkaava toiminta kohdistuisi ensisijaisesti kehenkään yksilönä, vaan yleisemmin valtioon tai yhteiskuntaan. Kansallisen turvallisuuden merkityssisältö muuttuu ja muotoutuu yhteiskunnallisen sekä myös maailmanlaajuisen muutoksen mukana. Muun muassa tästä syystä kansallisen turvallisuuden käsite on ja tulee saamaan tarkemman sisältönsä sitä uhkaavan toiminnan kautta. EIT on ratkaisukäytännössään katsonut, että ainakin sotilaallinen maanpuolustus, terrorismin torjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat kansallisen turvallisuuden piiriin (mm. Klass v. Saksa, Weber ja Saravia v. Saksa). Yleisperustelujen kansainvälisessä osiossa käsitellään tähän liittyviä kysymyksiä tarkemmin.

Kansallisessa turvallisuudessa kyse olisi siten eräänlaisesta kollektiivisesta suojeluintressistä, joka saa sisältönsä yksittäisten kansalaisten perusoikeuksista. Kuitenkin yksityishenkilöön hänen virkansa tai asemansa vuoksi kohdistuva väkivallanteon uhka voisi olla säännöksessä tarkoitettua toimintaa, jos sen perusteena on vaikuttaa valtioon tai yhteiskuntaan. Tällainen tilanne voisi olla esimerkiksi silloin, kun uhka kohdistuu valtion ylimpään johtoon. Lisäksi esimerkiksi kansainväliseen kriisinhallinta- tai avunantotehtäviin osallistuviin henkilöihin kohdistuva uhkaava toiminta voisi olla säännöksessä tarkoitettua. Tällaisiin tehtäviin osallistuminen on osa Suomen ulko- ja turvallisuuspolitiikan toteuttamista.

Kansainvälistymisen myötä valtioiden ulkoisen ja sisäisen turvallisuuden välinen raja on muuttunut yhä häilyvämmäksi. Myös uhkien ja riskien rajaaminen alue- tai paikkasidonnaiseksi on entistä vaikeampaa taloudellisten, teknisten ja sosiaalisten järjestelmien valtiorajat ylittävästä luonteesta ja keskinäisriippuvuudesta johtuen.

Toiminta, joka muodostaa uhkan kansalliselle turvallisuudelle voidaan karkeasti jakaa siviililuonteiseen ja sotilaalliseen toimintaan. Täsmällistä jakoa niiden välillä ei kuitenkaan ole mahdollista tehdä, koska sekä sotilaallinen uhka että siviililuontoinen uhkatoiminta voi kumpikin muodostaa uhkan tai vakavan uhkan kansalliselle turvallisuudelle. Uhkatoiminnan jaot-

telu on enemmänkin tarkoituksenmukaisuuskysymys siviilitiedusteluviranomaisen ja sotilastiedusteluviranomaisen tehtävienjaon kannalta. Keskeisiä siviililuontoisia turvallisuusuhkia ovat ainakin terrorismi, ulkovaltojen Suomeen ja sen etuihin kohdistama vakoilu, joukkotuhoaseiden ja kaksikäyttötuotteiden levittämispyrkimykset sekä sellainen kansainvälinen järjestäytynyt rikollisuus, joka pyrkii vaikuttamaan yhteiskunnalliseen päätöksentekoon tai soluttautumaan valtiorakenteisiin. Viime vuosina erityisesti tietoverkkoympäristössä tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion turvallisuudelle ja sen eduille. Kansallista turvallisuutta vakavasti uhkaavasta toiminnasta säädetään tarkemmin 5 a luvun 3 §:ssä.

Kansallisen turvallisuuden suojaaminen kuuluu julkiselle vallalle. Tiedon hankkiminen kansallista turvallisuutta uhkaavasta tai sitä vakavasti uhkaavasta toiminnasta käyttämällä tiedustelutoimivaltuuksia on useissa maissa keskitetty tietyille tiedusteluviranomaisille. Nykyisin suojelupoliisin tehtävänä on muun muassa torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta sekä suorittaa tällaisten rikosten tutkintaa. Suojelupoliisin tehtäväalueelle kuuluvien rikosten estäminen ja paljastaminen kohdistuvat niin varhaisen vaiheen tiedonhankintaan, mitä rikosperusteisilla salaisilla tiedonhankintakeinoilla on mahdollista. Tätä perustelee muun muassa se, että kyseisten rikosten tunnusmerkistön täyttyessä tapahtunut vahinko voisi olla hyvin merkittävä esimerkiksi Suomen ulkomaansuhteille, valtiontaloudelle, ulkomaankaupalle, energiahuollolle tai turvallisuudelle. Näistä syistä myös tiedustelumenetelmien käyttäminen siviilitiedustelussa voisi tulla kysymykseen lähinnä suojelupoliisin toiminnassa. Tämä ilmenee myös jäljempänä lakiehdotuksen 5 a luvussa sekä ehdotettavan poliisin hallinnosta annetun lain 10 §:n 1 momentissa, jonka mukaan suojelupoliisin tehtävänä on sisäministeriön ohjauksen mukaisesti hankkia tietoa kansallisen turvallisuuden suojaamiseksi sekä havaita, estää ja paljastaa sellaisia toimintoja, hankkeita ja rikoksia, jotka voivat uhata valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta yhteiskunnan turvallisuutta uhkaavan toiminnan havaitsemiseksi ja estämiseksi

Poliisilain 1 luvun 1 §:n tehtäväsäännös ei perusta poliisille toimivaltaa eikä poliisi siis voi pelkästään sen perusteella puuttua ihmisten lailla suojattuihin oikeuksiin. Silloin kun poliisi puuttuu henkilön oikeuspiiriin, tulee toimivallan aina perustua nimenomaiseen säännökseen. Näin ollen kansallisen turvallisuuden suojaaminen ei itsessään osoittaisi kuin sen, että suojelupoliisilla olisi lainmukainen ja yhteiskunnallisesti toivottu motiivi menettelylleen. Tämä ei siis vielä sellaisenaan oikeuttaisi puuttumaan ihmisten perusoikeuksiin, vaan sille tulee löytyä toimivaltaperuste laista.

5 luku **Salaiset tiedonhankintakeinot**

5 §. *Telekuuntelu ja sen edellytykset.* Pykälän 1 momentin ensimmäisessä virkkeessä ehdotetaan muutettavaksi telekuuntelun määritelmää, koska voimassa olevan lain määritelmässä viitataan kumottuun viestintämarkkinalakiin.

Ehdotettavan määritelmän mukaan telekuuntelulla tarkoitettaisiin sähköisen viestinnän palveluista annetun lain (917/2014) 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 8 §:ssä tarkoitettujen tunnistamistietojen selvittämiseksi. Telekuuntelua saataisiin kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jonka voidaan perustellusti olettaa syyllistyvän 2 momentissa mainittuun rikokseen.

Muutoksen tarkoituksena ei ole asiallisesti muuttaa telekuuntelun määritelmää tai sen soveltamisalaa, vaan muutos olisi tekninen.

7 §. *Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen.* Pykälän 1 momenttia ehdotetaan muutettavaksi niin, että tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta pakkokeinolain 2 luvun 9 §:n 1 momentin 1 kohdassa tarkoitetun poliisimiehen (pidättämiseen oikeutettu poliisimies) taikka suojelupoliisin päällikön, apulaispäällikön, osastopäällikön, ylitarkastajan tai tarkastajan (suojelupoliisin päällystöön kuuluva poliisimies) vaatimuksesta. Lisäksi 3 momentin 6 kohtaa muutettaisiin niin, että siinä viitattaisiin 1 momentissa tarkoitettuun poliisimieheen.

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän raportin mukaan, jos suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, tulee harkita suojelupoliisin esitutkintatehtävien rajoittamista ja sen esitutkintatoimivaltuuksien rajoittamista tai poistamista. Tätä asiaa käsitellään tarkemmin yleisperusteluissa sekä esitutkinta- ja pakkokeinolain muuttamista koskevan lakiehdotuksen yksityiskohtaisissa perusteluissa.

Esitutkintatoimivallan poistaminen tarkoittaisi myös pakkokeinotoimivaltuuksien rajoittamista tai poistamista, jolloin suojelupoliisissa ei olisi enää pidättämiseen oikeutettuja virkamiehiä eikä myöskään pidättämiseen oikeutettuja poliisimiehiä. Suojelupoliisin päällystöön kuuluvista poliisimiehistä olisi tarpeen ottaa käyttöön uusi termi ”suojelupoliisin päällystöön kuuluva poliisimies”, jolla tarkoitettaisiin suojelupoliisin päällikköä, apulaispäällikköä, osastopäällikköä, ylitarkastajaa tai tarkastajaa.

8 §. *Televalvonta ja sen edellytykset.* Pykälän 1 momentissa ehdotetaan tarkistettavaksi televalvonnan määritelmää, koska voimassa olevan lain määritelmässä viitataan kumottuun sähköisen viestinnän tietosuojalakiin sekä viittausketjun kautta telekuuntelun määritelmäsäännöksessä (5 §) olevaan viestintämarkkinalakiin, joka on myös kumottu.

Ehdotettavan määritelmän mukaan televalvonnalla tarkoitettaisiin 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 tarkoitettaisiin sähköisen viestinnän palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun tilaajaan tai mainitun pykälän 30 kohdassa tarkoitettuun käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Muutoksen tarkoituksena ei ole asiallisesti muuttaa televalvonnan määritelmää tai sen soveltamisalaa, vaan muutos olisi tekninen.

10 §. *Televalvonnasta päättäminen.* Pykälän 1—4 ja 6 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa tarkoitettu suojelupoliisin päällystöön kuuluva poliisimies.

12 §. *Tukiasematietojen hankkimisesta päättäminen.* Pykälän 1 momenttia muutettaisiin niin, että siihen lisättäisiin päätöksentekijäksi suojelupoliisin päällystöön kuuluva poliisimies. Pykälän 3 momentin 5 kohtaa muutettaisiin niin, että tiedonhankinnasta päättävän poliisimiehen osalta viitattaisiin pykälän 1 momenttiin, jolloin vaatimuksessa ja päätöksessä olisi mainittava tukiasematietojen hankkimisen suorittamista johtava ja valvova 1 momentissa tarkoitettu poliisimies. Tämän osalta voidaan viitata 7 §:n perusteluissa esitettyyn.

LUONNOS

14 §. *Suunnitelmallisesta tarkkailusta päättäminen.* Perustelujen osalta voidaan viitata 12 §:ssä esitettyyn.

16 §. *Peitellystä tiedonhankinnasta päättäminen.* Pykälän 1 momenttia muutettaisiin niin, että päätöksentekijäksi lisättäisiin 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies. Hänen tulisi olla myös salaiseen tiedonhankintaan erityisesti koulutettu.

18 §. *Teknisestä kuuntelusta päättäminen.* Pykälän 2 momenttia muutettaisiin niin, että siihen lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies. Pykälän 4 momentin 6 kohtaa muutettaisiin niin, että siinä viitattaisiin teknisen kuuntelun suorittamista johtavaan ja valvovaan 2 momentissa tarkoitettuun poliisimieheen.

20 §. *Teknisestä katselusta päättäminen.* Pykälän 1, 2 ja 4 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

22 §. *Teknisestä seurannasta päättäminen.* Pykälän 1, 2 ja 4 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

24 §. *Teknisestä laitetarkkailusta päättäminen.* Pykälän 1 ja 3 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

25 §. *Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen.* Pykälän 3 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

32 §. *Peitetoiminnasta päättäminen.* Pykälän 1 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

36 §. *Valeostosta päättäminen.* Pykälän 1 ja 3 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

38 §. *Valeoston toteuttamista koskeva päätös.* Pykälän 1 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

39 §. *Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa ja valeostossa.* Pykälän 1 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

40 §. *Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset.* Pykälän mukaan tietolähdetoiminnalla tarkoitettaisiin muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun viranomaisen ulkopuoliselta henkilöltä (tietolähde).

Voimassa olevassa laissa tietolähde voi olla ainoastaan poliisin ja muun esitutkintaviranomaisen ulkopuolinen henkilö. Käytännössä on esiintynyt tulkinnanvaraisuutta sen suhteen, onko muu kuin esitutkintaviranomaisen palveluksessa oleva virkamies rekisteröitävä tietolähteeksi. Siksi määritelmää ehdotetaan täsmennettäväksi mainitulla tavalla, ja tietolähde olisi poliisiviranomaisen ja muun viranomaisen ulkopuolinen henkilö.

42 §. *Tietolähteen ohjatusta käytöstä päättäminen.* Pykälän 1 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

44 §. *Valvotusta läpilaskusta päättäminen.* Pykälän 1 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

47 §. *Suojaamisesta päättäminen.* Pykälän 2 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

48 §. *Salaista tiedonhankintaa koskeva ilmaisukielto.* Pykälän 1 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

52 §. *Tallenteiden tutkiminen.* Pykälään lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

57 §. *Kiireellisessä tilanteessa saadun tiedon hävittäminen.* Pykälään lisättäisiin 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

58 §. *Salaisen tiedonhankintakeinon käytöstä ilmoittaminen.* Pykälän 1 momentista ehdotetaan poistettavaksi suunnitelmallinen tarkkailu ja peitelty tiedonhankinta. Poistaminen johtuu siitä, että pykälän 5 momentin 1. virkkeessä säädetään, ettei suunnitelmallisesta tarkkailusta ja peitellystä tiedonhankinnasta ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa. Saman momentin 2. virkkeessä todetaan, että jos esitutkinta aloitetaan, noudatetaan soveltuvin osin, mitä pakkokeinolain 10 luvun 60 §:ssä säädetään.

Muutoksen tarkoituksena on poistaa pykälän 1 momentin ja 5 momentin välinen käytännön toiminnassa esille tullut tulkintaepäselvyys.

61 §. *Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin.* Pykälän 2 momenttiin lisättäisiin päätöksentekijäksi 7 §:n 1 momentissa määritelty suojelupoliisin päällystöön kuuluva poliisimies.

63 §. *Salaisen tiedonhankinnan valvonta.* Pykälän 2 momenttiin tehtäisiin tekninen tarkistus, jolla sisäasiainministeriö muutettaisiin sisäministeriöksi.

5 a luku **Siviilitiedustelun tiedustelumenetelmät**

1 §. *Siviilitiedustelu.* Pykälässä säädettäisiin siviilitiedustelun määritelmästä. Siviilitiedustelulla tarkoitettaisiin suojelupoliisin suorittamaa tiedonhankintaa ja tiedon hyödyntämistä kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi sekä muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

Sääntelyn tarkoituksena olisi korostaa sitä, että suojelupoliisi olisi ainoa viranomainen, jolla olisi oikeus käyttää tässä luvussa säädettyjä tiedustelumenetelmiä ja hankkia kyseisillä toimivaltuuksilla tietoa kansallista turvallisuutta uhkaavasta toiminnasta. Siviilitiedustelulla ja tiedustelumenetelmillä mahdollistettaisiin suojelupoliisin riittävän tehokas tiedonhankinta kaikkein vakavimmista yhteiskuntaa uhkaavista ilmiöistä ja hankkeista.

Kansallisen turvallisuuden suojaaminen itsessään olisi käsitteenä laajempi kuin suojelupoliisin tiedustelumenetelmien käytön perusteena oleva toiminta, joka potentiaalisesti muodostaa uhkan kansalliselle turvallisuudelle. Kansallisen turvallisuuden suojaaminen käsittäisi suojelupoliisin toimivaltuuksien käytön lisäksi myös toimivaltuuksilla saadun tiedon riittävän tehokkaan hyödyntämisen. Tällä tarkoitettaisiin ainakin sitä, että varmistettaisiin valtion ylimmän johdon päätöksenteon perustuminen oikeaan, ajantasaiseen ja luotettavaan tietoon sekä mahdollistettaisiin muiden toimivaltaisten viranomaisten ryhtyminen uhkien torjuntaan.

Toisaalta kansallisen turvallisuuden suojaamista voitaisiin katsoa olevan myös tiedustelutoiminnan riittävän tehokas valvonta, jottei tiedustelutoiminta muodostuisi epätarkoituksensukaseksi tai tehottomaksi. EIT on painottanut ratkaisukäytännössään viranomaisten salaisten tarkkailutoimivaltuuksien valvontaa, joka tulee järjestää tehokkaasti. Valvontaa ei myöskään voida jättää pelkästään viranomaisen suorittaman sisäisen valvonnan varaan.

Siviilitiedustelun määritelmässä mainittaisiin nimenomaisesti ylin valtionjohto sekä muut kansallisen turvallisuuden viranomaiset. Tällä olisi tarkoitus korostaa suojelupoliisin suorittaman tehtävään liittyvän tiedonhankinnan tarkoitussidonnaisuutta. Siviilitiedustelun tarkoituksena olisi siten suojelupoliisin toteuttamalla tiedonhankinnalla suojata kansallista turvallisuutta joko käyttämällä tietoa itse tai jakamalla tietoa relevanteille muille viranomaisille, joilla on kansallisen turvallisuuden suojaamiseen kuuluvia tai siihen liittyviä tehtäviä. Lisäksi analysoidun tiedon toimittaminen valtion ylimmälle johdolle on jo nykyisinkin suojelupoliisin tehtävänä, mutta nyt se nimenomaisesti mainittaisiin laissa. Kansallisen turvallisuuden suojaamisen lisäksi suojelupoliisi ei saisi käyttää valtuuksiaan muuhun kuin tehtävään nimenomaisesti liittyviin tarkoituksiin. Jäljempänä säädettäisiin poikkeuksista käyttötarkoitussidonnaisuuteen (ks. 44 §).

2 §. *Tiedustelumenetelmät*. Pykälässä säädettäisiin tiedustelumenetelmistä eli niistä tiedustelutoimivaltuuksista, joita suojelupoliisi saisi käyttää siviilitiedustelussa.

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

Perusoikeuksien ja ihmisoikeuksien kunnioittamiseen on tiedustelumenetelmien käytön kohdalla syytä kiinnittää erityistä huomiota. Tiedustelumenetelmillä lähtökohtaisesti puututaan perustuslaissa suojattuihin perusoikeuksiin. Tämä koskee erityisesti yksityiselämän ja luottamuksellisen viestin suojaa. Perus- ja ihmisoikeuksien suojaa on toisaalta punnittava kansallisen turvallisuuden suojaamisintressiä vasten. Sinällään nämä vastinintressit eivät ole toisensa poissulkevia, sillä kansallisen turvallisuuden suojaamisella ja yhteiskunnan kannalta vahingollisten tapahtumien estämisellä suojataan samalla jokaisen perus- ja ihmisoikeuksia. Tiedustelumenetelmän käyttö ei myöskään saisi olla syrjivää eikä sen kohdentaminen saisi perustua esimerkiksi etniseen profilointiin eli siihen, että henkilöstä hankittaisiin tietoa yksinomaan tai pääasiallisesti henkilön etnisen taustan, ihonvärin tai uskonnon perusteella.

Myös muilla poliisioikeudellisilla periaatteilla, suhteellisuusperiaatteella, vähimmän haitan periaatteella ja tarkoitussidonnaisuusperiaatteella, olisi korostunut merkitys tiedustelumenetelmiä käytettäessä. Suhteellisuusperiaate edellyttäisi aina arviointia toimenpiteiden oikeasuhtaisuutta ja siten käytettyjen keinojen ja niillä aiheutettujen haittojen, kuten esimerkiksi yksityisyyden suojaan puuttumisen, tulee aina olla järkevässä suhteessa tavoiteltuun päämäärään nähden. Oikeasuhtaisuus ei siis tarkoita vain sitä, ettei toimenpide saa olla ylimitoitettu tiedustelun kohteensa olevan henkilön näkökulmasta, vaan kyse on myös siitä, että toimenpiteen on oltava riittävän tehokas tavoitellun päämäärän, kuten esimerkiksi tietyn tiedon saamisen, saavuttamiseksi. Suhteellisuusperiaatetta osaltaan ilmentää myös lain 1 luvun 3 §:ssä säädetyn li-

LUONNOS

säksi myös saman luvun 9 §:n 1 momentissa säädetty oikeus luopua toimenpiteestä, jos sen loppuun suorittaminen voisi johtaa kohtuuttomaan lopputulokseen tavoiteltavaan päämäärään nähden.

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

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

Pykälän 1 momentissa lueteltaisiin ne 5 luvussa säädetyt salaiset tiedonhankintakeinot, joiden käyttöedellytyksistä säädettäisiin tässä luvussa tarkemmin. Koska lain 5 luvussa jo säädetään salassa käytettävien tiedonhankintakeinojen määritelmistä, niin määritelmäsäännöksiä ei sellaisenaan olisi tarpeen säätää toistamiseen 5 a luvussa. Siksi 5 a luvussa säädetäisiin ainoastaan kyseisten toimivaltuuksien käyttöedellytyksistä ja tiedustelumenetelmien päätöksenteosta.

Tiedustelumenetelmiä olisivat 5 luvussa tarkoitetut telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja ohjattu tietolähdetoiminta. Valvottua läpilaskua ei edellä mainitussa luettelossa mainittaisi, eikä se olisi tiedustelumenetelmä. Kyseinen toimivaltuus ei sovellu tiedustelutoimivaltuutena käytettäväksi, koska lähtökohtaisesti valvotun läpilaskun kohteena olevan esineen, aineen tai omaisuuden hallussapitämisen tai kuljettamisen perusteella on syytä epäillä rikosta tai jonkun on perusteltua syytä epäillä syyllistyvän rikokseen. Tällöin salaisessa tiedonhankinnassa tulee lähtökohtaisesti käyttää rikosperusteisia tiedonhankintatoimivaltuuksia.

Momentissa ei myöskään mainittaisi järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun osallistumista. Siviilitiedustelussa olisi tarpeen sulkea pois kyseinen toimivaltuus, koska sen soveltaminen siviilitiedustelussa ei tulisi kyseeseen. Järjestäytyneen rikollisryhmän toimintaan ja valvottuun läpilaskuun osallistuminen liittyvät rikosperusteisen peitetoiminnan käyttämiseen. Käytännössä ei kuitenkaan ole mahdollista tehdä kovin jyrkkää eroa sellaisten

henkilöryhmien, joiden toiminta vakavasti uhkaa kansallista turvallisuutta ja sellaisten, joissa tehdään rikoksia, välillä.

Rikoksentekokieltoa sitä vastoin sovellettaisiin siviilitiedustelussa, koska peitetoiminnan perusteena ja tarkoituksena ei ole hankkia tietoa kohdehenkilöiden syyllistymisestä rikoksentekokieltoa koskevassa pykälässä tarkoitettuihin rikkomuksiin. Kyse on siitä, että peitehenkilön voi olla välttämätöntä pystyä tekemään kyseisiä rikkomuksia peitetoiminnan paljastumisen estämiseksi. Paljastumisen estämisintressi ei siten ole kytköksissä siihen kysymykseen, tehdäänkö peitetoimintaa rikostorjuntaa vai siviilitiedustelua varten.

Pykälän 2 momentin mukaan tiedustelumenetelmiä olisivat myös tässä luvussa säädettävät kokonaan uudet toimivaltuudet paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten ja tietojen saanti yksityiseltä yhteisöltä. Kyseisille toimivaltuuksille ei löydy vastinetta 5 luvusta, joten ne olisi tarpeen määritellä tiedustelumenetelmiksi omassa momentissaan.

Pykälän 3 momentin mukaan tässä luvussa säädettäisiin siitä, millä edellytyksillä 1 momentissa tarkoitettuja tiedustelumenetelmiä sekä paikkatiedustelua, jäljentämistä, lähetyksen pysäyttämistä jäljentämistä varten ja tietojen saantia yksityiseltä yhteisöltä käytetään siviilitiedustelussa.

Edellytyksillä viitattaisiin nimenomaan tässä luvussa säädettyihin edellytyksiin ja ilmaisu "millä edellytyksillä" olisi poissulkeva 5 luvun salaisten tiedonhankintakeinojen käyttöedellytyksiin nähden. Asiasta olisi tarpeen säätää, koska 1 momentissa tarkoitettujen tiedustelumenetelmien määritelmäsäännökset ilmenevät 5 luvusta ja käyttöedellytykset sekä päätöksentekosäännökset tästä luvusta.

Tiedustelumenetelmiä tultaisiin käyttämään tiedon hankkimiseksi toiminnasta, joka ei liity rikosepäilyyn. Mikäli jonkin tässä luvussa tarkoitetun toimivaltuuden määritelmäsäännöksessä (5 luku) ilmenisi rikoselementti, niin sitä ei sovellettaisi 5 a luvun tiedustelumenetelmiä käytettäessä, koska tiedustelumenetelmällä ei hankita tietoa rikoksen estämiseksi, paljastamiseksi tai selvittämiseksi. Lisäksi "millä edellytyksillä" viitattaisiin myös toimivaltuuden käytön kohdistamiseen. Tiedustelumenetelmän käyttöä ei olisi myöskään mahdollista kohdistaa aina tiettyyn henkilöön tiedustelutoiminnan luonteen vuoksi, vaan kyseeseen saattaisi tulla myös esimerkiksi myös henkilöryhmä.

Esimerkiksi suunnitelmallisen tarkkailun määritelmästä säädetään 5 luvun 13 §:n 2 momentissa seuraavasti: Suunnitelmallisella tarkkailulla tarkoitetaan muun kuin lyhytaikaisen tarkkailun kohdistamista henkilöön, jonka voidaan perustellusti olettaa syyllistyvän rikokseen. Rikoselementillä tarkoitetaan määritelmän lopussa olevaa relatiivilausetta. Tiedustelumenetelmänä käytettävän suunnitelmallisen tarkkailun käyttöedellytykset ilmenisivät 5 a luvun 4 §:stä sekä 9 §:stä. Ensinnäkin suunnitelmallista tarkkailua käytön edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka uhkaa kansallista turvallisuutta. Siviilitiedustelun kohteista säädetään 3 §:n tyhjentävässä luettelossa. Suunnitelmallisen tarkkailun käytön edellytyksenä on myös, että sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi siviilitiedustelun kohteena olevasta toiminnasta, joka uhkaa kansallista turvallisuutta. Suunnitelmallista tarkkailua koskeva päätös voitaisiin 9:n 2 momentin mukaan tehdä kerrallaan enintään kuudeksi kuukaudeksi. Siviilitiedustelussa suunnitelmallisen tarkkailun kohteena voisi 9 §:n 3 momentista ilmenevällä tavalla henkilön ohella olla myös henkilöryhmä.

Kuten edellä on todettu, niin tiedustelumenetelmien käyttö ei olisi rikossidonnaista 5 luvussa säädetyillä tavoin. Tiedustelumenetelmien käyttöedellytykset määriteltäisiin 5 a luvussa kansallisen turvallisuuden suojaamisen lähtökohdista. Tällä tarkoitetaan ennen kaikkea sitä, että tiedonhankintaintressi suuntautuu kansallista turvallisuutta uhkaavaan tai sitä vakavasti uhkaavaan toimintaan, eikä epäiltyyn tai oletettuun rikokseen ja siihen osallisiin. Lisäksi tiedustelumenetelmien käytön konkreettisista kohteista (esim. henkilö, henkilöryhmä, tila tai muu paikka) säädetään tiedustelumenetelmäkohtaisesti jäljempänä.

Käyttöedellytysten lisäksi tiedustelumenetelmien päätöksentekosäännöksistä säädettäisiin 5 a luvussa. Niiden mukaan tulisi yksittäistapauksellisesti yksilöidä ja perustella tiedustelumenetelmän käytön kohteena oleva toiminta. Tiedustelumenetelmän käytön edellytyksenä ei olisi, että uhkaavan toiminnan taustalla oleva taho olisi tunnistettu sillä hetkellä kun tiedustelumenetelmän käyttöön ryhdytään. Tällä tarkoitettaisiin sitä, että tiedustelumenetelmiä voitaisiin käyttää myös uhkien havaitsemiseksi ja niiden aiheuttajina olevien tahojen tunnistamiseksi. Näin ollen tiedustelumenetelmän kohteena voisi olla henkilö tai henkilöryhmä, jolla voidaan olettaa olevan tietoa kansallista turvallisuutta uhkaavasta toiminnasta. Tiedustelua voitaisiin kohdistaa sekä valtiolliseen että ei-valtiolliseen toimijaan tai sellaiseen henkilöön, joka toimii valtiollisen toimijan puolesta tai hyväksi.

Pykälän 4 momentissa viitattaisiin tietoliikennetiedustelusta siviilitiedustelussa annettavaan lakiin. Tietoliikennetiedustelu olisi myös tiedustelumenetelmä ja suojelupoliisin käytössä oleva siviilitiedustelutoimivaltuus, jolla saataisiin hankkia tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

3 §. *Siviilitiedustelun kohteet.* Pykälässä säädettäisiin siviilitiedustelun kohteista, joista voidaan hankkia tietoa tässä luvussa tarkoitettuja tiedustelumenetelmiä käyttäen. Kyseinen kohdeluettelo olisi tyhjentävä. Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 3 §:ään ehdotetaan otettavaksi samansisältöinen säännös kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Pykälän 1 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi terrorismista.

Terrorismi määritellään yleisesti toiminnaksi, jonka tarkoituksena on pelotella vakavasti väestöä, pakottaa aiheettomasti viranomaiset tai kansainvälinen järjestö johonkin tekoon tai pidättymään jostakin teosta taikka horjuttaa vakavasti jonkin maan tai kansainvälisen järjestön poliittisia, perustuslaillisia, taloudellisia tai sosiaalisia perusrakenteita tai tuhota ne (ks. esim. YK:n turvallisuusneuvoston päätöslauselma 1566 (2004) sekä Euroopan neuvoston puitepäätös 2002/475/YOS). Tiedustelumenetelmillä voitaisiin hankkia tietoa terrorismista ilmiötasolla tai konkreettisten hankkeiden tasolla.

Tietoa voitaisiin hankkia esimerkiksi vierastaistelijailmiöstä (ks. vierastaistelijakäsitteestä YK:n turvallisuusneuvoston päätöslauselma 2178 (2014)) tai sen tukemisesta taikka siitä, mitä suunnitelmia, tavoitteita taikka millainen iskun toteuttamiskyky jollain terroristijärjestön johdolla Suomea koskien on, ketkä henkilöt kytkeytyvät tällaisen järjestön toimintaan ja kuinka heitä ohjataan ulkomailta käsin. Tiedustelumenetelmillä voitaisiin hankkia tietoa myös terrorismiin liittyvästä väkivaltaisesta radikalisoitumisesta. Riittävän aikaisella tiedonhankinnalla tuettaisiin Suomeen tai johonkin vieraaseen valtioon Suomesta käsin tehtyjen terrori-iskujen estämistä sekä Suomessa tai Suomesta käsin tapahtuvan terroristisen toiminnan leviämisen estämistä. Pykälän 2 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi ulkomaisesta tiedustelutoiminnasta.

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, Suomen sotilaallinen valmius, yhteiskunnan kriisinsietokyky, huoltovarmuus sekä korkeateknologia sekä sen tutkimus ja tuotekehitys. Tiedonhankinnan lisäksi vieraiden valtioiden tiedustelutoiminnan päämääränä on vaikuttaa muun muassa edellä mainittuihin kohteisiin liittyvään päätöksentekoon vieraan valtion etujen edistämiseksi tai Suomen tai toisen vieraan valtion vahingoksi.

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. Tietoa voitaisiin hankkia myös esimerkiksi siitä, 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 pyrkivät vieraan valtion tiedustelupalvelulta saamiensa käskyjen tai ohjeiden mukaisesti vaikuttamaan päätöksentekoon Suomen tai toisen vieraan valtion vahingoksi. Tietoa voitaisiin hankkia myös yrityksiin kohdistuvasta tiedustelusta, jonka tavoitteena olisi hankkia yritysten tietopääomaa vieraan valtion haltuun.

Pykälän 3 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi joukkotuhoaseista.

Joukkotuhoaseilla tarkoitetaan aseita, jotka on suunniteltu suurten ihmisjoukkojen tuhoamiseen, kuten esimerkiksi kemialliset aseet, biologiset aseet ja ydinaseet. Tiedustelumenetelmillä voitaisiin tässä tarkoituksessa hankkia tietoa esimerkiksi valmistelusta tai suunnitelmasta valmistaa tai välittää joukkotuhoaseita.

Pykälän 4 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi kaksikäyttötuotteiden vientivalvonnasta annetun lain 2 §:ssä (562/1996) tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä.

Kaksikäyttötuotteilla tarkoitetaan kaksikäyttötuotteiden vientivalvonnasta annetun lain 2 §:n (562/1996) mukaan tuotetta, teknologiaa, palvelua ja muuta hyödykettä, jota normaalin siviililuontoisen käyttönsä tai sovellutuksensa ohella voidaan käyttää joukkotuhoaseiden tai niiden maaliin saattamiseen tarkoitettujen ohjusjärjestelmien kehittelyyn tai valmistukseen taikka jolla voidaan edistää yleistä sotilaallista toimintakykyä. Kaksikäyttötuotteiden vientivalvonnan tärkeimpänä tavoitteena on joukkotuhoaseiden leviämisen estämiseen tähtäävä asesulkupolitiikka.

Kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö voisi ilmetä esimerkiksi kaksikäyttötuotteiden hankkimisena, kauttakuljetuksena tai välityksenä vastoin voimassa olevaa vientivalvontalainsäädäntöä taikka Euroopan unionin rajoittavia toimenpiteitä tai Yhdistyneiden kansakuntien asettamia pakotteita. Tietoa voitaisiin hankkia esimerkiksi ulkomaisen toimijan pyrkimyksistä, suunnitelmista tai valmisteluista hankkia vilpillisesti tai harhauttamalla suomalaiselta yritykseltä kaksikäyttötuotteita EU:n tai YK:n asettamien pakotteiden vastaisesti.

Pykälän 5 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminnasta.

LUONNOS

Perustuslain 2 §:n mukaan valtiovalta Suomessa kuuluu kansalle, jota edustaa valtiopäiville kokoontunut eduskunta. Kansanvaltaan sisältyy yksilön oikeus osallistua ja vaikuttaa yhteiskunnan ja elinympäristönsä kehittämiseen. Kansanvaltaista yhteiskuntajärjestystä uhkaavalla toiminnalla tarkoitetaan kansanvallan sellaisia kumoamis- tai muutospyrkimyksiä, joissa käytetään väkivaltaisia keinoja, niillä uhkaamista, kiristämistä tai muuta valtiosäännön vastaista menettelytapaa. Suomen perustuslain mukaan valtiojärjestyksen perusteisiin kuuluu kansanvaltaisuuden lisäksi valtiosääntö, oikeusvaltioperiaate, valtiollisten tehtävien jako ja parlamentarismi. Valtion oikeusjärjestyksen keskeisen osan puolestaan muodostavat oikeusnormit, joiden avulla ohjataan yhteiskuntaelämää (HE 188/2002 vp, s. 60).

Kansanvaltaista yhteiskuntajärjestystä uhkaava toiminta voisi ilmetä esimerkiksi suunnitelmana käyttää asevoimaa valtionsisäisen vallankaappauksen tai -kumouksen toteuttamiseksi taikka suunnitelmana liittää Suomi vieraan vallan alaisuuteen. Suomen kansanvaltaisuutta 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. 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. Kansanvaltaista yhteiskuntajärjestystä uhkaavana olisi pidettävä myös toimia äänestämisen estämiseksi tai häiritsemiseksi eduskuntavaaleissa tai valittaessa tasavallan presidenttiä.

Pykälän 6 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi toiminnasta, joka uhkaa suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja.

Suuren ihmismäärän henkeä tai terveyttä uhkaavalla toiminnalla tarkoitetaan sellaista toimintaa, jonka potentiaalisten uhrien lukumäärän vuoksi voidaan katsoa kohdistuvan laajemmin yhteiskuntaan tai kollektiiviseen turvallisuuden tunteeseen. Päinvastoin kuin terrorismissa uhkaava toiminta olisi määritelty tahtoneutraalisti siten, että uhkan taustalla olevalla toimijalla ei edellytetä olevan tiettyä tarkoitusta. Uhka voisi muodostua esimerkiksi sytyttämällä tulipalo, räjäyttämällä, levittämällä vaarallista kemikaalia tai muulla vastaavalla yleisvaarallisella toiminnalla. Tietoa voitaisiin hankkia esimerkiksi suunnitelmasta tai muusta valmistelusta, jonka yhteydessä hankitaan räjähdysaineita tai poikkeavalla tavalla kemikaaleja tai aineita, joita voidaan käyttää räjähteen valmistukseen. Koska uhkaavan toiminnan edellytettäisiin kohdistuvan suureen ihmismäärän, ei toiminta, joka uhkaa ainoastaan yksittäistä henkilöä tai vähäistä määrää henkilöitä, voisi olla siviilitiedustelun kohteena nyt kyseessä olevan kohdan nojalla. Yksittäisen henkilön tai suurta vähäisemmän ihmismäärän henkeä tai terveyttä uhkaavassa toiminnassa voisi sen sijaan tapauskohtaisesti olla kyse esimerkiksi 1 kohdan mukaisesta terrorismista tai 3 kohdan mukaisesta valtio- tai yhteiskuntajärjestystä uhkaavasta toiminnasta. Ratkaisevaa tämän kannalta olisi muun muassa uhkaavan toiminnan taustamotiivi ja uhkan kohteena olevan henkilön tai henkilöiden asema valtiollisessa päätöksentekojärjestelmässä.

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 yhteiskunnan elintärkeitä toimintoja uhkaavalla toiminnalla tarkoitettaisiin esimerkiksi niiden merkittävään heikentämiseen tai keskeyttämiseen pyrkivää toimintaa. Toisaalta uhka voisi muodostua aktiivisen toiminnan lisäksi myös laiminlyönnistä tai varsinaisen toiminnan sivuvaikutuksesta, joka voi altistaa Suomen ympäristökatastrofille vaarantamalla ilman tai veden puhtauden tai aiheuttamalla säteilytason nousun. Tietoa voitaisiin hankkia myös esimer-

kiksi toiminnasta, jossa pyritään keskeyttämään tai tuhoamaan sellaisia yhteiskunnalle keskeisiä toimintoja kuten sähköntuotanto, tietoliikenne ja tietojärjestelmät, kuljetuslogistiikka, yhdyskuntatekniikka, elintarvikehuolto tai rahoitus- ja maksujärjestelmä. 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.

Pykälän 7 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi vieraan valtion toiminnasta tai toiminnan valmistelusta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille.

Vieraan valtion vahinkoa aiheuttavalla toiminnalla tarkoitettaisiin esimerkiksi toimintaa, jossa pyritään vihamielisellä tavalla vaikuttamaan Suomen päätöksentekoon. Vieraan valtion vihamielisen vaikuttamisen keinovalikoima voi olla laaja ja se voi vaihdella maailmanpoliittisen tilanteen mukaan poliittisista, taloudellisista ja informaatiovaikuttamisen keinoista aina viranomaistoiminnan taktiseen laiminlyöntiin tai poikkeukselliseen aktivoitumiseen, jolle ei löydy tosiasialliseen toimintaympäristöön liittyvää perustetta.

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 ovat Suomeen kohdistetun informaatiovaikuttamisen takana sekä siitä, mitä tällaisella toiminnalla tavoitellaan.

Pykälän 8 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä.

Kansainvälistä rauhaa ja turvallisuutta uhkaavalla kriisillä tarkoitetaan esimerkiksi jossain vieraassa valtiossa aseelliseksi selkkaukseksi eskaloitunutta tilannetta tai sellaista toimintaa joka vasta ennakoi rauhan rikkoutumisen uhkaa. Uhkaa kansainväliselle rauhalle tai turvallisuudelle voi syntyä aseellisen selkkauksen lisäksi hyvin monenlaisista tekijöistä, kuten väestökehityksestä, valtioiden välisistä muuttoliikkeistä, ruokapulasta tai luonnonvarojen niukkuudesta. Kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi voi aiheutua myös autoritaaristen ja puoliautoritaaristen hallitusten ja hauraiden demokratioiden toiminnoista, joissa ne rajoittavat demokraattisten instituutioiden toimintaa sekä kaventavat perus- ja ihmisoikeuksia. Kansainvälistä rauhaa ja turvallisuutta uhatakseen kriisin on lähtökohtaisesti oltava laajempi kuin vain yhden valtion sisäinen tai sillä on oltava vähintään alueellisia heijastevaikutuksia ympäröiviin valtioihin. Tietoa voitaisiin hankkia esimerkiksi kriisin tai siihen liittyvän vieraan valtion poliittisen tilanteen kehittymisestä sekä siitä mitä turvallisuuspoliittisia seurauksia siitä voisi Suomelle mahdollisesti aiheutua.

Pykälän 9 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi kansainvälistä kriisinhallintaoperaation turvallisuutta uhkaavasta toiminnasta.

Siviilihenkilöstön osallistumisesta kriisinhallintaan annetun lain (1287/2004) 1 §:n mukaan Suomi osallistuu kansainväliseen kriisinhallintaan muun muassa konfliktien ehkäisemiseksi ja rajoittamiseksi, niistä aiheutuneiden tuhojen korjaamiseksi ja yhteiskunnan häiriöttömän toiminnan palauttamiseksi sekä suuronnettomuuden tai luonnonkatastrofin aiheuttamien tuhojen lieventämiseksi. Sotilaallisesta kriisinhallinnasta säädetään sotilaallisesta kriisinhallinnasta annetussa laissa (211/2006).

Tietoa voitaisiin hankkia kriisinhallintaoperaatiota tai siihen osallistuvia henkilöitä uhkaavasta toiminnasta. Tietoa voitaisiin hankkia esimerkiksi kriisinhallintaoperaatioalueen olosuhteista ja alueelle lähetettävän henkilöstön turvallisuuteen vaikuttavista tekijöistä, kuten siitä kohdistuuko kriisinhallintaoperaation Suomesta lähetettyyn väkivaltaisen iskun uhkaa sekä missä, milloin ja kenen toimesta mahdolliset väkivallanteot olisi tarkoitus toteuttaa.

Pykälän 10 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi Suomen kansainvälisen avun antamisen tai muun kansainvälisen toiminnan turvallisuutta uhkaava toiminta.

Valtiot, EU ja kansainväliset järjestöt ovat luoneet erilaisia koordinaatio- ja yhteistyömekanismeja sisäisen turvallisuuden uhkien torjuntaan ja hallintaan. Ne perustuvat kahden- ja monenvälisiin sopimuksiin ja yhteistyörakenteisiin. Tarkoituksena on, että valtiot voivat antaa apua toisille valtioille sekä EU:n ja kansainvälisten järjestöjen käyttöön esimerkiksi terrorismirikoksissa, luonnononnettomuuksissa, katastrofeissa ja muissa hätätilanteissa tai niiden uhatessa. Lissabonin sopimuksessa jäsenvaltioiden yhteisvastuuta vahvistettiin sisällyttämällä Euroopan unionin toiminnasta tehtyyn sopimukseen niin sanottu yhteisvastuulauseke (SEUT 222 artikla) tällaisia tilanteita varten.

Sisäministeriön hallinnonalalla on useita kansainvälisiä ja EU-tason järjestelyitä, joita hyödyntäen poliisi-, pelastus- ja rajaturvallisuusviranomaiset voivat antaa ja vastaanottaa apua sisäistä turvallisuutta koskevien uhkien ja riskien torjunnassa ja hallinnassa. Esimerkkeinä EU-tason lainsäädäntöön perustuvasta yhteistyöstä voidaan mainita unionin pelastuspalvelumekanismi, Euroopan rajaturvallisuusviraston (Frontex) koordinoima yhteistyö sekä niin sanottu Prüm- ja Atlas-yhteistyö, joilla pyritään tehostamaan lainvalvonta- ja poliisiviranomaisten yhteistyötä terrorismin ja rajat ylittävän rikollisuuden torjumiseksi.

Lainkohdassa tarkoitettua kansainvälisen avun antamisen tai muun kansainvälisen toiminnan turvallisuutta uhkaavalla toiminnalla tarkoitetaan sellaista joko vieraan valtion tai yksittäisen toimijan toimintaa tai sen valmistelua, jonka pyrkimyksenä on vahingoittaa esimerkiksi poliisin yhdyshenkilöitä tai muita valtion ulkomaille lähettämiä henkilöitä. Tietoa voitaisiin hankkia siitä, kohdistuuko kansainvälisen avun operaatioihin osallistuviin turvallisuusuhkia.

Pykälän 11 kohdan mukaan tiedustelumenetelmiä saisi käyttää tiedon hankkimiseksi yhteiskuntajärjestystä uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta.

Lainkohdassa tarkoitettua toimintaa voisi olla esimerkiksi kansainvälisen järjestäytyneen rikollisuuden soluttautuminen valtionhallinnon merkittäviin virkoihin ja sitä kautta vaikuttaminen yhteiskunnan kannalta merkittävään päätöksentekoon tai esimerkiksi taloudellisen ja poliittisen vaikutusvallan hankkiminen ostamalla kokonaisuudessaan omistukseensa valtion toiminnalle keskeisestä infrastruktuuria tai yhteiskunnan elintärkeitä toimintoja kuten sähköntuotantoa, jätehuoltoa tai kuljetus- ja huolintayrityksiä.

4 §. *Tiedustelumenetelmien käytön yleiset edellytykset.* Pykälän 1 momentissa säädettäisiin kaikille tiedustelumenetelmille yhteisestä yleisestä käyttöedellytyksestä "voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta". Kyse olisi perustelua edellyttävästä tuloksellisuusvaatimuksesta, jolloin tiedustelumenetelmän käytön odotusarvona on sen perusteltu hyödyllisyys. Tiedustelumenetelmän käytön hyödyllisyys tulisi pystyä yksittäistapauksellisesti perustelemaan, mitä ilmentäisi ilmaisu "perustellusti". Perustelu voisi liittyä esimerkiksi siihen, miksi nimenomaan tiettyä henkilöä tai henkilöryhmää taikka tiettyä tilaa tai muuta paikkaa tulisi voida tarkkailla ja miksi näin pystyttäisiin oletetusti saamaan kansallisen turvallisuuden kan-

nalta hyödyllistä tietoa. Tämä voisi liittyä esimerkiksi henkilön tai henkilöryhmän käyttäytymiseen taikka muutoin siitä saatuihin tietoihin. Siviilitiedustelun kohteena olevalla toiminnalla tarkoitettaisiin 3 §:ssä (Siviilitiedustelun kohteet) tarkoitettua toimintaa. Perusteluedellytys liittyisi myös siihen, että 3 §:ssä tarkoitettua toimintaa vastaan olisi perusteltua syytä ryhtyä suojautumaan.

Kansallista turvallisuutta vakavasti uhkaavan toiminnan vaatimus johtuu ehdotettavan perustuslain 10 §:n 4 momentista. Kyseisen perustuslain kohdan perusteella vakavuusedellytys nostaa luottamuksellisen viestin suojaan puuttuvien keinojen soveltamiskynnystä asettaessaan kvalifioinnin uhkan laadusta. Siten pelkästään jonkinasteisen uhkan kansalliselle turvallisuudelle muodostava toiminta ei vielä täyttäisi säännöksessä asetettua vaatimusta. Uhkan vakavuusaste kytkeytyy myös edellä 3 §:ssä käsiteltyihin sisällöllisiin määrittelyihin siitä, millainen siviilitiedustelun kohteena oleva toiminta muodostaa vakavan uhkan kansalliselle turvallisuudelle.

Kansallista turvallisuutta vakavasti uhkaavan toiminnan lajit tyhjentyisivät 3 §:ssä tarkoitettuihin siviilitiedustelun kohteisiin. Tiedustelumenetelmän käytön perusteeksi ei kuitenkaan riittäisi pelkkä abstraktin tason uhka, vaan yksittäistapauksellisesti tulisi tosiseikastotasolla pystyä osoittamaan, että siviilitiedustelun kohteena oleva toiminta muodostaisi vakavan uhkan tai sen voitaisiin olettaa vakavasti uhkaavan kansallista turvallisuutta. Tätä ilmentäisi relatiivilause "joka vakavasti uhkaa kansallista turvallisuutta." Ilmaisulla ”uhkaa” tarkoitettaisiin sitä, ettei säännöksessä edellytettäisi kansallisen turvallisuuden olevan välittömästi vaarantumassa. Näin ollen säännöksessä tarkoitettu tiedonhankinta voisi koskea myös siviilitiedustelun kohteena olevaa toimintaa, joka jatkuessaan vakavasti uhkaisi kansallista turvallisuutta. Uhkalta kuitenkin edellytettäisiin tietynasteista ajallista läheisyyttä tai sillä tulisi olla ainakin välillinen liityntä Suomen kansalliselle turvallisuudelle. Esimerkiksi kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi ei uhkaisi kansallista turvallisuutta silloin, jos sillä ei olisi mitään liityntäpintaa Suomeen tai sen ei edes voitaisi olettaa laajentuvan Suomeen tai Suomea koskevaksi. Sitä vastoin esimerkiksi terrorismin kohdalla Suomen naapurimaissa tai Euroopassa taikka maailmalla tapahtuneiden iskujen osalta voitaisiin useassa tapauksessa olettaa, että kyseisenlainen toiminta saattaisi laajeta myös Suomen alueella tapahtuvaksi. Tiedon hankkiminen sisältäisi myös Suomeen kohdistuvien ulkoisten uhkien kartoittamisen. Kyse olisi siten esimerkiksi turvallisuusympäristön kehityksen seuraamisesta kansalliseen turvallisuuteen kohdistuvan tilannekuvan muodostamiseksi.

Ilmaisu ”kansallinen turvallisuus” tarkoittaisi sitä, ettei säännöksessä tarkoitettu uhkaava toiminta kohdistuisi ensisijaisesti kehenkään yksilönä vaan yleisemmin yhteiskuntaan ja sen ihmisyhteisöön. Kuitenkin myös esimerkiksi yksityishenkilöihin kohdistuvat väkivallanteot voisivat olla säännöksessä tarkoitettua toimintaa, jos ne laajuudeltaan tai merkitykseltään olisivat kansallisen turvallisuuden kannalta merkittäviä ja voisivat siten muodostaa vakavan uhan sille. On selvää, että esimerkiksi valtiojohtoon tai yhteiskunnan perustoiminnoista huolehtiviin henkilöihin samoin kuin heidän turvallisuusjärjestelyistään vastaaviin kohdistuvat uhat voivat muodostaa vakavan uhan kansalliselle turvallisuudelle. Kansallisen turvallisuuden määritelmää käsitellään tarkemmin perustuslain 10 §:n 3 momentin muuttamista koskevassa hallituksen esityksessä. Yleisperusteluissa on käsitelty EIT:n ratkaisukäytännössä tehtyjä kannanottoja kansallisesta turvallisuudesta ja siihen kohdistuvista uhkista sekä tämän käsitteen muuttuvasta ja toisinaan myös ennakoimattomasta luonteesta.

"Voidaan perustellusti olettaa" olisi todennäköisyysasteena vastaava kuin rikosperusteisissa toimivaltuuksissa nykyisin käytettävä "on syytä olettaa" tai "on syytä epäillä", jota käytetään muun muassa salaisten pakkokeinojen käytön todennäköisyysasteena. Nykyisin pienintä todennäköisyysastetta kuvaa ilmaisu "on syytä olettaa", joka kuvaa esimerkiksi pakkokeinolain

7 luvun 1 §:ssä takavarikoimisen edellytyksiä. "On syytä olettaa" rinnakkaisilmaisuna käytetään esimerkiksi vakuustakavarikon edellytyksiä koskevassa pakkokeinolain 6 luvun 11 §:ssä käytettyä ilmaisua "on syytä epäillä". Kyseistä ilmaisuvaihtoehtoa käytetään silloin, kun kysymyksessä on inhimillinen toiminta, joka on joko jo tapahtunut (esim. rikos) tai jonka arvellaan voivan tapahtua tulevaisuudessa (esim. esitutkinnan karttaminen). Ilmaisua ”on syytä epäillä” käytetään myös esitutkinnan toimittamisvelvollisuutta koskevassa ETL 3:3,1:ssä. HE:n 14/1985 perustelujen (s. 16) mukaan rikosta on syytä epäillä, kun asioita huolellisesti harkitseva ihminen havaintojensa perusteella päätyy tällaiseen tulokseen.

Tiedustelumenetelmän käyttö tulisi lisäksi kyetä kohdistamaan mahdollisimman tarkasti. Kyseinen vaatimus johtuu poliisioikeudellisista periaatteista, erityisesti vähimmän haitan periaatteesta.

Pykälän 2 momentissa säädettäisiin tiedustelumenetelmäkohtaisista erityisistä käyttöedellytyksistä. Momentin 1. virkkeen mukaan sen lisäksi, mitä tiedustelumenetelmien käytön erityisistä edellytyksistä jäljempänä säädetään, telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitetusta toiminnasta. Momentin 2. virkkeen mukaan peitetoiminnan ja valeoston käyttäminen edellyttäisi lisäksi, että menetelmän käyttö olisi välttämätöntä. Momentin 3. virkkeen mukaan peitetoiminnan käyttäminen edellyttäisi myös, että tiedonhankintaa olisi toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena.

Jokaisella tiedustelumenetelmällä olisi tässä säännöksessä mainittujen edellytysten lisäksi pykäläkohtaisia erityisiä edellytyksiä. Esimerkiksi telekuuntelun (6 §) käyttämisestä päätöksen tekisi tuomioistuin ja silloin, kun toimenpiteen kohteena on henkilö, lupa voidaan antaa enintään kolmeksi kuukaudeksi kerrallaan.

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

Välttämättömyyden lisäksi peitetoimintaa käytön edellytyksenä olisi sen kohdistuminen järjestäytyneeseen kansallista turvallisuutta vakavasti uhkaavaan toimintaan. Järjestäytyneeseen toimintaan liittyy usein suunnitelmallisuus. Suunnitelmallisuuden mainitseminen säännöksessä tarkoittaisi myös sitä, että menetelmää olisi mahdollista kohdistaa jatkossakin esimerkiksi saman yksittäisen toimijan suunnitelmalliseen toimintaan. Peitetoiminnan käytön edellytyksenä olisi myös, että sen käyttäminen on tarpeellista kansallista turvallisuutta vakavasti uhkaavan toiminnan ennakoitavissa olevan jatkuvuuden tai toistuvuuden kannalta. Tällä tarkoitettaisiin sitä, että toiminnan ei tarvitse olla suunnitelmallista, järjestäytynyttä tai ammattimaista, mutta kylläkin oletettavasti jatkuvaa tai toistuvaa, jolloin kyse voisi olla esimerkiksi yksittäisistä ei-järjestäytyneistä henkilöistä.

Peitetoiminnan käyttöä rajoittaisi 4 momentissa säädetty kielto käyttää tiedustelumenetelmää vakituiseen asumiseen käytettävissä tiloissa eikä peitetoimintavaltuus oikeuttaisi menemään vakituiseen asumiseen käytettävään tilaan. Toisaalta peitetoimintaa suorittavalla henkilöllä tulisi olla oikeus paljastumisen estämiseksi mennä kyseisiin tiloihin käyttämällä hyväkseen luo-

tua peitettä. Peitetoimintaa suorittava poliisimies ei useinkaan voisi paljastumatta kieltäytyä tällaisessa tilanteessa esimerkiksi asuinhuoneistoon menosta. Paljastuminen saattaisi aiheuttaa peitehenkilölle hengen ja terveyden vaaran. Lisäksi tämä mahdollistaisi testaamisen onko kyseessä peitehenkilö vai ei. Peitetoiminnassa tulisi kuitenkin pyrkiä välttämään sellaista tilannetta, että peitetoiminta ajautuisi vakituiseen asumiseen käytettävään tilaan. Tämä edellyttäisi peitetoiminnan täsmällistä suunnittelua.

Telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, televalvonnan, teknisen kuuntelun, ja lähetyksen jäljentämisen lisäksi myös jäljentämisen käyttämisen edellytykset olisivat tiukemmat silloin, kun jäljentäminen kohdistuisi viestiin. Viestillä tarkoitettaisiin nimenomaan perustuslain 10 §:ssä turvattua luottamuksellista viestiä. Jäljentäminen kohdistuisi viestiin ainakin silloin, kun jäljentämisen kohteena olisi esimerkiksi pöydälle jätetty kirje tai tietokoneen näytöllä oleva sähköpostiviesti. Näissä tapauksissa valokuvan ottamisen tai muunlaisen jäljentämisen edellytyksenä olisi, mitä momentin 1. virkkeessä säädetään. Sitä vastoin, jos suojelupoliisin tiedossa olisi, että lähetyksen jäljentämisen kohteena olisi sellainen lähetys, joka ei sisältäisi mainittua viestiä, niin lähetyksen kvalifioidut edellytykset eivät tulisi sovellettavaksi.

Pykälän 3 momentissa säädettäisiin matalammasta käyttökynnyksestä niissä tapauksissa, joissa tiedustelumenetelmän käyttö kohdistetaan valtiolliseen toimijaan tai siihen rinnastuvaan tahoon. Luottamuksellisen viestin suojaan puuttuvan tiedustelumenetelmän kohdalla tämä tarkoittaisi, että esimerkiksi telekuuntelun käyttö pystyttäisiin kohdistamaan kahden valtiollisen toimijan väliseen viestintään, joka ei nauti perustuslaissa säädettyä luottamuksellisen viestin suojaa. Tällainen tilanne voisi olla esimerkiksi silloin, jos viestintä tapahtuu viranomaisverkossa. Mikäli virkamies käyttäisi viranomaisverkkoa yksityispuhelujensa soittamiseen, niin hän samalla ottaa riskin siitä, että viestinnän toinen osapuoli myös joutuu tiedustelun kohteeksi. Oletuksena on, että viranomaisverkkoja käytetään ainoastaan viranomaisten väliseen viestintään.

Viranomaiseen toimijaan rinnastuvalla taholla 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.

Viranomaiseen toimijaan rinnastuvalla taholla tarkoitettaisiin myös viranomaisen puolesta toimivaa tahoa eli ns. välillistä toimijaa, joka toimii puhtaasti valtiollisen toimijan lukuun. Kyseessä voisi siten olla 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 olisi kiinnitettävä esimerkiksi siihen, minkälainen tosiasiallinen määräysvalta ja ohjaus valtiolla olisi yritykseen ja kuinka konkreettisesti valtio voisi määrätä yrityksen toiminnasta.

Muiden ryhmittymien osalta edellä sanotun lisäksi huomiota olisi kiinnitettävä siihen, kuinka järjestäytynyttä toiminta on, kuinka merkittävät resurssit ryhmittymällä on käytössään esimerkiksi aseellisen hyökkäyksen tekemiseksi ja voisiko tällainen hyökkäys tekona rinnastua vaikutuksiltaan vieraan valtion tekemäksi sekä pyrkiikö ryhmittymä toimimaan valtion tavoin.

Itsestään selvää olisi, että valtiollisen toimijan tulisi olla edeltä käsin tunnistettu valtiolliseksi toimijaksi ja toimijan valtiollinen asema olisi ilmeinen. Tämä tarkoittaisi sitä, että esimerkiksi

tiedustelumenetelmän käytöstä päätettäessä tai lupavaatimusta laadittaessa suojelupoliisilla olisi ennakkotieto, että kohde olisi valtiollinen toimija ja tiedustelumenetelmän käytön aikana kohteena oleva toimisi tässä roolissa. Tiedustelutehtävän aikana tiedustelumenetelmän käyttö saattaisi alkaa muuhun kuin valtiolliseen toimijaan kohdistuvana tiedonhankintana, mutta tiedustelumenetelmällä saatujen tietojen perusteella tiedustelumenetelmän käyttö voisi myöhemmässä vaiheessa jatkua valtiolliseen toimijaan kohdistuvana tiedustelumenetelmän käyttönä, jos kävisi ilmeiseksi kohteena olevan toimijan valtiollinen status. Viime kädessä päätöksentekijän olisi ratkaistava se, onko vaatimuksen tueksi esitetty riittävä tosiseikasto sen tueksi, että kohteena oleva taho olisi valtiolliseksi toimijaksi katsottava.

Pykälän 4 momentin mukaan tiedustelumenetelmää ei saisi kohdistaa vakituiseen asumiseen käytettävään tilaan. Perustuslaissa turvattu kotirauhan piiri kattaa lähtökohtaisesti kaikenlaiset pysyväisluonteiseen asumiseen käytetyt tilat (esim. PeVL 43/2010 vp, s. 2, PeVL 40/2010 vp, s. 4, PeVL 18/2010 vp, s. 7, PeVL 6/2010 vp, s. 4, PeVL 8/2006 vp). Kotirauhan suojaama piiri määritellään kuitenkin eri tavoin perustuslaissa kuin esimerkiksi rikoslaissa. Tästä johtuen tiedustelumenetelmän käyttöä ei saisi kohdistaa rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan asuntoon tai muuhun asumiseen tarkoitettuun tilaan, jollei voitaisi osoittaa paikkaa tosiasiallisesti käytettävän muuhun kuin pysyväluonteiseen asumiseen (PeVL 36/1998 vp, KKO 2009:54). Ainoa poikkeus tästä olisi peitetoiminta ja valeosto, jolloin peitetoimintaa tai valeostoa suorittavalla suojelupoliisin virkamiehellä tulisi olla oikeus paljastumisen estämiseksi mennä kyseisiin tiloihin käyttämällä hyväkseen luotua peitettä. Siksi momentissa säädettäisiin, että peitetoiminta ja valeosto kuitenkin olisi asunnossa sallittua, jos sisäänkäynti tai oleskelu tapahtuisi asuntoa käyttävän aktiivisella myötävaikutuksella. Puheena olevan sääntelyn ulottaminen koskemaan myös valeostoa olisi oikeusturvasyistä perusteltua, koska valeosto voidaan toteuttaa myös asunnossa.

Pykälän 5 momentin mukaan tiedustelumenetelmän käyttö olisi lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Tällä korostettaisiin sitä, ettei tiedustelumenetelmiä voida missään tapauksessa käyttää kauempaa kuin on tarpeen, vaikka lupa olisikin vielä voimassa. Selvää on, että tiedustelumenetelmän käyttö on lopetettava viimeistään silloin, kun luvan voimassaolo päättyy.

Tiedustelumenetelmien määritelmistä, lukuun ottamatta paikkatiedustelua, jäljentämistä, lähetyksen pysäyttämistä jäljentämistä varten ja tietoliikennetiedustelua, säädettäisiin 5 luvussa, ja tiedustelumenetelmien käytön edellytyksistä ja kohdistamisesta sekä päätöksenteosta puolestaan tässä luvussa tai laissa tietoliikennetiedustelusta siviilitiedustelussa.

Tiedustelumenetelmiä käytettäessä poliisioikeudellisten periaatteiden merkitys on korostunut. Perusoikeuksien ja ihmisoikeuksien kunnioittaminen, suhteellisuus, pyrkimys vähimpään haittaan ja tarkoitussidonnaisuus ovat kaikki tärkeitä periaatteita tiedustelumenetelmiä käytettäessä. Näiden periaatteiden noudattaminen siviilitiedustelussa varmistaa osaltaan tiedustelumenetelmien käytön edellytyksiä koskevan tulkinnan pysymisen sallituissa rajoissa.

Perustuslakivaliokunta on lausunnossaan (PeVL 32/2013, s. 4 ja 33/2013, s. 4) painottanut yleisesti poliisilakiin ja pakkokeinolakiin sisältyvien yleisten periaatteiden sekä salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käytön yleisten ja erityisten edellytysten merkitystä sekä lupaa haettaessa että tuomioistuimen harkitessa luvan myöntämistä (ks. myös KKO 2007:7 ja 2009:54). Tiedustelumenetelmien käytön edellytyksissä ei ole mahdollista porrastaa menetelmien käytön edellytyksiä seuraamusuhkan täyttävän rikoksen perusteella, joten tämä asettaa päätöksentekijälle korostuneen tiedonsaantioikeuden luvan ehtojen arvioimiseksi. Jotta päätöksentekijällä olisi näissä tapauksissa mahdollisuus huolellisesti harkita luvan myöntämisen tarvetta ja laajuutta, hänellä tulee olla käytössään riittävät tiedot.

5 §. *Tiedonhankinnan jatkaminen eräiden rikosten estämiseksi ja paljastamiseksi*. Pykälässä säädettäisiin tiedustelumenetelmän käytön jatkamisesta sellaisissa tapauksissa, joissa tiedonhankintaa olisi tarve pystyä jatkamaan rikoksen estämiseksi tai paljastamiseksi. Suojelupoliisi saisi jatkaa tiedonhankintaa rikoksen estämiseksi ja paljastamiseksi tämän luvun nojalla annetun luvan tai päätöksen voimassaoloajan, jos tiedustelumenetelmän käytön aikana ilmenee, että henkilön voidaan perustellusti olettaa syyllistyvän 5 luvun 3 §:ssä mainittuun rikokseen taikka valtiopetokseen, törkeään valtiopetokseen tai laittomaan sotilaalliseen toimintaan tai voidaan olettaa, että sellainen rikos on tehty eikä tiedustelumenetelmän käytöllä enää voida olettaa saatavan tietoja luvan tai päätöksen perusteena olevasta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Pykälässä olisi kyse kansallisen turvallisuuden perusteella toteutettavan tiedustelumenetelmän käytön jatkamisesta suojelupoliisin torjuntavastuulle kuuluvien maanpetosrikosten, valtiopetosrikosten ja terrorismirikosten estämiseksi ja paljastamiseksi toisin kuin 5 luvun 4 §:ssä tarkoitetuissa tilanteissa, joissa on kyse salaisen tiedonhankinnan jatkamisesta minkä tahansa sen kohteena olevan rikoksen selvittämiseksi. Koska viittaus 5 luvun 3 §:ään kattaa vain maanpetosrikokset ja terrorismirikokset, eräät valtiopetosrikokset on mainittu pykälässä erikseen. Pykälässä mahdollistettaisiin tiedustelumenetelmän käyttö annetun luvan tai päätöksen voimassaoloajan silloin, kun 5 a luvun mukainen peruste tiedustelumenetelmän käytölle poistuu, mutta tiedonhankintaa olisi tarve jatkaa rikoksen estämiseksi tai paljastamiseksi. Ilman ehdotettavaa pykälää tiedustelumenetelmän käyttö olisi lopetettava esimerkiksi heti, kun kansallisen turvallisuuden perusteella käynnistetty tiedusteluintressi kaventuisi yksin tarpeeseen hankkia tietoa rikoksen estämiseksi tai paljastamiseksi.

Pykälän nojalla poliisilain 5 a luvun perusteella aloitettua tiedustelumenetelmän käyttöä saataisiin jatkaa vielä luvan voimassaolon ajan, enintään kuitenkin kuukauden ajan. Tämä merkitsisi sitä, että jos alkuperäisestä lupa-ajasta olisi jäljellä kaksi päivää, niin menetelmää saataisiin käyttää kahden päivän ajan, ja jos alkuperäistä lupa-aikaa olisi jäljellä enemmän kuin kuukausi, niin menetelmää saataisiin käyttää yhden kuukauden ajan. Edellä kerrottujen aikamääreiden mukaisesti tulisi hakea 5 luvun mukainen lupa tai päätös taikka lopettaa tiedustelumenetelmän käyttö.

Paikkatiedustelua, jäljentämistä ja lähetyksen pysäyttämistä jäljentämistä varten ei saisi jatkaa tämän pykälän perusteella rikoksen estämiseksi ja paljastamiseksi, koska näitä tiedustelumenetelmiä vastaavista salaisista tiedonhankintakeinoista ei säädetä poliisilain 5 luvussa.

Sen sijaan niissä tilanteissa, joissa kansallista turvallisuutta vakavasti uhkaava toiminta ei tyhjene siitä erottuvaan yksittäiseen maan-, valtiopetos- tai terrorismirikokseen, suojelupoliisi saisi jatkaa tiedustelumenetelmän käyttöä tämän luvun nojalla myös jatkoluvan tai -päätöksen voimassaoloajan. Kyse on toisin sanoen siitä, että kansallisen turvallisuuden perusteella toteutettava tiedustelumenetelmän käyttö saa jatkua annettujen lupien ja päätösten rajoissa niin kauan kuin tällaisella tiedonhankinnalla voidaan edelleen olettaa saatavan tietoja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

6 §. *Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Vaatimuksen käsittelystä tuomioistuimessa säädettäisiin 35 §:ssä. Päätöksentekotaso vastaisi 5 luvussa säädettyä.

Pykälän 2 momentin 1. virkkeen mukaan lupa telekuunteluun tai tietojen hankkimiseen telekuuntelun sijasta voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Lupa-aika olisi

pidempi kuin mitä 5 luvun telekuuntelussa, jolloin lupa voidaan myöntää enintään 1 kuukaudeksi kerrallaan. Pidempi lupa-aika olisi perusteltua siviilitiedustelun luonteen ja tiedustelumenetelmien käytön perusteen vuoksi. Tiedustelutoiminnan luonne poikkeaa merkittävästi rikostorjunnan tarpeista. Jos tiedustelumenetelmän käytölle tarvittaisiin kuuden kuukauden jälkeen jatkoa, uusi käsittely antaisi myös tuomioistuimelle aidon mahdollisuuden kontrolloida luvan edellytysten olevan edelleen olemassa vaarantamatta oikeusturvaa.

Tiedustelumenetelmiä ei saisi käyttää yksittäisten rikosten estämiseksi, paljastamiseksi tai selvittämiseksi eikä menetelmillä saatua tietoa saisi käyttää rikostorjunnassa kuin ainoastaan 44 §:ssä säädetyin edellytyksin. Tiedustelu on rikostorjuntaan verrattuna usein pidempikestoisempaa ja operaatiot ennakkoon tarkoin suunniteltuja. Operaation tavoitteena voi olla esimerkiksi kerätä tietoa kohdevaltion Suomen etuja vahingoittavasta toiminnasta ja siihen liittyvistä seikoista. Jos tiedusteluoperaation kohde on merkittävä, sen kesto voi olla hyvinkin pitkäaikaista. Näin tarkoituksena ei ole yksittäisen rikoksen estäminen tai selvittäminen, vaan varhaisen vaiheen tiedon kerääminen kokonaiskuvan saamiseksi. Säännös mahdollistaisi näin ollen ennakoivan ja pidempiaikaisemman tiedonhankinnan yhdellä lupapäätöksellä.

Säännöksessä ehdotettu kuuden kuukauden lupa-aika ei kuitenkaan automaattisesti tarkoittaisi sitä, että lupa voitaisiin aina hakea kuudeksi kuukaudeksi tai että se tulisi myöntää kuuden kuukauden määräajaksi. Suhteellisuus- ja vähimmän haitan periaatteen mukaista harkintaa edellyttäisi säännöksessä oleva ilmaisu "enintään kuudeksi kuukaudeksi kerrallaan". Siksi lupaa haettaessa sekä sitä myönnettäessä tulisi harkita tiedustelumenetelmän käytön ajallisen keston tarpeellisuutta tapauskohtaisesti.

Pykälän 2 momentin 2. virkkeen mukaan silloin, kun toimenpiteen kohteena olisi henkilö, niin lupa voitaisiin antaa enintään kolmeksi kuukaudeksi kerrallaan. Telekuuntelussa (ja televalvonnassa) toimenpiteen kohteena voisi olla 5 luvusta poiketen teleosoitteen tai telepäätelaitteen lisäksi myös henkilö. Tällaisessa menettelyssä olisi perusteltua noudattaa lyhyempää lupa-aikaa. Jos telekuuntelun käytölle tarvittaisiin kolmen kuukauden jälkeen jatkoa, uusi käsittely antaisi myös tuomioistuimelle aidon mahdollisuuden kontrolloida telekuuntelun kohdistamista. Esimerkiksi pelkästään se, ettei tiedusteluvaltuutettu olisi puuttunut telekuuntelun käyttöön, ilmentäisi telekuuntelun käytön hyväksyttävyyttä sekä sen lainmukaisuutta.

Pykälän 3 momentissa säädettäisiin vaatimukseen ja päätökseen sisällytettävistä tiedoista. Momentin 1 kohdan mukaan vaatimukseen ja päätökseen tulisi sisällyttää 3 §:ssä tarkoitettu toiminta, joka vakavasti uhkaisi kansallista turvallisuutta. Vähintään yhden 3 §:ssä tarkoitetuista kohdista tulisi olla mainittuna tiedustelumenetelmän käytön perusteena.

Momentin 2 kohdassa säädettäisiin edellytyksestä sisällyttää vaatimukseen ja päätökseen tiedustelumenetelmän kohde, joka olisi telekuuntelussa henkilö, teleosoite tai telepäätelaite. Poliisilain 5 luvun 5 §:ssä ja pakkokeinolain 10 luvun 3 §:ssä tarkoitetuista telekuunteluista poiketen siviilitiedustelussa telekuuntelun kohteena voisi olla myös henkilö. Kun telekuuntelulupa kohdistettaisiin henkilöön, lupa käsittäisi telekuunteluluvan kohteena olevan henkilön hallussa olevat tai luvan voimassaoloaikana haltuunsa tulevat tai hänen oletettavasti muuten käyttämänsä teleosoitteet tai telepäätelaitteet. Telekuuntelulupa ei siten olisi teleosoite- tai telepäälaitekohtainen. Luvan hakijan tulisi kuitenkin pystyä osoittamaan perusteet sille, miksi kyseisen henkilön hallussa on kansallisen turvallisuuden kannalta merkityksellistä tietoa. Kun tuomioistuimen luvassa määritelty toimenpiteen kohteena oleva henkilö ottaisi käyttöönsä tai hänen oletettaisiin ottaneen käyttöönsä uusia teleosoitteita tai telepäätelaitteita taikka hänen ilmenisi, että hänen hallussaan on teleosoite tai telepäätelaite, joita ei olisi jo tuomioistuimelle toimitetussa lupahakemuksessa yksilöity, niin tiedusteluviranomainen voisi kohdistaa toimen-

piteen näihin. Myös näiden teleosoitteiden tai telepäätelaitteiden kohdalla tulisi ilmoitus tehdä tiedusteluvaltuutetulle.

Momentin 3 kohta olisi päätöksenteon kannalta merkityksellinen. Sen mukaan vaatimukseen ja päätökseen tulee sisällyttää tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuvat. Kyseinen kohta velvoittaisi suojelupoliisia esittämään ja perustelemaan tosiseikkoja siten, että tuomioistuimella olisi tosiasiallinen mahdollisuus huolelliseen lupaharkintaan ja tuomioistuin voisi tehdä tiedustelumenetelmän käytön edellytysten täyttymisestä omat johtopäätöksensä. Mainituissa edellytyksissä on kyse ensinnäkin 5 a luvun 4 §:ssä säädettävistä tiedustelumenetelmän käytön yleisistä edellytyksistä. Lisäksi vaatimuksessa ja päätöksessä olisi esitettävä riittävät tosiseikat siitä, mistä 3 §:ssä tarkoitetusta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta on kyse ja miksi lupa-ajan tulisi olla tietyn pituinen. Lupaa haettaessa ja päätöstä perusteltaessa erityisen tärkeässä asemassa ovat poliisioikeudelliset periaatteet.

Momentin 4 kohdan mukaan vaatimukseen ja päätökseen tulee sisällyttää telekuuntelua tai telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevan luvan voimassaoloaika kellonajan tarkkuudella. Kellonaikatarkkuutta 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 suojelupoliisin päällystöön kuuluva poliisimies.

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, ne olisi kirjattava siihen.

7 §. *Televalvonnasta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi televalvonnasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos televalvontaa koskeva asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Momentissa tarkoitettu päätösvalta vastaisi osittain voimassa olevan lain 5 luvun 10 §:n 1 ja 2 momentin sääntelyä. Jos suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies on kiireellisessä tilanteessa tehnyt päätöksen 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 46 §). Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentin mukaan.

Suojelupoliisin päällystöön kuuluvan poliisimiehen perehtyneisyysvaatimus kuitenkin eroaisi 5 luvussa säädetystä koulutusvaatimuksesta jonkin verran. Tiedustelumenetelmien käytön perusteista ja tiedustelumenetelmien välisistä toisinaan tulkinnanvaraisista rajanvedoista johtuen olisi tarpeen edellyttää päällystöön kuuluvalta suojelupoliisin poliisimieheltä riittävää taitotasoa tiedustelumenetelmien käyttämiseen. Suojelupoliisin päällikön lisäksi päällystöön kuuluvia poliisimiehiä ovat suojelupoliisin apulaispäällikkö, osastopäällikkö, poliisilakimies, ylitarkastaja ja tarkastaja. Jotta mainitulla virkamiehellä olisi itsenäinen päätösvalta asiassa, tämän

tulisi olla myös tehtävään määrätty ja tiedustelumenetelmien käyttöön perehtynyt. Perehtyneisyysvaatimus täyttyisi joko salaiseen tiedonhankintaan liittyvällä koulutuksella tai riittävällä kokemuksella salaisen tiedonhankinnan käyttämisestä. Lisäksi poliisimiehen tulisi olla perehtynyt tiedustelutoimivaltuuksia koskevaan lainsäädäntöön. Ennen nykyisten poliisi- ja pakkokeinolakien voimaantuloa sekä lakien voimaantulon jälkeen on poliisihallinnossa järjestetty niin sanottuja STEKPOV (salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu virkamies) -koulutuksia, joiden tarkoituksena on ollut tuottaa pidättämiseen oikeutetuille poliisimiehille paremmat ammatilliset edellytykset salaisten tiedonhankintakeinojen ja salaisten pakkokeinojen käyttämisessä. Tämäntyyppinen koulutus antaisi perehtyneisyyden myös tiedustelumenetelmien käyttöön.

Suojelupoliisin päällikön tai tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen tekemä kiirepäätös tulisi saattaa tuomioistuimen käsiteltäväksi siitä huolimatta, että televalvonnan käyttäminen lopetetaan 24 tunnin kuluessa sen käytön aloittamisesta. Muuten hyvin lyhytaikaisella tiedonhankinnalla voitaisiin kiertää päätöksentekomenettelyä koskevia vaatimuksia. Asian saattaminen tällaisissakin tapauksissa tuomioistuimen käsiteltäväksi edistää toimimista lainmukaisesti. Tämä koskisi muitakin tilanteita, joissa suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies voi väliaikaisesti päättää tiedustelumenetelmän käytöstä.

Pykälän 2 momentissa säädettäisiin suostumukseen perustuvasta televalvonnasta. Suojelupoliisi saisi kohdistaa televalvontaa tietyn henkilön hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen, jos sillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Teleosoitteeseen 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 omistajan viestinnän osalta. Suostumus tulisi antaa kirjallisessa muodossa. Kiireellisissä tilanteissa suostumus voitaisiin kuitenkin antaa suullisesti, mutta se tulisi vahvistaa kirjallisesti niin pian kuin mahdollista.

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 suojelupoliisi ei saa käyttää taivuttelua tai johdattelua. Suojelupoliisi voi tuoda esiin mahdollisuuden antaa suostumus televalvonnan käyttämiselle, mutta johtopäätösten tekeminen tiedonhankintakeinon käytöstä on aina jätettävä asianomaiselle henkilölle (HE 224/2010 vp, s. 99–100).

Pykälän 3 momentin mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi 2 momentissa tarkoitetusta televalvonnasta.

Pykälän 4 momentin mukaan lupa voitaisiin 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. Lupa-ajan osalta voidaan viitata pääosin 6 §:n 2 momentin perusteluissa esitettyyn.

Pykälän 5 momentissa säädettäisiin asioista, jotka televalvontaa koskevassa vaatimuksessa ja päätöksessä pitää mainita. Tämän osalta voidaan viitata 6 §:n 3 momentin perusteluissa esitettyyn.

8 §. *Tukiasematietojen hankkimisesta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi tukiasematietojen hankkimisesta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä suojelupoliisin päällystöön kuuluva poliisimies saisi 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.

Tukiasematietojen hankkiminen merkitsee televalvontaa vähäisempää puuttumista luottamuksellisen viestinnän suojaan. Jos suojelupoliisin päällystöön kuuluva poliisimies on kiireellisessä tilanteessa tehnyt päätöksen 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 (46 §). Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1, 2 ja 3 momentin mukaan.

Pykälän 2 momentin mukaan lupa annettaisiin tietyksi ajanjaksoksi. Momentti vastaisi asiallisesti 5 luvun 12 §:n 2 momenttia.

Pykälän 3 momentissa säädettäisiin vaatimuksessa ja päätöksessä mainittavista tiedoista. Tämän osalta voidaan pääosin viitata 6 §:n 3 momentin perusteluissa esitettyyn. Tukiasematietojen hankkiminen ei ole sidottu erityisesti keneenkään tiettyyn henkilöön vaan kansallisen turvallisuuden kannalta merkitykselliseen ajankohtaan ja paikkaan, riittäisi 3 §:ssä tarkoitettua toimintaa koskevien tosiseikkojen mainitseminen. Vaatimuksessa ja päätöksessä pitäisi perustella myös 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.

9 §. *Suunnitelmallisesta tarkkailusta päättäminen.* Pykälän 1 momentin mukaan suojelupoliisin päällystöön kuuluva poliisimies päättäisi suunnitelmallisesta tarkkailusta.

Pykälän 2 momentin mukaan suunnitelmallista tarkkailua koskeva päätös voitaisiin tehdä kerrallaan enintään kuudeksi kuukaudeksi. Tämän osalta voidaan viitata 6 §:n 2 momentin perusteluissa esitettyyn.

Pykälän 3 momentissa säädettäisiin vaatimuksessa ja päätöksessä mainittavista tiedoista. Näiltä osin voidaan viitata pääosin 6 §:n 3 momentin perusteluissa esitettyyn. Suunnitelmallista tarkkailua voitaisiin kohdistaa momentin 2 kohdan mukaisesti myös henkilöryhmään. Siviilitiedustelussa voi ilmetä tarve seurata tietyn henkilöryhmän toimintaa. Suunnitelmallisessa tarkkailussa tiedonhankinta olisi luonteeltaan enemmän passiiviseen kanssakäymiseen perustuvaa.

Tiedustelumenetelmän käytössä kysymys ei ole rikoksen estämiseen, paljastamiseen tai selvittämiseen tähtäävistä toimista. Näin ollen tietyn henkilön yksilöinnin kautta ei siviilitiedustelussa ilmene vastaavanlaista tarvetta arvioida toimivaltuuden käytön erityisiä edellytyksiä, kuten onko kyseistä henkilöä syytä epäillä tietyn seuraamusuhkan täyttävästä rikoksesta tai voidaanko hänen olettaa syyllistyvän sellaiseen. Tiedustelumenetelmän käytön tarkoituksena voi olla esimerkiksi tiedonhankinta tietyn henkilöryhmän organisaatiosta, ryhmään kuuluvista

henkilöistä ja henkilöryhmän aktiivisuudesta tietyillä alueilla sekä ryhmän toiminnan eri muodoista.

Vähimmän haitan periaatteen mukaisesti tulee toimivaltuuden käyttö ensisijaisesti kohdistaa tiettyyn henkilöön. Tiedustelutoiminnassa saattaa kuitenkin olla tarpeen selvittää keitä johonkin tiettyyn henkilöryhmään kuuluu tai voi olla tarpeen selvittää tietyn ryhmän esimerkiksi terroristiryhmän tai vieraan tiedustelupalvelun organisaation henkilöiden toimintaa tietyllä alueella. Silloin, kun tiedonhankinta kohdistuisi johonkin tiettyyn henkilöryhmään eikä se täsmentyisi Suomessa olevaan yksittäiseen tai yksittäisiin henkilöihin, niin 46 §:ssä tarkoitettua ilmoitusta ei olisi tarpeen tehdä. Jos tiedustelumenetelmän käyttö kohdistuisi johonkin tiettyyn Suomessa olevaan henkilöryhmään ja ryhmästä yksilöityisi henkilö niin, että hänen henkilöllisyytensä selviäisi, niin tiedustelumenetelmän käytöstä ilmoittamiseen sovellettaisiin tiedustelumenetelmän käytöstä ilmoittamista koskevaa 46 §:ää samalla tavoin kuin suunnitelmallinen tarkkailu olisi kohdistettu henkilöön.

Kuten muidenkin tiedustelumenetelmien kohdalla, niin myös suunnitelmallista tarkkailua koskevassa päätöksessä tulisi kertoa henkilöön tai henkilöryhmään kohdistuvan tiedonhankinnan perusteena olevat tosiseikat, jotta menetelmän käyttämisestä päättävällä olisi mahdollisuus huolelliseen päätösharkintaan. Kun tiedustelumenetelmän käytöstä päättää tiedusteluviranomainen itse, niin päätökseen merkittävillä seikoilla on merkittävä asema niin sisäisen valvonnan kuin myös tiedusteluvaltuutetun suorittaman valvonnan mahdollistamisessa.

10 §. *Peitellystä tiedonhankinnasta päättäminen.* Pykälän 1 momentin mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi peitellystä tiedonhankinnasta.

Suojelupoliisin päällystöön kuuluvan poliisimiehen perehtyneisyysvaatimus johtuu siitä, että olisi erityisen tärkeä tiedostaa peitellyn tiedonhankinnan ja peitetoiminnan raja. Perehtyneisyydellä voidaan myös vähentää tiedonhankinnan paljastumisen riskiä sekä edistää toiminnan tuloksellisuutta. Vielä peiteltyä tiedonhankintaa voimakkaammin nämä näkökohdat korostuvat peitetoiminnassa ja valeostossa.

Pykälän 2 momentin mukaan päätös peitellystä tiedonhankinnasta olisi tehtävä kirjallisesti. Päätöksessä olisi mainittava: 1) toimenpide ja sen tavoite riittävästi yksilöityinä; 2) 3 §:ssä tarkoitettu toiminta; 3) toimenpiteen kohteena oleva henkilö tai henkilöryhmä; 4) tosiseikat, joihin peitellyn tiedonhankinnan edellytykset ja kohdistaminen perustuvat; 5) peitellyn tiedonhankinnan suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies; 6) toimenpiteen suunniteltu toteuttamisajankohta; 7) mahdolliset peitellyn tiedonhankinnan rajoitukset ja ehdot.

Toimenpiteellä tarkoitettaisiin varsinaista peitellyn tiedonhankinnan toimenpidettä, kuten toimimista taksinkuljettajana tavoitteena kuljettaa henkilö tietystä paikasta toiseen paikkaan. Toimivaltuuden käytön osalta edellytettäisiin erikseen siitä vastaavan poliisimiehen nimeämistä, jonka tehtävänä olisi huolehtia muun muassa siitä, ettei toiminnassa ole tosiasiallisesti kysymys peitetoiminnasta eikä taksikuskina toimiva peitemies ryhtyisi luomaan peitetoiminnan edellyttämää luottamuksellista suhdetta kuljetettavana olevaan.

Peitellyn tiedonhankinnan osalta ei edellytettäisi alkamis- ja päättymisajankohdan määrittelyä kellonaikatarkkuudella, koska kysymys on useimmiten yksittäisen toimenpiteen suorittamisesta ennakolta määräämättömänä ajankohtana.

Peitellyssä tiedonhankinnassa osalta päätöksentekijä (suojelupoliisin päällikkö tai tehtävään määrätty tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies) 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 olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Tiedusteluoperaatiossa on mahdollista, että tiedonhankinnan kohde täsmentyy, jolloin tiedustelumenetelmän käyttö tulisi kohdistaa siihen henkilöön tai henkilöryhmään, josta alun perinkin on ollut tarkoitus hankkia tietoa. Tämä velvoittaisi toimenpiteestä vastaavan poliisimiehen 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 tarvitsisi laatia kirjallisesti ennen peiteltyä tiedonhankintaa. Päätös on kuitenkin laadittava kirjallisesti viipymättä toimenpiteen jälkeen.

Säännös olisi 5 luvun 16 §:ssä säädettyyn nähden uusi. Suojelupoliisi voisi tilanteen edellyttäessä ryhtyä kiireellisesti toteuttamaan peiteltyä tiedonhankintaa. Tämä ei poistaisi päätöksen kirjallisuusvaatimusta, vaan mahdollistaisi kyseisen tiedustelumenetelmän käytön myös kiiretilanteessa. Päätös peitellystä tiedonhankinnasta olisi tehtävä kirjallisesti heti, kun se olisi mahdollista. Kiiretilanteessa tulisi huolehtia siitä, että toimenpiteen suorittajalle on kerrottu tämän työturvallisuuden ja oikeusturvan kannalta päätökseen kirjattavat tiedot suullisesti.

11 §. *Teknisestä kuuntelusta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi vapautensa menettäneen henkilön teknisestä kuuntelusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei sietäisi viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Vapautensa menettäneellä tarkoitettaisiin vangittua, pidätettyä tai muulla lainmukaisella perusteella kiinniotettua ja vapautensa menettänyttä henkilöä. Kuuntelun osalta ei edellytettäisi sitä, että kuuntelun kohteena olevan henkilön tulisi olla sellissä tai suorittaa rangaistusta rangaistuslaitoksessa taikka ole pakkolaitokseen eristetty tai tutkintavanki taikka poliisin säilytystiloissa oleva henkilö. Kyseisen edellytyksen mainitseminen on tarpeetonta, koska käytännössä vapautensa menettänyttä voidaan kuunnella ainoastaan niissä tiloissa, joissa hänellä on lupa käydä tai oleskella.

Kiirepäätöksen osalta voidaan viitata 7 §:n 1 momentin perusteluissa esitettyyn. Kiiretilannepäätöksen mahdollistamista perustelee operatiivisen toiminnan luonne. Äkillisesti voi syntyä tilanne, jolloin tuomioistuimen lupaa ei ehdittäisi hakea ilman, että menetetään kansallisen turvallisuuden suojaamiseksi merkityksellinen tieto. Tällainen äkillinen tilanne voisi syntyä esimerkiksi vankilaradikalisaation yhteydessä. Tällöin vankien tai vangin ja hänen tapaajansa välinen keskustelu voitaisiin nauhoittaa siihen itse lainkaan osallistumatta.

Pykälän 2 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi muusta kuin 2 momentissa tarkoitetusta teknisestä kuuntelusta.

Pykälän 3 momentin mukaan lupa voitaisiin antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan. Tältä osin voidaan viitata 6 §:n 2 momentin perusteluissa esitettyyn.

Pykälän 4 momentissa säädettäisiin asioista, jotka teknistä kuuntelua koskevassa vaatimuksessa ja päätöksessä pitää mainita. Näiltä osin voidaan viitata pääosin 6 §:n 3 momentin ja 9 §:n 3 momentin perusteluissa esitettyyn.

Teknistä kuuntelua voitaisiin momentin 2 kohdan mukaisesti kohdistaa myös tilaan tai muuhun paikkaan. Tilalla tarkoitettaisiin seinillä ja katolla taikka vastaavilla rakenteilla rajattua paikkaa. Tila siis erotetaan jollakin rakenteellisella tavalla paikasta, joka puolestaan voi olla yleinen tai yksityinen paikka. Muulla paikalla tarkoitettaisiin seinillä ja katolla taikka vastaavilla rakenteilla rajatun tilan ulkopuolista paikkaa, kuten esimerkiksi liikekiinteistön pihaaluetta.

Teknisen kuuntelun tarkoituksena on hankkia tietoa ainoastaan kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. On kuitenkin todennäköistä, että tiedustelumenetelmän rikostorjuntatoimivaltuuksiin nähden laveampien kohdistamisedellytysten - henkilö, henkilöryhmä, tila tai muu paikka - takia myös muut kuin siviilitiedustelun kannalta relevantit henkilöt joutuvat väistämättä kuuntelun kohteeksi. Tätä asetelmaa tasapainotettaisiin tiedusteluvaltuutetun suojelupoliisiin kohdistamalla oikeudellisella valvonnalla. Lähtökohtaisesti tilakuuntelulla pyrittäisiin saamaan tietoa tilassa olevista henkilöistä, heidän keskinäisestä kanssakäymisestä, mutta toisaalta kansallisen turvallisuuden kannalta tilakuuntelu voi olla merkityksellistä myös sen selvittämiseksi, ettei tiettyä tilaa käytetä.

Teknisen kuuntelun kohdistuessa muuhun paikkaan kuin tilaan, luvassa ja päätöksessä olisi määriteltävä niin täsmällisesti kuin mahdollista, kuinka suurelle alueelle teknistä kuuntelua on tarkoitus kohdistaa. Teknisen kuuntelun kohteena oleva alue olisi mahdollisuuksien mukaan rajattava niin pieneksi kuin mahdollista.

Teknisen kuuntelun käyttämisessä vakituiseen asumiseen käytettävien tilojen ja muiden paikkojen rajaus tulisi määrittää tapauskohtaisesti. Tekniseen kuunteluun liittyisi lupavaatimuksen tekevän suojelupoliisin päällystöön kuuluvan poliisimiehen tai tiedustelumenetelmästä päättävän arviointivelvollisuus, ja tarvittaessa myös selonottovelvollisuus. Jos tila tai muu paikka olisi vakituiseen asumiseen käytettävä, 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 voidaan tosiasiallisesti käyttää toimistona.

12 §. *Teknisestä katselusta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi vapautensa menettäneen henkilön teknisestä katselusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei sietäisi viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saisi päättää teknisestä katselusta 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. Tältä osin viitataan edellisen pykälän 1 momentin perusteluissa esitettyyn. Jos suojelupoliisin päällystöön kuuluva poliisimies on kiireellisessä tilanteessa tehnyt päätöksen 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 (46 §). Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentin mukaan.

Pykälän 2 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi muusta kuin 1 momentissa tarkoitetusta teknisestä katselusta. Tältä osin viitataan edellisen pykälän 2 momentin perusteluissa esitettyyn.

Pykälän 3 momentin mukaan lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan. Tältä osin viitataan edellisen pykälän 3 momentin perusteluissa esitettyyn.

Pykälän 4 momentissa säädettäisiin teknistä katselua koskevan vaatimuksen ja päätöksen sisällöstä tavalla, joka vastaa edellisen pykälän 4 momentissa säädettyä.

13 §. *Teknisestä seurannasta päättäminen.* Pykälän 1 momentin mukaan tuomioistuin päättäisi henkilön teknisestä seurannasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saisi päättää seurannasta 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 suojelupoliisin päällystöön kuuluva poliisimies on kiireellisessä tilanteessa tehnyt päätöksen 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 (46 §). Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1, 2 ja 3 momentin mukaan.

Pykälän 2 momentin mukaan suojelupoliisin päällystöön kuuluva poliisimies päättäisi muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta. Tämä vastaisi päätöksentekotasoltaan muutoin kuin kiirepäätöstä koskevilta osin 5 luvun 22 §:n 2 momentissa säädettyä.

Pykälän 3 momentin mukaan lupa voitaisiin antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan. Säännös vastaisi 5 luvun 22 §:n 3 momentissa säädettyä.

Pykälän 4 momentissa säädettäisiin teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä mainittavista tiedoista tavalla, joka vastaisi pääosin muita tiedustelumenetelmiä koskevissa vaatimuksissa ja päätöksissä mainittavia tietoja. Momentin 2 kohdan mukaan vaatimuksessa ja päätöksessä tulisi mainita myös esine, aine tai omaisuus, jos tekninen seuranta kohdistuisi tällaiseen objektiin.

14 §. *Teknisestä laitetarkkailusta päättäminen.* Teknisellä laitetarkkailulla tarkoitetaan 5 luvun 23 §:n 1 momentin mukaan 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. Siviilitiedustelussa "rikoksen estämiselle merkityksellisen seikan tutkimisen" sijasta kyse olisi seikan tai tiedon hankkimisesta 3 §:ssä tarkoitetusta toiminnasta, jonka voidaan olettaa uhkaavan kansallista turvallisuutta.

Pykälän 2 momentin mukaan teknisellä laitetarkkailulla ei saa hankkia tietoa viestin sisällöstä eikä (5 luvun) 8 §:ssä tarkoitetuista tunnistamistiedoista. Tunnistamistiedoilla tarkoitetaan lain sanamuodon mukaan tilaajaan tai käyttäjään yhdistettävissä olevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Voimassa olevasta laista tai sen perusteluista ilmenee ainakin välillisesti, että säännöksessä mainitulla viestin sisällöllä tarkoitetaan nimenomaan viestin sisältöä telekuuntelun ja teknisen kuuntelun tarkoituksessa esimerkiksi silloin, kun viestintä tapahtuu kahden ihmisen välillä reaaliaikaisesti esimerkiksi tietokoneelta tai älypuhelimesta. Siten kyseiselle laitteelle jo tallentuneet tai talletetut asiakirjat, jotka eivät ole tekniseen kuunteluun tai telekuunteluun reaaliaikaisessa yhteydessä, kuuluvat teknisen laitetarkkailun piiriin.

Pykälän 1 momentin mukaan tuomioistuin päättäisi teknisestä laitetarkkailusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, suojelupoliisin päällystöön kuuluva poliisimies saisi päättää teknisestä laitetarkkailusta 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 tiedonhankintakeinon käytön aloittamisesta.

Jos suojelupoliisin päällystöön kuuluva poliisimies on kiireellisessä tilanteessa tehnyt päätöksen 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 (46 §). Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1, 2 ja 3 momentin mukaan.

Pykälän 2 momentin mukaan lupa voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Tältä osin voidaan viitata 6 §:n 2 momentin perusteluissa esitettyyn. Pykälän 3 momentissa puolestaan säädettäisiin vaatimuksen ja päätöksen sisällöstä muita tiedustelumenetelmiä vastaavasti.

15 §. *Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen.* Pykälän 1 momentin mukaan suojelupoliisi saisi hankkia teknisellä laitteella teleosoitteen tai telepäätelaitteen yksilöintitiedot. Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisen edellytyksenä olisi 4 §:n 1 momentissa tarkoitettu yleinen edellytys, jonka mukaan tiedustelumenetelmällä voidaan perustellusti olettaa saatavan tietoja 3 §:ssä tarkoitetusta toiminnasta, jonka voidaan olettaa vakavasti uhkaavan kansallista turvallisuutta.

Pykälän 2 momentissa säädettäisiin tiedusteluvaltuutettu tarkastusoikeudesta. Teknisin ja valvonnallisin keinoin olisi varmistettava, ettei laite ominaisuuksiensa vuoksi aiheuta haitallista häiriötä yleisen viestintäverkon laitteille tai palveluille. Käytännössä vähäisen ja lyhytaikaisen häiriön aiheutuminen olisi sallittavaa, mutta laite ei kuitenkaan saisi aiheuttaa vähäistä suurempaa tai pitkäaikaista häiriötä. Käytännössä on havaittu, että teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisessa käytettävä tekninen laite saattaa aiheuttaa hetkellistä ja vähäistä häiriötä joillekin muille ympäröiville laitteille.

Siviilitiedustelussa ei olisi tarkoituksenmukaista rajata pykälässä tarkoitettua teknistä laitetta toiminnallisuudeltaan ainoastaan teleosoitteen ja telepäätelaitteen yksilöimiseen. Tämä liittyy erityisesti ulkomaan tiedustelussa toteutettavaan telekuunteluun ja televalvontaan.

Pykälän 3 momentin mukaan teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättäisi suojelupoliisin päällystöön kuuluva poliisimies.

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisen käytössä ei olisi vastaavanlaista muihin tiedustelumenetelmiin verrattavaa luetteloa vaatimuksessa ja päätöksessä mainittavista asioista. Menetelmän käyttö tulisi kuitenkin dokumentoida riittävän tarkasti. Päätöksestä tulisi ilmetä ainakin teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisen yleiset edellytykset, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päätöksen teh-

nyt virkamies ja päätöksen antopäivä, päätöksen voimassaoloaika sekä päätöksen mahdolliset muut ehdot.

16 §. *Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen.* Pykälän 1 momentin mukaan suojelupoliisin palveluksessa olevalla virkamiehellä olisi oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan ja tekniseen laitetarkkailuun käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos tarkkailun toteuttaminen sitä edellyttää. Suojelupoliisin palveluksessa olevalla 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 kohteen tai tietojärjestelmän suojaus tai haitata sitä.

Vastaava säännös on 5 luvun 26 §:n 1 momentissa. Erona olisi, että tässä pykälässä ei käytettäisi poliisimiehen käsitettä, vaan puhuttaisiin suojelupoliisin palveluksessa olevasta virkamiehestä. Tällä mahdollistettaisiin se, että asentamisessa ja poisottamisessa voitaisiin käyttää myös muuta virkamiestä kuin poliisivirkamiestä. Teknisen kehityksen myötä tiedustelumenetelmien käyttäminen voi edellyttää laitteen, menetelmän tai ohjelmiston asentamisessa ja poisottamisessa teknisen asiantuntijan käyttämistä. Esimerkiksi eräiden kohteiden tai tietojärjestelmien suojaus tulee voida tilapäisesti kiertää, purkaa tai ohittaa.

Pykälän 2 momentin mukaan telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan ja tekniseen laitetarkkailuun käytettävän laitteen, menetelmän tai ohjelmiston saa asentaa vakituiseen asumiseen käytettävään tilaan vain, jos tuomioistuin on antanut siihen luvan suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Jos tiedustelumenetelmän käytöstä päättäisi tuomioistuin, niin myös tiedustelumenetelmän käyttöä koskevassa luvassa tulisi erikseen sallia laitteen, menetelmän tai ohjelmiston asentaminen. Sitä vastoin laitteen, menetelmän tai ohjelmiston poistamiseen lupaa ei tarvittaisi. Jos tiedustelumenetelmän käytöstä päättäisi suojelupoliisin päällystöön kuuluva poliisimies tai suojelupoliisin poliisimies, voitaisiin päätökseen merkitä laitteen, menetelmän tai ohjelmiston asentamista ja poisottamista koskevat tarpeelliset tiedot. Suojelupoliisin päällystöön kuuluvia poliisimiehiä ovat suojelupoliisin päällikkö, apulaispäällikkö, osastopäällikkö, poliisilakimies, ylitarkastaja ja tarkastaja.

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen olisi toissijainen toimivaltuussäännös, joka mahdollistaisi varsinaisen tiedustelumenetelmän käytön. Tämä ei poistaisi velvollisuutta hakea lupaa esimerkiksi telekuuntelun tai televalvonnan käytön osalta.

Suojelupoliisin palveluksessa olevalla virkamiehellä olisi laitteen, menetelmän tai ohjelmiston asentamiseksi, käyttöön ottamiseksi ja poistamiseksi oikeus mennä salaa tilaan tai muuhun paikkaan taikka tietojärjestelmään. Myös kohteiden tai tietojärjestelmien suojaus voitaisiin tilapäisesti kiertää, purkaa tai ohittaa. Suojausta voitaisiin myös tilapäisesti haitata. Kyseinen toimivaltuus ei kuitenkaan mahdollistaisi niin sanottua jälkikäteen ilmoitettavaa kotietsintää. Tiedustelutoiminnan luonteesta johtuen eteen voi tulla tilanteita, joissa laitteen, menetelmän tai ohjelmiston asentaminen edellyttää kotirauhan suojan piiriin menemistä, sillä esimerkiksi teknisessä laitetarkkailussa laite tai ohjelmisto voi olla tarpeen asentaa vakituiseen asumiseen käytettävässä tilassa esimerkiksi tekniselle laitteelle.

Säännöksessä ei oteta kantaa siihen, kuinka varhain laite, menetelmä tai ohjelmisto voidaan asentaa tai kuinka myöhään se voidaan poistaa, vaan tämä jätetään soveltajan harkintaan. Hyväksyttävää ei olisi, että esimerkiksi teknisen tarkkailun kohde pidettäisiin varustettuna teknistä tarkkailua varten ikuisesti. Tällä tarkoitetaan nimenomaan suojelupoliisin asentamia laitteita eli soveltamisalan ulkopuolelle jäisivät teknisessä laitteessa itsessään olevat teknisen tarkkailun käytön mahdollistamat ominaisuudet. Tässä suhteessa tiedustelumenetelmän käytön paljastumisen estämisen kannalta on kuitenkin tärkeää, ettei kiinteitä aikarajoja aseteta, vaan säännös antaa liikkumavaraa. On mahdollista, että kohdehenkilön tai -henkilöiden valmiuksien ja valveutuneisuuden vuoksi tilaisuutta asentamiseen, käyttöönottamiseen tai poistamiseen ei saada tarpeen mukaan vaan silloin, kun siihen tulee tilaisuus.

Laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä tulisi aina pohtia sen mahdollisesti aiheuttamaa kiinnijäämisriskiä sekä myös asentamisen kohteelle aiheutuvaa mahdollista vahingon riskiä. Esimerkiksi salaa tietojärjestelmään asennettu ohjelmisto sisältää aina mahdollisen riskin tietojärjestelmän toiminnalle ja on omiaan heikentämään sen turvallisuutta. Suojelupoliisin toimenpiteillä ei siten saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä laitteen, menetelmän tai ohjelmiston asentamisen ja poisottamisen yhteydessä.

17 §. *Peitetoimintaa koskeva esitys ja suunnitelma.* Pykälässä säädettäisiin peitetoiminnasta siviilitiedustelussa.

Peitetoiminnalla tarkoitetaan 5 luvun 28 §:n 1 momentin mukaan 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.

Erona 5 luvun 28 §:n 1 momentissa tarkoitettuun peitetoimintaan olisi käyttöedellytysten lisäksi, että tietojen hankkimiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta toteutettavaa peitetoimintaa olisi mahdollista kohdistaa myös henkilöryhmään. Tältä osin voidaan viitata 9 §:n 3 momentin perusteluissa esitettyyn.

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 Suomeen aiheuttamalla vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille elintärkeille eduille. Tällaista toiminta voisi olla esimerkiksi laajamittaisen Suomeen kohdistuvan maahantulon ohjaaminen.

Kohteena olevaa henkilöä tai henkilöryhmää ei olisi tarpeen nimetä tai yksilöidä esimerkiksi fyysisiltä ominaisuuksiltaan, vaan riittävää on, että henkilö tai henkilöryhmä voitaisiin yksilöidä esimerkiksi toiminnan kautta.

Pykälän 1 momentin mukaan peitetoimintaa koskevassa esityksessä olisi mainittava: 1) toimenpiteen esittäjä, 2) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöityinä, 3) 3 §:ssä tarkoitettu toiminta, 4) peitetoiminnan tavoite, 5) peitetoiminnan tarpeellisuus, 6) muut peitetoiminnan edellytysten arviointia varten tarvittavat tiedot. Momentti vastaisi 5 luvun 31 §:n 2 momenttia.

LUONNOS

Pykälän 2 momentin mukaan peitetoiminnan toteuttamisesta olisi laadittava kirjallinen suunnitelma, jonka tulisi sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa olisi olosuhteiden muuttuessa tarvittaessa tarkistettava.

Suunnitelman tarkistamisvelvollisuus merkitsee jatkuvaa peitetoimintaoperaation seuraamisvelvoitetta. Pykälässä luetellaan varsin yksityiskohtaisesti suunnitelman laatimiseksi ja päätöksenteon tueksi tarvittavat tiedot. Suunnitelman tulee sisältää peitetoimintaa koskevan päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaan voitaisiin myös sisällyttää peitetoiminnan purkamista koskeva suunnitelma, jos sellainen ylipäätään olisi peitetoiminnan aloittamista suunniteltaessa mahdollista. Suunnitelman laatimisen jälkeen ajankohtaistuu peitetoimintaa koskeva päätöksenteko.

18 §. *Peitetoiminnasta päättäminen.* Pykälän 1 momentin mukaan suojelupoliisin päällikkö päättäisi 17 §:ssä tarkoitetusta peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää suojelupoliisin päällikkö taikka tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Säännös vastaisi pääosin 5 luvun 32 §:n 1 momenttia.

Pykälän 2 momentin mukaan peitetoimintaa koskeva päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Säännös vastaisi 5 luvun 32 §:n 2 momenttia.

Pykälän 3 momentin mukaan päätös peitetoiminnasta olisi tehtävä kirjallisesti. Päätöksessä on mainittava: 1) toimenpiteen esittäjä, 2) peitetoiminnan toteuttamisesta vastaava poliisimies, 3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä, 4) 3 §:ssä tarkoitettu toiminta, 5) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöityinä, 6) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat, 7) peitetoiminnan tavoite ja toteuttamissuunnitelma, 8) päätöksen voimassaoloaika, 9) peitetoiminnan mahdolliset rajoitukset ja ehdot. Säännös vastaisi pääosin 5 luvun 32 §:n 3 momenttia.

Pykälän 4 momentin mukaan päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös. Säännös vastaisi 5 luvun 32 §:n 4 momenttia.

Peitetoiminnan edellytyksistä annettavasta tuomioistuimen ratkaisusta ei 5 a luvussa olisi tarpeen säätää. Ensinnäkin tiedustelumenetelmänä käytettävän peitetoiminnan kohdalla olisi vahva presumptio siitä, ettei saatua tietoa tultaisi käyttämään rikosprosessissa. Vaikka näin voisi erittäin poikkeuksellisissa olosuhteissa käydä, niin tuomioistuimen arviointia peitetoiminnan edellytyksistä ei olisi vastaavassa määrin tarpeellinen kuin mitä 5 luvussa ja pakkokeinolain 10 luvussa, sillä siviilitiedustelua ja tiedustelumenetelmien käyttöä valvoo tiedusteluvaltuutettu.

19 §. *Rikoksentekokielto.* Pykälän 1 momentissa todettaisiin selvyyden vuoksi se lähtökohta, että peitetoimintaa suorittava suojelupoliisin poliisimies ei saisi tehdä rikosta eikä aloitetta rikoksen tekemiseen. Myös sellainen aloitteellisuus, joka ei vielä ole rikoslain tarkoittamaa rikokseen yllyttämistä, olisi peitehenkilöltä kielletty.

Pykälän 2 momentissa säädettäisiin eräistä rikkomuksia koskevista vastuuvapaustilanteista. Jos peitetoimintaa suorittava suojelupoliisin poliisimies tekisi liikennerikkomuksen, järjestysrikkomuksen tai muun niihin rinnastettavan rikoksen, josta on säädetty rangaistukseksi rikesakko, hän olisi rangaistusvastuusta vapaa, jos teko on ollut tarpeen peitetoiminnan tavoitteen saavuttamiseksi tai tiedonhankinnan paljastumisen estämiseksi.

Säännös ei olisi siinä mielessä yleisluonteinen, että peitetoimintaa suorittava suojelupoliisin poliisimies voisi automaattisesti vapautua rangaistusvastuusta tehdessään pykälässä tarkoitetun rikkomuksen. Laissa on useita säännöksiä, joiden perusteella poliisimiehellä on oikeus toimia tietyllä tavalla, joka ilman nimenomaista toimivaltasäännöstä katsottaisiin lainvastaiseksi menettelyksi. Esimerkiksi tieliikennelain (267/1981) 48 §:n 5 momentin mukaan poliisimiehellä, tullimiehellä, rajavartiomiehellä sekä sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa tarkoitetulla rikosten ennaltaestämis- ja paljastamistehtävissä toimivalla virkamiehellä on tarkkailutehtävässä ja teknisen tarkkailun tehtävässä ja poliisimiehellä peitetoimintatehtävässä ja valeostotehtävässä toimiessaan erityistä varovaisuutta noudattaen sama oikeus kuin säädettyjä ääni- ja valomerkkejä antavan poliisiauton kuljettajalla poiketa tämän lain säännöksistä.

Vastuuvapaus voisi tulla kysymykseen vain silloin, kun todetaan, että teko on ollut tarpeen peitetoiminnan tavoitteen saavuttamiseksi tai tiedonhankinnan paljastumisen estämiseksi. Rangaistusvastuusta vapautuminen olisi siten varsin rajoitettua. Suhteessa mainittuun tieliikennelain 48 §:n 5 momenttiin ehdotettu säännös tulisi sovellettavaksi esimerkiksi silloin, kun peitetoimintaa suorittava poliisimies ei ole noudattanut erityistä varovaisuutta, jolloin myöskään mainittu momentti ei tulisi sovellettavaksi. Peitetoimintaa suorittava poliisimies voisi tällöin vapautua rangaistusvastuusta ehdotetun momentin perusteella.

Ensi vaiheessa peitetoimintatehtävässä toimineen suojelupoliisin poliisimiehen menettelyä arvioisi tiedustelutoimintaa valvova tiedusteluvaltuutettu.

20 §. *Valeostosta päättäminen.* Valeostolla tarkoitetaan 5 luvun 35 §:n 1 momentin mukaan poliisin tekemää esineen, aineen, omaisuuden tai palvelun ostotarjousta tai ostoa, jonka tavoitteena on rikoksen estämiseksi saada poliisin haltuun tai löytää estettävään rikokseen liittyvä esine, aine tai omaisuus. Erona edellä mainittuun tässä pykälässä tarkoitetulla valeostolla olisi tarkoitus hankkia tietoja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Kyse voisi siten olla esimerkiksi sellaisen kaksikäyttötuotteen valeostosta, jonka hallussapitäminen ei olisi rangaistavaa, mutta kansallisen turvallisuuden kannalta valeostotoimi saattaisi olla välttämätöntä toteuttaa.

Pykälän 1 momentin mukaan suojelupoliisin päällikkö päättäisi valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saisi päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Pykälän 2 momentin mukaan valeostoa koskeva päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Tämän osalta voidaan viitata pääosin 5 §:n 2 momentin perusteluissa esitettyyn.

Pykälän 3 momentin mukaan päätös valeostosta olisi tehtävä kirjallisesti. Päätöksessä on mainittava: 1) 3 §:ssä tarkoitettu toiminta, 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. Momentti vastaisi pääosin 5 luvun 36 §:n 2 momenttia.

Valeoston tuloksellisuusodotus (3 kohta) liittyisi asetettavaan todennäköisyyden vaatimukseen. Luvun 2 §:n 2 momentin mukaan valeostolla tulisi voida olla erittäin tärkeä merkitys tietojen saamiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta ja valeoston tulisi olla välttämätön tiedon saamiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Valeosto voisi kohdistua myös niin sanotusti vilpittömässä mielessä toimivaan henkilöön. Tehokas tiedonhankinta esimerkiksi terrorismista edellyttää, että suojelupoliisi pystyy saamaan riittävästi tietoa terroristisoluista, maksuyhteyksistä ja kauppapaikoista sekä taustalla toimivasta organisaatiosta ja sen johdosta. Tällaisessa tilanteessa valeosto voi olla tarpeen kohdistaa esimerkiksi terroristisolun kauppakumppaniin.

21 §. *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.

Pykälä vastaisi 5 luvun 37 §:ssä säädettyä. Erillinen valeoston toteuttamista koskeva suunnitelma voi olla tarpeen erityisesti toimintaan sisältyvien riskien torjumiseksi.

Valeoston vaativuuden ja siihen sekä tiedustelutoimintaan liittyvien riskien vuoksi suunnitelma tulee käytännössä kysymykseen kaikissa operaatioissa. Suunnitelma voitaisiin jättää laatimatta esimerkiksi yksinkertaisen lehti-ilmoituksen tai muun vastaavan syyn perusteella toteutettavissa valeostoissa.

Suunnitelman tarkistamisvelvollisuus merkitsee jatkuvaa valeosto-operaation seuraamisvelvoitetta. Mikään ei estäisi laatimasta myös valeoston purkamista koskevaa suunnitelmaa, jos sellainen olisi valeostoa suunniteltaessa mahdollista ja tarpeen.

22 §. *Valeoston toteuttamista koskeva päätös.* Pykälän 1 momentin mukaan päätös valeoston toteuttamisesta olisi tehtävä kirjallisesti. Päätöksen tekisi valeoston toteuttamisesta vastaava tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Momentti vastaisi 5 luvun 37 §:n 1 momenttia.

Pykälän 2 momentin mukaan päätöksessä olisi mainittava: 1) valeostosta päättänyt poliisimies, päätöksen antopäivä ja sisältö; 2) tunnistetiedot valeoston suorittavista poliisimiehistä; 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. Momentti vastaisi 5 luvun 37 §:n 2 momenttia.

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. Momentti vastaisi 5 luvun 37 §:n 3 momenttia.

Pykälän 4 momentin mukaan valeoston toteuttamista koskevaa päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Momentti vastaisi 5 luvun 37 §:n 4 momenttia.

Monenkertaisen asiakirjaprosessin tarkoituksen on varmistua siitä, että valeosto voidaan toteuttaa asianmukaisesti. Lisäksi koko prosessi tulee luotettavasti dokumentoitua, mikäli ilmenee tarvetta jälkikäteisarvioinnille. Erityisesti valeostoon liittyvien riskien vuoksi on mahdollista, että toimintaa joudutaan selvittämään vielä jälkikäteen.

23 §. *Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa, valeostossa ja tietolähdetoiminnassa.* Pykälän 1 momentin mukaan suojelupoliisin päällystöön kuuluva poliisimies saisi päättää, että tässä luvussa tarkoitettua peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava sekä tietolähdetoimintaa valmisteleva tai toteuttava poliisimies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.

Momentti vastaisi osin 5 luvun 39 §:n 1 momenttia. Momentti koskisi niin sanottua turvakuuntelua ja -katselua. Siihen lisättäisiin, että tietolähdetoimintaa valmisteleva tai toteuttava voitaisiin myös varustaa turvakuuntelun ja -katselun mahdollistavilla teknisillä laitteilla.

Tietolähdetoiminnan valmistelulla tarkoitettaisiin ainakin sitä, kun suojelupoliisin poliisimies selvittää onko tietolähteeksi rekrytoitava henkilö henkilökohtaisilta ominaisuuksiltaan sopiva tietolähteeksi. Suojelupoliisin poliisimies saattaa altistaa itsensä tietolähdetoiminnassa vastaavantasoiselle hengen ja terveyden vaaralle kuin esimerkiksi peitetoiminnassa. Tämä koskee erityisesti tilanteita, joissa tietolähteeksi rekrytoitavan suhtautumisesta häntä lähestyvään poliisimieheen ei ole vielä varmuutta. Suojelupoliisin poliisimiehen turvaamisen tulisi olla perusteltua hänen turvallisuutensa varmistamiseksi.

Pykälän 2 momentin mukaan kuuntelu ja katselu saataisiin tallentaa. Tallenteet olisi hävitettävä heti sen jälkeen, kun niitä ei tarvita poliisimiehen turvaamiseen. Jos niitä on kuitenkin tarpeen säilyttää asiaan osallisen oikeusturvaan liittyvistä syistä, tallenteet saataisiin säilyttää ja niitä saataisiin käyttää tässä tarkoituksessa. Tällöin tallenteet on hävitettävä, kun asia on lainvoimaisesti ratkaistu tai jätetty sillensä.

Momentti vastaisi pääosin 5 luvun 39 §:n 2 momenttia. 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 poliisimieheen on kohdistettu väkivaltaa tai että hän on joutunut käyttämään väkivaltaa taikka että peitellyn tiedonhankinnan, peitetoiminnan tai valeoston yhteydessä on jollekin aiheutunut vahinkoa. Näissä tapauksissa tallenteita saatettaisiin tarvita rikosasian tai vahingonkorvausasian käsittelyn yhteydessä (HE 224/2010 vp., s. 124).

24 §. *Tietolähteen ohjatusta käytöstä päättäminen.* Pykälän 1 momentin mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi tietolähteen ohjatusta käytöstä.

Tietolähdetoiminnalla tarkoitetaan 5 luvun 40 §:n 1 momentin mukaan muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun esitutkintaviranomaisen ulkopuoliselta henkilöltä (tietolähde). Luvun 40 §:n 2 momentin mukaan poliisi saa pyytää tähän tarkoitukseen hyväksyttyä, henkilökohtaisilta ominaisuuksiltaan 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.

Myös siviilitiedustelussa tietolähteen henkeä ja terveyttä olisi tarpeen suojata riittävällä tavalla tiedonhankinnan aikana ja sen jälkeen. Jos olisi syytä epäillä, että tietolähteen turvallisuutta olisi tarpeen suojata jo ennen tiedonhankintaa tai tietolähdettä olisi tarpeen suojata intensiivisemmin, tilanteessa tulisi sovellettavaksi 36 §:n säännös suojaamisesta päättämisestä. Jos tietolähteen suojaaminen olisi aloitettu 36 §:n perusteella, sitä voitaisiin myös jatkaa kyseisen säännöksen perusteella.

Pykälän 2 momentin mukaan tietolähteen ohjattua käyttöä koskeva päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Momentti vastaisi 5 luvun 42 §:n 2 momentin sääntelyä.

Pykälän 3 momentissa säädettäisiin tietolähteen ohjattua käyttöä koskevan päätöksen kirjallisesta muotovaatimuksesta ja päätöksessä mainittavista asioista. Momentti vastaisi pääosin 5 luvun 42 §:n 3 momentin sääntelyä.

Pykälän 4 momentin mukaan päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava. Tietolähteen ohjatun käytön lopettamisesta olisi tehtävä kirjallinen päätös. Sääntely vastaisi lain 5 luvun 42 §:n 4 momentissa olevaa.

Pykälän 5 momentin mukaan tietolähdettä koskevien tietojen tallettamisesta henkilörekisteriin ja palkkion maksamisesta säädetään 5 luvun 41 §:ssä.

Lähtökohtana tiedustelumenetelmien käytössä on, ettei niitä saa 2 §:n 3 momentin mukaan kohdistaa vakituiseen asumiseen käytettävään tilaan. Tietolähdetoiminnassa on kuitenkin muihin tiedustelutoimivaltuuksiin nähden erilainen tilanne, sillä poliisimies ei ole itse toteuttamassa tiedonhankintaa. Näin ollen tietolähteen toiminta ei myöskään olisi poliisimiehen kontrollissa. Tietolähteen ohjatussa käytössä tietolähteen sen sijaan voitaisiin katsoa ainakin välillisesti olevan suojelupoliisin poliisimiehen kontrollissa tai ainakin tietolähteelle esitettävissä tiedonhankintapyynnöissä pitäisi huomioida se, että tiedonhankinta ei edellyttäisi menemistä vakituiseen asumiseen käytettävään tilaan. Tästä syystä tietolähteen kanssa asioivan poliisimiehen tulisi myös kertoa tietolähteelle edellä mainitusta rajoitteesta. Tietolähde saisi kuitenkin samalla tavoin kuin peitetoiminnassa mennä vakituiseen asumiseen käytettävään tilaan silloin, kun se olisi tarpeen tietolähdetoiminnan paljastumisen estämiseksi.

25 §. *Tietolähteen turvaaminen.* Pykälässä säädettäisiin tietolähteen turvaamisesta. Suojelupoliisilla 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 suojelupoliisi voisi 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 olisi tarpeen tietolähteen henkeä tai terveyttä uhkaavan vaaran torjumiseksi. Suostumuksen saamisella varmistetaan se, että tietolähde myös itse haluaa tulla turvatuksi. Tietolähteen turvaamisesta ei tarvitsisi ilmoittaa sivullisille.

Momentissa mahdollistettaisiin erilaisten tietolähteiden turvaamiseksi tarpeellisten turvajärjestelmien, kuten esimerkiksi valvontakameroiden, liiketunnistimien ja muiden anturien asentaminen suojelun tarpeessa olevan tietolähteen asuntoon ja sen välittömään lähiympäristöön. Muulla tietolähteen asumiseen käyttämällä tilalla tarkoitettaisiin esimerkiksi hotellihuonetta.

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, mitä henkilöitä 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 ja terveyden suojaamiseksi.

Pykälän 2 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 3 momentin mukaan edellä 1 ja 3 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 esimerkiksi siitä, että tietolähteeseen on kohdistettu väkivaltaa 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. Rikos- tai vahingonkorvauskäsittely saattaisi kuitenkin edellyttää suljettua käsittelyä.

Tietolähteen turvaamistoimivaltuus ei korvaisi todistajansuojeluohjelmasta annetussa laissa tarkoitettua todistajansuojeluohjelmaa. Jos tietolähdettä olisi tarpeen suojella pidempiaikaisesti ja häneen kohdistuisi vakava hengen tai terveyden uhka eikä uhkaa voitaisi tehokkaasti torjua muilla toimenpiteillä, tietolähteen suojaamiseksi voitaisiin harkita todistajansuojeluohjelman käynnistämistä.

Pykälän 4 momentissa säädettäisiin tietolähteen turvaamisesta turvakuuntelulla ja -katselulla. Siviilitiedustelussa tietolähteitä olisi tarpeen värvätä kansallista turvallisuutta vakavasti uhkaavan toiminnan ytimestä, mistä seuraa, että tietolähteeksi suostuessaan henkilö saattaa altistaa itsensä hengen ja terveyden vaaralle. Tietolähteillä ei myöskään ole vastaavanlaista koulutusta voimankäyttöön kuin salaiseen tiedonhankintaan osallistuvilla poliisimiehillä, mistä johtuen heidän turvallisuudestaan huolehtiminen viranomaistoimenpitein nousee erittäin tärkeään asemaan.

Tietolähteen varustaminen turvakuuntelun tai -katselun mahdollistavilla teknisillä laitteilla olisi sallittua ainoastaan lyhytaikaisesti sellaisissa tilanteissa, joissa tietolähteen turvallisuutta ei voitaisi muin viranomaistoimin riittävän tehokkaasti taata tai tietolähteen turvaaminen olisi muilla keinoin lähes mahdotonta. Yksittäistapauksellisuudella tarkoitettaisiin sitä, että toimenpide rajoittuisi johonkin yksittäiseen tiedonhankintaa koskevaan tapahtumaan. Toimenpi-

teen välttämättömyyttä ilmentäisi se, ettei tietolähteen turvallisuutta millään muulla keinoin pystyttäisi turvaamaan.

Päätöksentekijällä tulisi olla riittävä perehtyneisyys tietolähdetoimintaan. Tätä ilmentäisi muun muassa se, että toimenpiteestä päättäisi tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Kyseisen poliisimiehen päätöksen lisäksi turvakuuntelun ja -katselun tulisi perustua tietolähteen suostumukseen. Tietolähteen tulisi olla henkilökohtaisilta ominaisuuksiltaan sellainen, että hän kykenisi toimimaan luontevasti, vaikka hänen yllään olisi turvakuuntelun mahdollistava tekninen laite.

Kyseisen toimenpiteen tarkoituksena on ainoastaan tietolähteen turvaaminen. Näin ollen sillä ei saisi kiertää teknistä kuuntelua ja katselua. Tätä ilmentäisi se, että kuuntelu- ja katselutallenteet olisi hävitettävä heti sen jälkeen, kun niitä ei tarvita tietolähteen turvaamiseen.

26 §. *Paikkatiedustelu.* Pykälässä säädettäisiin paikkatiedustelun määritelmästä.

Paikkatiedustelulla tarkoitettaisiin muussa kuin vakituiseen asumiseen käytettävässä tilassa tai sellaisessa tilassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

Toimivaltuus olisi uusi. Paikkatiedustelu toteutettaisiin lähtökohtaisesti salaa niin, ettei paikan omistaja, haltija tai muu henkilö tietäisi suojelupoliisin käyvän siellä. Tätä ilmentää välillisesti myös tiedustelumenetelmän nimi, paikkatiedustelu.

Paikkatiedustelu kohdistuisi määritelmänsä mukaisesti paikkaan tai tilaan. Se voisi ensinnäkin kohdistua pakkokeinolain 8 luvun 1 §:n 4 momentissa tarkoitettuun paikkaan. Lainkohdan mukaan paikanetsinnällä tarkoitetaan etsintää, joka toimitetaan muussa kuin mainitun pykälän 2 tai 3 momentissa tarkoitetussa paikassa, vaikka siihen ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty etsinnän toimittamisajankohtana, taikka jonka kohteena on kulkuneuvo.

Toiseksi paikkatiedustelu voisi kohdistua rikoslain 24 luvun 11 §:ssä tarkoitetussa kotirauhan suojaamaan paikkaan, mutta ei kuitenkaan vakituiseen asumiseen käytettävään tilaan. Näin ollen paikanetsinnän kohteena voisivat olla loma-asunnot ja muut asumiseen tarkoitetut tilat, kuten hotellihuoneet, teltat, asuntovaunut ja asuttavat alukset, sekä asuintalojen porraskäytävät ja asukkaiden yksityisaluetta olevat pihat niihin välittömästi liittyvine rakennuksineen. Jos kuitenkin ilmenisi, että jotain paikkaa tai tilaa käytettäisiin vakituiseen asumiseen, niin paikkatiedustelua ei saisi sinne kohdistaa.

Paikkatiedustelu ei kuitenkaan saisi kohdistaa rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan asuntoon, jollei voitaisi osoittaa paikkaa tosiasiallisesti käytettävän muuhun kuin pysyväluonteiseen asumiseen (PeVL 36/1998 vp, KKO 2009:54).

Paikkatiedustelua ei saisi kohdistaa myöskään sellaiseen tilaan, jossa tilatiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta. Säännöksessä tarkoitettuja paikkoja olisivat esimerkiksi lääkärin vastaanotot, asianajo- ja lakiasiaintoimistot, mediatalot ja lehtien toimitukset, uskonnonvapauslaissa (453/2003) tarkoitetun rekisteröidyn uskonnollisen yhdyskunnan papin tilat, palvelinkeskukset, joiden voidaan olettaa siirtävän lainkohdassa tarkoitettua vaitiolovelvollisuuden tai -oikeuden alaista tietoa. Paik-

katiedustelun hyväksyttävyyttä perusoikeuksien näkökulmasta arvioidaan tarkemmin säätämisjärjestystä koskevassa jaksossa.

Paikkatiedustelun kohteena voisi esimerkiksi olla suljettu kulkuneuvo, jota ei käytetä vakituiseen asumiseen. Esineen tai asiakirjan löytämiseksi ja jäljentämiseksi auton tavaratilaan tai hansikaslokeroon kohdistuva salassa tehtävä etsintä olisi tyyppiesimerkki paikkatiedustelusta. Muina esimerkkeinä paikkatiedustelun piiriin kuuluvista paikoista voidaan mainita hotellihuoneet, teltat, asuntovaunut ja asuttavat alukset, sekä asuintalojen porraskäytävät, myymälät, virastot, kahvilat tai liiketilojen huoneet.

Suljettuun tilaan meneminen saattaisi joissain tapauksissa edellyttää esteen poistamista, kuten esimerkiksi lukitun oven tai lukitun kaapinoven avaamista olosuhteisiin soveltuvalla tavalla.

Ilmaisua "paikka" käytetään yläkäsitteenä, joka käsittää tilat ja muut paikat. Viimeksi mainittuja olisivat lähinnä ulkoalueet. "Tilalla" tarkoitetaan seinin ja usein myös katolla rajattuja paikkoja.

Paikkatiedustelussa tarkoituksena on löytää kansallisen turvallisuuden kannalta olennaista tietoa. Paikkatiedustelussa ei kuitenkaan saisi ottaa haltuun tilassa olevia esineitä, asiakirjoja tai muuta omaisuutta, vaan niitä koskevat tarvittavat tiedot tulisi tallentaa esimerkiksi valokuvaamalla tai jäljentämällä. Jos tilassa oleva esine olisi tarpeen jäljentää, se tulisi jäljentää sellaisella teknisellä laitteella tai menetelmällä, joka ei edellyttäisi esineen haltuun ottamista.

Paikkatiedustelua koskevassa päätöksenteossa tulee kiinnittää erityistä huomiota 1 luvun 2 §:ssä tarkoitettuun perusoikeuksien ja ihmisoikeuksien kunnioittamisen periaatteeseen erityisesti silloin, kun harkitaan paikkatiedustelun kohdistamista kotirauhan suojan alueelle.

Paikkatiedustelusta ilmoittamisesta tiedustelun kohteelle sekä paikan omistajalle tai haltijalle säädettäisiin 46 §:ssä.

27 §. *Paikkatiedustelusta päättäminen.* Pykälässä säädettäisiin paikkatiedustelusta päättämisestä.

Silloin kun paikkatiedustelun kohteena olisi kotirauhan suojaama paikka tai paikka, johon ei ole yleistä pääsyä tai johon yleinen pääsy on rajoitettu tai estetty, paikkatiedustelusta päättäisi tuomioistuin. Toimivaltuuden luonteesta seuraisi, että tuomioistuimen päätöksen perusteella suojelupoliisilla olisi oikeus mennä suljettuun paikkaan oven tai muun kulun estävän esteen lukitus ohittamalla taikka muutoin tarkoitukseen soveltuvalla tavalla olosuhteet huomioon ottaen.

Vaikka paikkatiedustelulla ei puututtaisi kotirauhan suojan ydinalueelle, päätöksentekotoimivallan osoittaminen tuomioistuimelle 1 momentissa tarkoitetuissa tapauksissa on perusteltua paikkatiedustelun vaivihkaisen luonteen johdosta, sillä paikkatiedustelussa ei noudatettaisi kotietsintämenettelyä. Tällöin tiedonhankinnan kohteella ei ole mahdollisuuksia seurata viranomaisen toimintaa vastaavalla tavalla kuin esimerkiksi yleisessä kotietsinnässä tai paikanetsinnässä.

Pykälän 2 momentin mukaan jos 1 momentissa tarkoitettu asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saisi päättää paikkatiedustelusta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia olisi saatettava tuo-

mioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Kiiretilanteen päätöksenteko olisi käytännössä hyvin poikkeuksellisesta, koska Helsingin käräjäoikeuden pakkokeino-osastolla, missä tiedustelumenetelmien käyttämisestä päätettäisiin, on järjestetty ympärivuorokautinen päivystys.

Jos suojelupoliisin päällikkö tai päällystöön kuuluva poliisimies on kiireellisessä tilanteessa tehnyt päätöksen 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 (46 §).

Pykälän 3 momentin mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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. Lisäksi momentin alaan kuuluisivat sellaiset kulkuneuvot, joita ei käytetä vakituiseen asumiseen.

Pykälän 4 momentin mukaan lupa voitaisiin antaa ja päätös tehdä enintään kuukaudeksi kerrallaan.

Paikkatiedustelu on tiedonhankintakeino, jonka tarkoituksena on löytää kansallisen turvallisuuden kannalta olennaista tietoa. Tiedustelun luonteeseen kuuluu se, että tietyssä paikassa ilmenisi tarvetta käydä useammin kuin kerran. Tällaiset tilanteet perustelevat lupa-aikaa eikä päätös paikkatiedustelun käyttämisestä olisi kertaluonteinen, vaikka se voitaisiin tehdä sellaisena. Mainittakoon esimerkkinä tilanne, jossa olisi tarpeen tilatiedustelun yhteydessä jäljentää kansallisen turvallisuuden suojaamiseksi merkityksellisiä asiakirjoja useammin kuin kerran.

Pykälän 5 momentin mukaan paikkatiedustelua koskevassa vaatimuksessa tai päätöksessä olisi riittävällä tarkkuudella yksilöitävä: 1) 3 §:ssä tarkoitettu toiminta; 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 jos paikkatiedustelun aikana ilmenisi, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti lopetettava ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

Ilmaisulla "on tiedustelu siltä osin heti lopetettava" tarkoitettaisiin sitä, ettei tilatiedustelua muilta osin tarvitsisi lopettaa, ellei paikkatiedustelun käytön tarkoitusta ole muutoin saavutettu tai edellytyksiä sen käyttämiselle ei enää ole.

28 §. *Jäljentäminen.* Pykälän mukaan suojelupoliisilla olisi oikeus jäljentää asiakirja tai esine.

Asiakirja tai esine tulisi jäljentää ilman haltuun ottamista siviilitiedusteluoperaation paljastumisriskin minimoimiseksi.

Asiakirja voitaisiin käytännössä jäljentää ottamalla siitä valokuva tai skannaamalla asiakirja esimerkiksi puhelimeen asennetulla skannausohjelmalla. Esineen jäljentämisellä tarkoitettaisiin esimerkiksi tilannetta, jossa olisi tarpeen jäljentää esine käyttämällä 3D-skanneria.

Jäljentäminen koskisi reaalimaailmassa olevia fyysisiä asiakirjoja ja esineitä. Silloin, kun tiedot olisivat tekniseen laitteeseen tallennetussa asiakirjassa, tiedot tulisi hankkia lähtökohtaisesti teknisellä laitetarkkailulla. Muistiinpanojen kirjoittaminen tietokoneen auki jääneeltä näytöltä voitaisiin vielä tehdä jäljentämistoimivaltuutta käyttäen. Jos näytöllä olevat tiedot hankittaisiin teknistä laitetta, kuten esimerkiksi kameraa käyttäen, kyse olisi teknisestä laitetarkkailusta.

29 §. *Jäljentämiskiellot.* Pykälässä säädettäisiin jäljentämiskielloista.

Tiedustelumenetelmillä saatua tietoa ei lähtökohtaisesti ole tarkoitus käyttää rikosprosessissa todisteena. Jäljentämiskielloille ei siten ole vastaavanlaista funktiota tiedustelutoiminnassa kuin mitä niillä on rikosprosessuaalisessa takavarikossa tai jäljentämisessä. Jäljentämiskielloista ei myöskään ole tästä syystä tarkoituksenmukaista säätää yhtenevästi vastaavien takavarikoimis- ja jäljentämiskieltojen sekä todistelukieltoja koskevien säännösten kanssa. Jäljentämiskieltojen taustalla oleva suojeluintressi sen sijaan olisi yhtäläinen.

Pykälän 1 momentin mukaan asiakirjaa tai muuta 26 §:ssä tarkoitettua kohdetta ei saisi jäljentää, jos se sisältää tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n nojalla on velvollisuus tai oikeus kieltäytyä todistamasta. Jäljentämiskieltojen alaan ei kuitenkaan sisällytettäisi oikeudenkäymiskaaren 17 luvun 10 ja 12 §:ää, koska suojelupoliisilla on tehtävänsä toteuttamiseksi tarpeen saada tietoja, jotka koskevat valtion turvallisuutta, Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön sekä tietoja, jotka voivat kuulua virkasalaisuuden piiriin.

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. Hallussa olemista tulkittaisiin vastaavalla tavalla, mitä voimassa olevassa lainsäädännössä. Hallussapito käsittäisi näin myös postin, kuriirin tai muun kolmannen osapuolen kuljetettavana olevan lähetyksen. 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, 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.

30 §. *Telekuunteluun, televalvontaan ja tukiasematietoihin liittyvät jäljentämiskiellot.* Pykälän 1 momentin mukaan sähköisen viestinnän palveluista annetun lain 3 §:n 27 kohdassa tarkoitetun teleyrityksen (teleyritys) tai mainitun lain 3 §:n 36 kohdassa tarkoitetun yhteisötilaajan hallusta ei saisi 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.

Pykälä liittyisi tiedustelumenetelmien käytön tarkoitussidonnaisuuteen sekä siihen, että perusoikeuksiin puuttuvan luonteensa vuoksi telekuuntelu, televalvonta ja matkaviestimien sijaintitiedon hankkiminen ovat korkeamman päätöksentekokynnyksen takana kuin jäljentäminen. Pykälässä säädettävä kielto olisi selvyyden vuoksi tarpeen sen korostamiseksi, ettei jäljentämisellä saisi kiertää teletiedustelumenetelmien käyttöä sekä niille säädettyjä korkeampia käyttöedellytyksiä.

31 §. *Lähetyksen jäljentäminen*. Pykälän mukaan suojelupoliisilla olisi oikeus jäljentää kirje tai muu lähetys ennen sen saapumista vastaanottajalle.

Kirje pitäisi sisällään ainakin postilaissa (415/2011) tarkoitetun kirjelähetyksen, jolla tarkoitetaan kuljetettavaksi jätettyä osoitteellista, enintään kahden kilogramman painoista lähetystä, joka sisältää fyysisellä alustalla olevan viestin. Muulla lähetyksellä tarkoitettaisiin postipakettia eli yleispalveluun kuuluvaa osoitteellista tavaralähetystä, joka on jätetty kuljetettavaksi. Muu lähetys pitäisi sisällään myös yli kahden kilogramman painoisen kirjelähetyksen.

Kirjelähetyksen fyysinen alusta voisi olla minkälaatuinen tahansa. Lähetyksen jäljentämisen ulkopuolelle jäisivät kuitenkin sähköiset viestit, joiden saamiseen käytettäisiin muuta toimivaltuutta. Sähköisiin viesteihin rinnastettavia ovat esimerkiksi digitaalisessa muodossa muistitikulla tai CD-levyllä lähetettävät viestit. Ehdotuksessa tarkoitetaan siten vain fyysisiä postilähetyksiä, ei sähköisessä muodossa välitettäviä viestejä. Näin ollen viestin tulisi olla viimeistään jakeluvaiheessa fyysisessä muodossa.

Lähetyksen ominaisuuksiin kuuluu määritelmän mukaan se, että se on jätetty kuljetettavaksi. Kirjelähetykseen sisältyvä viesti voidaan jättää kuljetettavaksi esimerkiksi kuoressa tai postikorttina. Kirjelähetykset voidaan erottaa pakettilähetyksistä sen perusteella, missä muodossa ne yleensä lähetetään. Kuori voi olla perinteinen kirjekuori taikka muu, esimerkiksi muovista valmistettu kääre.

Menetelmällisesti jäljentämisessä olisi osin kyse vastaavantyyppisestä toimenpiteestä kuin pakkokeinolain 7 luvun 5 §:ssä (Lähetyksen takavarikoiminen ja jäljentäminen). Lähetyksen jäljentämisessä siviilitiedustelussa olisi kuitenkin kyse kohteelta salaa tehtävästä lähetyksen jäljentämisestä. Siitä ilmoittamisesta tiedonhankinnan kohteena olevalle henkilölle säädetään 47 §:ssä.

32 §. *Lähetyksen pysäyttäminen jäljentämistä varten.* Pykälän 1 momentin mukaan jos olisi syytä olettaa, että kirje tai muu vastaava lähetys, joka voidaan jäljentää, on tulossa postin toimipisteeseen, rautatieliikennepaikkaan tai sen osaan tai lähetysten kuljetusta ammatikseen liikennöinnin yhteydessä tai muuten harjoittavan toimipaikkaan taikka on jo siellä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa määrätä lähetyksen pidettäväksi mainitussa toimipaikassa, kunnes jäljentäminen on ehditty suorittaa.

Momentti vastaisi osin pakkokeinolain 7 luvun 6 §:n 1 momentin sääntelyä. Tavaraliikenteen osalta edellytyksenä olisi, 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.

Momentin lopussa "mainitulla toimipaikalla" viitattaisiin kaikkiin momentissa mainittuihin paikkoihin eli postin toimipisteeseen, rautatieliikennepaikkaan tai sen osaan tai lähetysten kuljetusta ammatikseen liikennöinnin yhteydessä tai muuten harjoittavan toimipaikkaan.

Pykälän 2 momentin mukaan määräys annettaisiin enintään kuukauden määräajaksi, joka alkaa siitä, kun 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.

Toimipaikalla viitattaisiin 1 momentissa tarkoitettuihin toimipaikkoihin.

Pykälän 3 momentin mukaan 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.

33 §. *Jäljentämisestä päättäminen.* Pykälän 1 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi jäljentämisestä. Perehtyneisyysvaatimus johtuisi siitä, että olisi erityisen tärkeää osata tehdä rajanveto jäljentämisen ja muiden tiedustelumenetelmien, kuten teknisen laitetarkkailun välillä. Näihin liittyisi olennaisesti jäljentämiskieltojen hallitseminen. Koulutuksella voidaan myös vähentää tiedonhankinnan paljastumisen riskiä sekä edistää toiminnan tuloksellisuutta.

Pykälän 2 momentin mukaan jos asia ei siedä viivytystä, myös muu kuin 1 momentissa tarkoitettu suojelupoliisin poliisimies saisi yksittäistapauksessa päättää jäljentämisestä, kunnes 1 momentissa tarkoitettu poliisimies on ratkaissut asian. Asia olisi saatettava mainitun poliisimiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedonhankintakeinon käytön aloittamisesta.

Siviilitiedustelussa voi tulla eteen tilanteita, ettei tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies ole aina operatiivisessa toiminnassa mukana tai että paikkatiedustelu olisi tehtävä sellaisissa olosuhteissa, ettei päällystöön kuuluvana suojelupoliisin poliisimieheen olisi mahdollista olla yhteydessä. Esimerkiksi näissä tilanteissa olisi tarpeen pystyä tekemään kiirepäätös. Asiakirjan pikaisen jäljentämisen tarve voisi johtua myös tilanteen yllätyksellisyydestä.

34 §. *Jäljennöksen hävittäminen.* Pykälän mukaan tarpeettomaksi osoittautunut jäljennös olisi hävitettävä viipymättä, jos käy ilmi, että jäljentäminen on kohdistunut jäljentämiskiellon alaiseen materiaaliin tai tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi.

Pykälässä tarkoitettu tilanne konkretisoituu lähinnä silloin, kun vasta jäljennöksen ottamisen jälkeen käy ilmi, että jäljentäminen on kohdistunut asiakirjaan tai esineeseen, jota koskee jäljentämiskielto. Tällainen tieto olisi hävitettävä eikä sitä saisi millään tavalla hyödyntää. Hävit-

tämisvelvollisuus luonnollisesti koskisi myös tilannetta, jossa jäljennöksestä tehdyn analyysin perusteella olisi ehditty tallettamaan tietoa suojelupoliisin rekisteriin.

Jäljentämisen kohdistumisesta jäljentämiskiellon alaiseen materiaaliin olisi perusteltua ilmoittaa tiedusteluvaltuutetulle. Lähetyksen jäljentämisen ja viestiin kohdistuvan jäljentämisen ilmoittamisesta sen kohteelle säädettäisiin 47 §:n 1 momentissa.

Jos ilmenisi, että jäljennöksellä ei olisi merkitystä kansallisen turvallisuuden suojaamiseksi, niin jäljennös tulisi myös tässä tapauksessa heti hävittää.

Jäljennöksen hävittämisestä tulisi tehdä merkintä.

35 §. *Menettely tuomioistuimessa.* Pykälään koottaisiin keskeiset tiedustelumenetelmän tuomioistuinkäsittelyä koskevat säännökset. Näitä säännöksiä sovellettaisiin myös tietoliikennetiedustelusta siviilitiedustelussa annetun lain tarkoittamassa tietoliikennetiedustelussa.

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 mitä yleisen alioikeuden istunnosta säädetään. Tiedusteluvaltuutetun oikeudesta olla läsnä lupa-asian käsittelyssä säädetään tiedustelutoiminnan valvonnasta annettavassa laissa.

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 käytön vaatimusta koskisi näin ollen sama kirjallista muotoa edellyttävä 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 kansallisen turvallisuuden vaarantumiseen.

Momentissa säädettäisiin, 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 5 luvun 45 §:n 2 momentin nojalla salaisessa tiedonhankinnassa ja pakkokeinolain 10 luvun 43 §:n 2 momentin perusteella salaisissa pakkokeinoissa. Teknologian ja tietoliikenneyhteyksien salaustekniikoiden kehittymisen myötä voisi olla mahdollista pitää käsittely myös käyttäen videoneuvottelua tai muuta soveltuvaa teknistä tiedonvälitystapaa. Tämä ei kuitenkaan olisi velvoittava säännös ja käsittelyssä tulee aina huomioida 7 momentissa säädetty.

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 luvun 6-8 §:ssä, 11 - 14 §:ssä ja 27 §:ssä yksityiskohtaisesti säädetään.

Tuomioistuin olisi mainittuja seikkoja koskevassa arviossaan yksinomaan suojelupoliisin tuomioistuimelle ilmoittamien tietojen varassa. Tämän takia olisi erittäin tärkeää, että niin lupavaatimuksen kuin lupaa koskevan päätöksen perusteluista ilmenee luvan hakemiseen ja myöntämiseen johtaneet seikat ja oikeudellinen päättely. Vaikka suojelupoliisi toimii virkavastuulla, niin yksiasianosaissuhteeseen perustuva käsittely korostaisi tuomarin aktiivista kyselyoikeuden käyttämisen merkitystä ja selonottovelvollisuutta.

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.

Suojelupoliisin 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 uhkaavasta toiminnasta kuin aikaisemmin myönnetyssä luvassa.

Momentin jälkimmäisen virkkeen mukaiseen tapaukseen liittyvät samanlaiset tarkoituksenmukaisuusnäkökohdat kuin ensimmäisenkin virkkeen tarkoittamissa tilanteissa. Jälkimmäinen virke koskisi siis tilanteita, jossa suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies on väliaikaisesti päättänyt tiedustelumenetelmän käytöstä 7 §:n 1 momentin, 11 §:n 1 momentin, 12 §:n 1 momentin, 13 §:n 1 momentin tai 27 §:n 2 momentin nojalla sekä tilanteita, jossa suojelupoliisin päällystöön kuuluva poliisimies on väliaikaisesti päättänyt tiedustelumenetelmän käytöstä 8 §:n 1 momentin tai 14 §:n 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 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).

36 §. *Siviilitiedustelun suojaaminen.* Pykälässä säädettäisiin tiedonhankinnan suojaamisesta vastaavalla tavalla kuin 5 luvun 46 §:n 2 ja 3 momentissa. Kyseisen 46 §:n 1 momentissa tarkoitetusta puuttumisen siirtämisestä ei olisi tarpeen säätää 5 a luvussa, koska suojelupoliisin poliisimiehen puuttumis- tai toimimisvelvollisuus tulisi katettua poliisin hallinnosta annetun lain 15 c §:n 3 momentissa ja tämän luvun 44 §:ssä olevalla sääntelyllä.

Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa on kyse niin sanotusta jokaiselle poliisimiehelle kuuluvasta toimimisvelvollisuudesta. Poliisimiehen toimimisvelvollisuuden syntymiselle on myös asetettu eräitä edellytyksiä, kuten kiireellisyys ja välttämättömyys. Vakavan rikoksen estäminen ja tutkinnan aloittaminen saattaa tarkoittaa pelkästään ilmoituksen tekemistä alueella toimivalle poliisiyksikölle. Velvollisuus sisältää ainakin ne vähimmäistoimenpiteet, jotka on välttämättä suoritettava säännöksessä tarkoitetun tuloksen saavuttamiseksi. Poliisimiehen toimimisvelvollisuus on siis mahdollista täyttää esimerkiksi tekemällä hälytyskeskukselle ilmoitus antaen asiaa koskevat tarvittavat tiedot. Tässä yhteydessä ei ole tarpeen ilmoittaa sellaisia tietoja, jotka saattaisivat johtaa siviilitiedustelun paljastumiseen tai aiheuttaa työturvallisuusriskin. Esimerkiksi jos tilanne edellyttäisi, niin ilmoituksen voisi tehdä käyttäen peitehenkilöllisyyttä tai ilmoituksen voisi tehdä myös anonyymisti.

Mainitun lain 15 c §:n 3 momentissa tarkoitettu vakavan rikoksen käsite on riippuvainen ensinnäkin tilanteesta kokonaisuudessaan ja myös rikoksen kohteena olevasta henkilöstä ja tämän mahdollisuuksista puolustautumiseen. Jos rikos on kohdistumassa pieneen lapseen tai sairauden, iän tai muun syyn vuoksi puolustuskyvyttömään henkilöön, tämän mahdollisuudet puolustautua ovat vähäiset, jolloin tämä edellyttäisi intensiivisempää toimimisvelvollisuutta siviilitiedustelua hoitavalta poliisimieheltä kuin jos kyse olisi rikoksen kohdistumisesta puolustuskykyiseen aikuiseen henkilöön. Kyse on aina tapauskohtaisesta harkinnasta.

Tässä luvun 44 § (Tiedon luovuttaminen rikostorjuntaan) sääntely olisi erityissäännös suhteessa poliisin hallinnosta annetun lain 15 c §:n 3 momenttiin nähden, koska se muodostaa toimimisvelvollisuuden osalta kvalifioidun velvollisuuden puuttua sellaisiin rikoksiin, joista säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta (44 §:n 1 ja 2 momentti). Tämä liittyy poikkeuksetta tilanteeseen, jolloin suojelupoliisin poliisimies on virantoimituksessa, koska 44 §:ssä tarkoitetaan tilanteita, jolloin tiedustelumenetelmän käytön aikana ilmenee sellaista tietoa, jonka perusteella olisi mahdollista estää vakava rikos tai luovuttaa merkityksellistä tietoa rikoksen selvittämiseksi. Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa tarkoitetut tilanteet ulottuvat myös virantoimituksen ulkopuolelle poliisimiehen vapaa-ajalle.

Poliisin hallinnosta annetun lain 15 c §:n 3 momentissa säädetty poliisimiehen toimimisvelvollisuus ja 44 §:ää koskeva sääntely eivät muodosta ristiriitaa, vaikka säännöksissä ilmenee kuitenkin vakavan rikoksen estämisen kohdalla päällekkäisyyttä. Tiedon luovuttamisessa rikostorjuntaan olisi kyse tarvittavien tietojen luovuttamisesta rikoksen estämiseksi tai selvittämiseksi, jotta toimivaltainen viranomainen voisi ryhtyä tarvittaviin toimiin. Ilmoitusvelvollisuus tai -oikeus perustuisi kuitenkin tiedustelumenetelmän käytön aikana saatuihin tietoihin,

kun taas poliisimiehen toimimisvelvollisuus on riippumaton ajasta, paikasta ja siitä onko poliisimies virantoimituksessa vai ei. Tiedustelumenetelmien käytön aikana ilmenevän rikoksen kohdalla poliisimiehen toimimisvelvollisuus tulisi lähtökohtaisesti täytettyä 44 §:n mukaan tehtävällä ilmoituksella. Jos siviilitiedustelua toteuttava poliisimies voisi operaatioturvallisuuden sekä työturvallisuuden mahdollistaessa puuttua henkilökohtaisesti vakavan rikoksen estämiseen, 44 §:n sääntely ei tätä estäisi.

Pykälän 1 momentin mukaan suojelupoliisi saisi käyttää vääriä, harhauttavia tai peiteltyjä tietoja, tehdä ja käyttää vääriä, harhauttavia tai peiteltyjä rekisterimerkintöjä sekä valmistaa ja käyttää vääriä asiakirjoja, kun se on välttämätöntä siviilitiedustelun suojaamiseksi.

Suojaus voitaisiin antaa ainoastaan virkamiehelle. Ilmaisu "siviilitiedustelun suojaamiseksi" kattaisi jo toteutetun, käynnissä olevan ja tulevaisuudessa toteutettavan tiedustelumenetelmän käytön lisäksi myös muun siviilitiedusteluun liittyvän toiminnan. Tämä tarkoittaisi muun muassa sitä, että siviilitiedustelutehtävään määrätty virkamies voisi käyttää vääriä tai harhauttavia henkilötietoja niin kauan kuin se olisi välttämätöntä siviilitiedustelutehtävän hoitamiseksi. Momentin nojalla ei voitaisi kuitenkaan luoda tietolähteelle tai sivulliselle uutta identiteettiä. Kovin kevyesti suojausta ei saa tehdä siihen liittyvien erilaisten ongelmien ja oikeusturvasyiden johdosta. Esimerkiksi väärän asiakirjan käytöstä aiheutuu vääränsisältöinen rekisterimerkintä viranomaisen rekisteriin. Väärillä rekisterimerkinöillä ja väärillä asiakirjoilla tarkoitettaisiin nimenomaan viranomaisen asiakirjoja ja rekistereitä. Suojauksen tekemisen tulee siksi olla välttämätöntä.

Pykälän 2 momentin mukaan edellä 1 momentissa tarkoitettu rekisterimerkintä olisi oikaistava sen jälkeen, kun momentissa tarkoitettuja edellytyksiä ei enää ole. Rekisterimerkintä olisi siis oikaistava sen jälkeen kun momentissa tarkoitettuja edellytyksiä ei enää ole eli suojausta ei enää tarvita tai se ei ole enää välttämätöntä. Ehdotettava sääntely vastaisi tältä osin asiallisesti 5 luvun 46 §:n 3 momenttia.

37 §. *Suojaamisesta päättäminen.* Pykälän 1 momentin mukaan suojelupoliisin päällikkö päättäisi 36 §:n 1 momentissa tarkoitetun rekisterimerkinnän tekemisestä sekä asiakirjan valmistamisesta. Päätöksentekoa koskeva sääntely vastaisi lain 5 luvun 47 §:n 1 momentin sääntelyä.

Pykälän 2 momentin mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi muusta kuin 1 momentissa tarkoitetusta suojaamisesta.

Esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta annetun valtioneuvoston asetuksen 19 §:n mukaan suojelupoliisin päällikkö määrää harhauttavien tai peiteltyjen rekisterimerkintöjen ja väärien asiakirjojen käyttämisestä vastaavan tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen pidättämiseen oikeutetun poliisimiehen.

Pykälän 3 momentin mukaan rekisterimerkintöjen tekemisestä sekä asiakirjojen valmistamisesta päättäneen viranomaisen olisi pidettävä luetteloa merkinnöistä ja asiakirjoista, valvottava niiden käyttöä sekä huolehdittava merkintöjen oikaisemisesta.

Säännös vastaisi asiallisesti 5 luvun 47 §:n 3 momenttia. Tässä momentissa tarkoitettuun luetteloon ei saisi kohdistaa 36 §:n 1 momentissa tarkoitettuja toimenpiteitä.

38 §. *Ilmaisukielto.* Pykälän 1 momentin 1 virkkeen mukaan tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa kieltää si-

vullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä, jos se on perusteltua tiedustelumenetelmän käytön suojaamiseksi.

Tiedustelumenetelmän käytön perusteena on aina, että siviilitiedustelun kohteena oleva toiminta vakavasti uhkaa kansallista turvallisuutta. Tiedustelumenetelmää käytettäessä on mahdollista joutua tilanteeseen, joissa ulkopuolinen apu on tarpeen tai jopa välttämätöntä. Esimerkiksi paikkatiedustelussa voi olla tarpeen pyytää taloyhtiön huollosta vastaavan yhtiön palveluksia. Näin ollen sivulliset voivat saada tietoja, joiden ilmaiseminen voi vaarantaa ainakin tiedustelumenetelmän käytön, mutta samalla muodostaa uhkan kansalliselle turvallisuudelle. Tarkoitus olisi minimoida riski tiedustelumenetelmän käytön paljastumisesta sekä suojata samalla myös salassa pidettäviä taktisia ja teknisiä menetelmiä ja viime kädessä kansallista turvallisuutta.

Pykälän 1 momentin 2 virkkeen mukaan edellytyksenä olisi lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytön toteuttamisessa. Ilmaisukieltoa ei siten voitaisi antaa kenelle tahansa henkilölle, esimerkiksi taloyhtiön asukkaalle tai muulle sivulliselle, joka sattumalta havaitsee teknisen tarkkailun laitteen asennuksen.

Säännöksessä tiedustelumenetelmän käytöllä tarkoitettaisiin tiedustelumenetelmien käyttöä laajemmin, joka pitäisi esimerkiksi sisällään siviilitiedustelussa sekä sotilastiedustelussa käytettävien tiedustelumenetelmien käytön suojaamisen silloin, kun suojelupoliisi ja sotilastiedusteluviranomainen toimisivat yhteistyössä. Ilmaisukielto olisi perusteltua antaa ainakin silloin, jos tiedustelumenetelmän käyttö saattaisi paljastua ilman kiellon määräämistä sivulliselle.

Pykälän 2 momentin mukaan ilmaisukielto annettaisiin enintään vuodeksi kerrallaan. Kielto olisi annettava saajalleen kirjallisena todisteellisesti tiedoksi. Siinä olisi yksilöitävä kiellon kohteena olevat seikat, mainittava kiellon voimassaoloaika ja ilmoitettava sen rikkomiseen liittyvästä rangaistusuhasta. Momentin sääntely vastaisi 5 luvun 48 §:n 2 momentin sääntelyä.

Pykälän 3 momentissa säädettäisiin ilmaisukieltoa koskevan päätöksen valituskiellosta. Säännöksen mukaan ilmaisukieltoa koskevaan päätökseen ei saisi hakea muutosta valittamalla. Kiellon saanut saisi kuitenkin ilman määräaikaa kannella päätöksestä. Kantelu olisi käsiteltävä kiireellisenä.

Ilmaisukieltoa koskevasta päätöksestä tulisi aina ilmoittaa tiedusteluvaltuutetulle 57 §:n 2 momentin mukaisesti.

Ilmaisukieltoa koskevaan päätökseen olisi sisällytettävä ilmoitus siitä, minkä säännöksen nojalla valittaminen ei ole mahdollista. Valituskielto ei estäisi ilmaisukiellon saanutta ilmoittamasta ilmaisukiellon määräämisestä tiedusteluvaltuutetulle.

Ilmaisukieltopäätöksen valituskieltoa on käsitelty jäljempänä otsikon suhde perustuslakiin ja säätämisjärjestys alla.

Pykälän 4 momentin mukaan rangaistus ilmaisukiellon rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta. Momentin sääntely vastaisi 5 luvun 48 §:n 3 momentin sääntelyä.

Pykälän 5 momentissa säädettäisiin ilmaisukiellon saaneen oikeudesta 4 momentin estämättä ilmoittaa saamastaan ilmaisukiellosta tiedusteluvaltuutetulle. Tämä olisi perusteltua ilmaisu-

kiellon saaneen oikeusturvan vuoksi. Näin jokainen ilmaisukiellon kohteena oleva voisi ilmaisukiellon estämättä ilmoittaa tiedusteluvaltuutetulle oman näkemyksensä ilmaisukiellosta.

39 §. *Tiedustelumenetelmän käytöstä päättäminen eräissä tapauksissa.* Pykälän 1 momentin mukaan muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättäisi suojelupoliisin päällikkö.

Suojelupoliisin päällikkö toisin sanoen tekisi operatiivisen tason päätöksen siviilitiedustelun toteuttamisesta ulkomailla sekä sen yhteydessä käytettävistä tiedustelumenetelmistä. Ulkomaan tiedusteluun liittyvien ulkopoliittisten herkkyyksien johdosta päätöksenteossa olisi otettava huomioon tiedonhankinnalle asetetut prioriteetit sekä 58 §:n sääntely ja sen nojalla asetetut suuntaviivat.

Pykälän 2 momentin mukaan tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatettaisiin mitä esityksestä, suunnitelmasta, luvasta tai päätöksestä tässä luvussa säädetään.

Muualla kuin Suomessa käytettävää tiedustelumenetelmää koskevaan päätökseen tulisi kirjata vastaavat tiedot, mitä esitykseen, suunnitelmaan, vaatimukseen tai päätökseen tulee kirjata silloin, kun tiedustelumenetelmää käytetään Suomessa.

Pykälän 3 momentin mukaan tämän luvun 4 §:n 4 momentin, 16 §:n 3 momenttia, 41, 44, 46 ja 47 §:n säännöksiä voitaisiin soveltaa 1 momentissa tarkoitettuun siviilitiedusteluun ja tiedustelumenetelmän käyttöön.

Suojelupoliisin harkintavaltaa sekä tiedustelumenetelmien käyttöä myös ulkomaan tiedustelussa ohjaavat poliisioikeudelliset periaatteet, joiden merkitystä siviilitiedustelussa käsitellään tarkemmin 2 §:n perusteluissa. Erityisesti perus- ja ihmisoikeuksien kunnioittamisen periaatteen merkitys on ulkomaan tiedustelussa tärkeässä asemassa. Ulkomaan tiedustelussa EIS:n säännökset voivat osin muodostaa tulkintaperustan erityisesti silloin, jos aluevaltion oikeusjärjestelmä, kulttuuri ja olosuhteet eivät vastaa länsimaista. Ihmisoikeuslähtöistä argumentaatiota voitaisiin käyttää tulkintaa ohjaavana apuvälineenä ulkomaan tiedustelutoiminnassa.

Perustuslain 2 §:n 3 momentista yhdessä 22 §:n kanssa seuraa, että suomalainen virkamies ei voi ulkomaillakaan ollessaan toimia tavalla, joka loukkaa perus- ja ihmisoikeuksia. Ulkomaan tiedusteluun liittyvien herkkyyksien vuoksi olisi kuitenkin yksittäistapauksellisesti perusteltua, ettei momentissa erikseen mainittuja lainkohtia olisi aina tarpeen soveltaa. Tätä ilmentäisi ilmaisu "voidaan soveltaa". Tämä antaisi suojelupoliisin päällikölle harkintavallan arvioida, milloin säännöksiä voitaisiin soveltaa ja milloin niiden soveltaminen ei olisi perusteltua.

Luvun 4 §:n 4 momentissa säädetään kiellosta kohdistaa tiedustelumenetelmän käyttö vakituiseen asumiseen käytettävään tilaan. Lähtökohtana olisi, ettei ulkomaan tiedustelussakaan tiedustelumenetelmän käyttöä voitaisi kohdistaa kenenkään asuntoon. Rajanveto ulkomaan tiedustelussa saattaisi muodostua lähes mahdottomaksi määritellä ainakin sellaisissa tilanteissa, kun ulkomaan tiedustelua suoritettaisiin heikoimmin kehittyneessä maassa tai alikehittyneessä maassa, missä infrastruktuuri ei mahdollista asunnon käyttötarkoituksen selvittämistä viranomaisen ylläpitämistä rekistereistä.

Lähtökohtana on, ettei 16 §:ssä tarkoitettuja asennuksia tehtäisi pykälän 3 momentin piiriin kuuluvissa tiloissa. Ulkomaan tiedustelussa olisi kuitenkin tarpeen päästä tekemään asennuksia tiedustelutoimivaltuuksien käytön mahdollistamiseksi esimerkiksi palvelinkeskuksiin, joissa kytkentöjen tekeminen mahdollistaisi telekuuntelun ja -valvonnan käyttämisen.

Luvun 29 §:ssä säädetään jäljentämiskielloista ja 41 §:ssä säädetään kuuntelu- ja katselukielloista, jotka tulisivat myös harkinnanvaraisesti sovellettavaksi ulkomaan tiedustelutoiminnassa.

Luvun 46 §:ssä säädetään kiiretilanteessa saadun tiedon hävittäminen. Kyseinen säännös ei ulkomaan tiedustelussa tulisi sovellettavaksi, koska suojelupoliisin päällikkö päättäisi poikkeuksetta jokaisen tiedustelumenetelmän käytöstä.

Luvun 47 §:ssä säädetään tiedustelumenetelmän käytöstä ilmoittaminen. Pykälän 1 momentissa säädettäisiin velvollisuudesta ilmoittaa siinä mainittujen tiedustelumenetelmien käytöstä tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu. Tiedustelumenetelmän käytöstä ilmoittaminen sen kohteelle ulkomaan tiedustelussa paljastaisi tiedustelutoiminnan käyttämisen toisen valtion alueella, joka voisi vahingoittaa valtioiden välisiä suhteita. Tämä puoltaisi ilmoituksen tekemättä jättämistä ottaen huomioon, että suomalaisella tuomioistuimella ei ole toimivaltaa päättää ulkomaan tiedustelussa käytetyn tiedustelumenetelmän käytön ilmoittamisen lykkäämisestä tai kokonaan ilmoittamatta jättämisestä yhtä lailla, kun sillä ei ole toimivaltaa päättää tiedustelumenetelmän käyttämisestäkään. Näin ollen ilmoituksen tekemistä koskevan päätöksen harkinta jäisi kokonaan suojelupoliisille.

40 §. *Määräaikojen laskeminen.* Pykälän 1 momentin mukaan tässä luvussa 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 päättyy, määräaika päättyy kuukauden viimeisenä päivänä.

Pykälä vastaisi asiallisesti voimassa olevan lain 5 luvun 49 §:n sääntelyä.

41 §. *Kuuntelu- ja katselukiellot.* Pykälän 1 momentin mukaan telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua ja teknistä katselua ei 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 ja antaessaan oikeudellista neuvontaa oikeudenkäynnin käynnistämiseksi tai sen välttämiseksi. Lisäksi pykälässä säädetään asianajajista ja luvan saaneista oikeudenkäyntiavustajista annetuissa laeissa 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. Oikeudenkäymiskaaren 22 §:n 2 momentin sisältämä viittaus 11 §:n 2 ja 3 momentteihin ei tässä soveltuisi, koska oikeudenkäymiskaaren 11 §:ään liittyvästä nimenomaisesta kuuntelu- ja katselukiellosta ei muutenkaan esitetä säädettäväksi. Tähän liittyvästä tiedustelukiellosta ehdotetaan säädettäväksi siviilitietoliikennetiedustelulain 12 §:ssä.

Pykälän 1 momentissa tarkoitettua tiedustelumenetelmää ei myöskään saisi asentaa (16 §) käytettäväksi sellaisessa paikassa, jossa tiedustelun kohteeksi voitaisiin olettaa joutuvan 1 momentissa tarkoitettua tietoa, josta on momentissa tarkoitettu velvollisuus tai oikeus kieltäytyä todistamasta ja kyseinen kieltäytymisvelvollisuus tai -oikeus nauttisi Suomen perustuslaissa säädettyä perusoikeuksien suojaa. Tällaisia paikkoja olisivat esimerkiksi lääkärin vastaanotot, asianajo- ja lakiasiaintoimistot, mediatalot ja lehtien toimitukset, uskonnonvapauslaissa (453/2003) tarkoitetun rekisteröidyn uskonnollisen yhdyskunnan papin tilat ja sellaiset palvelinkeskukset, joiden voidaan olettaa siirtävän lainkohdassa tarkoitettua vaitiolovelvollisuuden tai -oikeuden alaista tietoa.

Pykälän 2 momentin mukaan jos telekuuntelun, telekuuntelun sijasta tapahtuvan tietojen hankkimisen, teknisen kuuntelun tai teknisen katselun aikana tai muulloin ilmenee, että kyseessä olisi viesti, jonka kuuntelu ja katselu on kielletty, toimenpide olisi keskeytettävä ja sillä saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Velvollisuus hävittää tiedot heti täydentäisi kuuntelu- ja katselukiellon noudattamista. Jos tiedonhankinnassa selviää, että ensimmäisessä momentissa tarkoitettua tiedustelumenetelmien kohdistamiskieltoa on loukattu, tulisi 2 momentissa asetettua tallenteita ja muistiinpanoja koskevaa hävittämisvelvollisuutta noudattaa heti kun viestinnän tiedustelukiellonalaisuus on käynyt ilmi.

Pykälän 3 momentin mukaan tässä pykälässä tarkoitetut kuuntelu- ja katselukiellot eivät kuitenkaan koskisi tapauksia, joissa 1 momentissa tarkoitettu henkilö osallistuu siviilitiedustelun kohteena olevaan toimintaan ja myös hänen osaltaan olisi tehty päätös telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, teknisestä kuuntelusta tai teknisestä katselusta. Nyt kyseessä olevassa momentissa sallittaisiin poiketa 1 momentissa tarkoitetusta tiedustelumenetelmien kohdistamiskiellosta tilanteissa, joissa tiedusteluimmuniteettia nauttiva viestinnän osapuoli joko itse osallistuu siviilitiedustelun kohteena olevaan toimintaan, joka vakavasti uhkaa kansallista turvallisuutta tai toimintansa kautta muutoin vaarantaa sitä. Poikkeaman soveltaminen olisi siitä riippumatonta, mistä 3 §:ssä tarkoitetusta siviilitiedustelun kohteena olevasta toiminnasta on kyse. Kuuntelu- ja katselukiellosta vapaa tiedustelumenetelmien käyttö ei toisin sanoen edellyttäisi sellaista välitöntä liityntää samaan toimintaan kuin mistä pakkokeinolain 10 luvun 52 §:n 4 momentissa rikosta koskevassa asiayhteydessä säädetään.

42 §. *Tallenteiden ja asiakirjojen tarkastaminen.* Pykälän mukaan suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen olisi ilman aiheetonta viivytystä tarkastettava tiedustelumenetelmän käytössä kertyneet tallenteet ja asiakirjat.

Tiedustelumenetelmien ja niiden suojaamisen sääntelyä koskevat ehdotukset rakentuvat sille lähtökohdalle, että suojelupoliisin päällystöön kuuluva poliisimies on keskeisessä asemassa

näitä toimenpiteitä toteutettaessa ja on velvollinen valvomaan niiden lainmukaista suorittamista. Näin ollen ehdotetaan, että hänen tulisi huolehtia myös tallenteiden ja asiakirjojen tarkastamisesta.

Mikäli suojelupoliisin päällystöön kuuluva poliisimies määräisi muun virkamiehen tarkastamaan tallenteita ja asiakirjoja, määräyksen antaja vastaisi siitä, että kyseisellä virkamiehellä on tarvittavat tiedot ja taito sekä kokemus tehtävän suorittamiseksi.

Tarkastamisvelvollisuus koskisi kaikkia tiedustelumenetelmiä. Tämä liittyisi siihen, että tarkastamisella on olennainen merkitys siltä kannalta, että toiminnasta vastaava suojelupoliisin päällystöön kuuluva poliisimies voi tosiasiallisesti valvoa keinojen lainmukaista käyttämistä. Tallenteista sekä asiakirjoista olisi poistettava muun muassa tiedustelukieltojen alainen materiaali sekä muu aineisto, jota sotilastiedusteluviranomainen ei saisi hankkia tiedustelumenetelmän käytöllä. Viivytyksetön tarkastaminen on tarpeen muun muassa tiedustelukieltojen alaisen aineiston toteamiseksi ja hävittämiseksi.

Tallenteiden 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.

Pykälä vastaisi asiallisesti 5 luvun 51 §:n sääntelyä.

43 §. *Tallenteiden tutkiminen.* Pykälän mukaan tiedustelumenetelmien käytössä kertyneitä tallenteita saisi tutkia vain tuomioistuin ja suojelupoliisin päällystöön kuuluva poliisimies. Suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saisi tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

Pykälä vastaisi 5 luvun 52 §:n sääntelyä. Silloin, kun suojelupoliisin päällystöön kuuluva poliisimies määräisi muun virkamiehen tarkastamaan tallenteita ja asiakirjoja, määräyksen antaja vastaisi siitä, että kyseisellä virkamiehellä on tarvittavat tiedot ja taito sekä kokemus tehtävän suorittamiseksi. Käytännössä tarkastavan päällystöön kuuluvan poliisimiehen sekä muun virkamiehen tulisi olla tiedustelumenetelmien käyttöön koulutuksen saanut.

44 §. *Tiedon luovuttaminen rikostorjuntaan.* Pykälässä säädettäisiin niin sanotusta palomuurista. Tiedustelutoimivaltuuksilla saatuja tietoja ei lähtökohtaisesti saisi käyttää muuhun tarkoitukseen kuin kansallisen turvallisuuden suojaamiseksi. Palomuurissa säädettäisiin eräistä poikkeuksista käyttötarkoitussidonnaisuuteen.

Pykälä kattaisi osin myös suojelupoliisin poliisimiehen toimimisvelvollisuuden piiriin kuuluvia asioita. Tältä osin viitataan 36 §:n alla kerrottuun.

Pykälän 1 momentin ensimmäisen virkkeen mukaan suojelupoliisin olisi ilman aiheetonta viivytystä ilmoitettava keskusrikospoliisille, jos tiedustelumenetelmän käytön aikana ilmenee, että voidaan olettaa tehdyksi sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Ilmoitus olisi käytännössä tehtävä heti, kun se on mahdollista. Jos ilmoituksen viivyttämiselle olisi erittäin tärkeä ja perusteltu syy, mahdollistaisi säännös ilmoituksen tekemisen viivyttämisen enintään muutamalla päivällä. Säännös ei asettaisi suojelupoliisille aktiivista velvoitetta seuloa tiedustelumenetelmillä saaduista tiedoista rikoksen selvittämisen kannalta merkityksellistä tietoa, jota ilmentäisi ilmaisu "ilmenee".

Tiedon todennäköisyyttä koskeva ilmaus ”voidaan olettaa” olisi perusteltua asettaa matalaksi. Tässä yhteydessä rikos voidaan olettaa tehdyksi, kun sillä hetkellä olevien tietojen perusteella muodostuu huolellisesti asioita harkitsevalle ihmiselle intuitio tehdystä rikoksesta. Käsillä tulisi lisäksi olla elementtejä sellaisesta rikoksesta, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Kyse ei olisi rikoksen paljastamisen kynnyksestä, koska edellä kerrotulla tavalla ei olisi aktiivista velvoitetta seuloa rikostietoa eikä näin ollen tavoitteena myöskään olisi selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta olemassa.

Suojelupoliisin vastuulla olisi ilmoituksen tekeminen keskusrikospoliisille. Keskusrikospoliisin vastuulla puolestaan olisi huolehtia siitä, että ilmoitus ohjattaisiin edelleen sille viranomaiselle, jolle esitutkinnan toimittaminen kuuluu tai joka päättää esitutkinnan toimittamisesta. Esitutkintaviranomaiset luetellaan esitutkintalain (805/2011) 2 luvun 1 §:ssä. Esitutkinnan toimittamisesta taas päättää eräissä tilanteissa syyttäjä. Esimerkiksi silloin, kun kyseessä olisi ulkomailla tehdyksi epäilty rikos, edellyttää sen tutkiminen Suomessa rikoslain 1 luvun 12 §:n (205/1997) nojalla valtakunnansyyttäjän syytemääräystä. Keskusrikospoliisin tulisi tämänkaltaisessa tilanteessa ohjata ilmoitus edelleen valtakunnansyyttäjänvirastoon samoin kuin epäillyssä poliisirikosasiassa, missä yhteydessä sovelletaan esitutkintalain 2 luvun 4 §:ssä säädettyjä erityisiä tutkintajärjestelyjä.

Momentin ensimmäisessä virkkeessä suojelupoliisille asetettaisiin velvollisuus ilmoittaa niin sanotuista ylitörkeistä rikoksista eli rikoksista, joista säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Tällaisen seuraamusuhan omaavia rikoksia leimaa jo niin merkittävä rikoksen selvittämisintressi ja rikosvastuun toteuttamisintressi, että niistä olisi rikosoikeusjärjestelmän uskottavuuden vuoksi välttämätöntä ilmoittaa toimivaltaiselle viranomaiselle, tässä tapauksessa keskusrikospoliisille.

Ilmoituksen ohella suojelupoliisin tulisi luovuttaa keskusrikospoliisille myös rikosta koskevat tarpeelliset tiedot. Luovutettavien tietojen tarpeellisuus voitaisiin arvioida ensinnäkin siltä kannalta, mitä esitutkinnan käynnistäminen välttämättä edellyttää. Tällaisten tietojen, kuten tapahtumaa ja asianosaisia koskevien tietojen tai muiden esitutkintalain 1 luvun 2 §:n 1 momentissa tarkoitettujen tietojen luovuttaminen tulisi luonnollisesti kyseeseen vain siinä laajuudessa kuin suojelupoliisi on sellaista tietoa tiedustelumenetelmän käytöllä ylipäätään saanut. Tietojen tarpeellisuutta voitaisiin toiseksi arvioida todistelun kannalta, missä yhteydessä olennaista on tieto sellaisista seikoista, jotka epäiltyä rikosta koskevan rangaistusvaatimuksen tueksi on näytettävä.

Momentin toisen virkkeen mukaan ilmoitusta saataisiin suojelupoliisin päällikön päätöksellä siirtää enintään vuodeksi kerrallaan, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Ilmoituksen siirtämiselle asetettaisiin siten korkea kynnys ("välttämätöntä"). Ilmoitusta voitaisiin siirtää enintään yhdeksi vuodeksi kerrallaan. Päätöksiä olisi kuitenkin mahdollista tehdä useampia, jos siihen olisi jokaisella kerralla esittää asianmukaiset perusteet.

Ensimmäinen siirtämistä koskeva päätös tulisi tehdä välittömästi, kun tiedustelumenetelmän käytön aikana ilmenisi säännöksessä tarkoitettua rikostietoa. Jos ilmoittamista olisi perusteltua vuoden määräajan jälkeen jatkaa, uusi päätös tulisi tehdä hyvissä ajoin ennen määräajan päättymistä. Jos määräajan päättymisen ja päätöksen tekemisen väliin jäisi aikaa, seurauksena olisi ensinnäkin se, että tieto tulisi ilman aiheetonta viivytystä luovuttaa keskusrikospoliisille. Toiseksi rauenneen päätöksen ja tehtävän uuden päätöksen väliaikana tiedonhankinnan kohde voisi asianosaisjulkisuuteen vedoten saada tiedon tiedustelumenetelmän käytöstä.

Ilmoituksen siirtäminen olisi ensinnäkin mahdollista, jos se olisi välttämätöntä kansallisen turvallisuuden varmistamiseksi. Kynnys "välttämätöntä" olisi korkea ja sillä tarkoitettaisiin viimesijaisuutta eli sitä, ettei kansallista turvallisuutta voitaisi muilla keinoin yksittäistapauksellisesti varmistaa kuin tekemällä päätös ilmoituksen siirtämisestä. Kyseisellä perusteella voitaisiin turvata tiedonhankinnan saattaminen siihen pisteeseen, ettei siitä ilmoittamisesta aiheudu esimerkiksi suojelupoliisin taktisten tai teknisten menetelmätietojen paljastumista edellyttäen, että niiden paljastuminen muodostaisi uhkan kansalliselle turvallisuudelle. Ilmoituksen siirtämisen perustelu voisi liittyä myös esimerkiksi tarpeeseen välttää ilmoituksesta vääjäämättä käynnistyvä esitutkinta, ja siitä aiheutuva vahinko Suomen kahdenvälisille suhteille samoin kuin Suomen edellytyksille toimia kansainvälisessä yhteistyössä. Kansallisen turvallisuuden varmistaminen tulisi tässä ilmoituksen lykkäämistä koskevassa asiayhteydessään tulkita lähtökohtaisesti samoin kuin valtion turvallisuuden varmistamista on tulkittu salaisen tiedonhankintakeinon käytöstä ilmoittamista koskevan poliisilain 5 luvun 58 §:n 2 momentin nojalla.

Ilmoittamisen siirtäminen olisi toiseksi mahdollista, jos se olisi välttämätöntä hengen tai terveyden suojaamiseksi. Tämä peruste voi esimerkiksi henkilön turvaamiseksi tehtyjen toimenpiteiden vuoksi poistua tietyn ajan kuluttua, jolloin ilmoittaminen tiedustelun kohteelle voitaisiin tehdä. Kyseisellä perusteella voitaisiin myös esimerkiksi turvata tiedonhankinnan saattaminen siihen pisteeseen, ettei siitä ilmoittamisesta aiheudu työturvallisuusriskiä.

Ilmoittamisen siirtämisen muista arviointikriteereistä säädettäisiin 4 momentissa. Ottaen huomioon, että suojelupoliisin siirtämistä koskeva päätös merkitsee poikkeusta lähtökohtana olevaan ilmoitusvelvollisuuteen, olisi siitä perusteltua heti antaa tieto myös tiedusteluvaltuutetulle. Tästä säädettäisiin 61 §:ssä. Tiedusteluvaltuutettu voisi tiedon saatuaan tehdä itsenäisen arvion muun muassa siitä, voidaanko lykkäämispäätöstä pitää tässä momentissa ja 4 momentissa mainittujen kriteerien valossa puolustettavana sekä tarvittaessa käyttää tarkastusoikeuttaan lykkäämispäätösten laillisuuden valvomiseksi.

Momentin kolmannen virkkeen mukaan suojelupoliisi saisi ilmoittaa tehdystä rikoksesta keskusrikospoliisille, jos rikoksesta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta. Momentissa asetettaisiin siis vähintään kolmen vuoden seuraamusuhan mukaan määrittyvä tiedon luovutuskielto rikoksen selvittämiseksi. Tiedot niistä rikoksista, joista säädetty ankarin rangaistus alittaisi kolme vuotta, olisi aina jätettävä rikoksen selvittämisen tarkoituksessa keskusrikospoliisille ilmoittamatta. Ottaen huomioon yhtäältä 1 momentin toisessa virkkeessä säädettäväksi ehdotettava ilmoitusvelvollisuus ja toisaalta tästä virkkeestä johtuva ilmoituskielto, suojelupoliisille jäisi vähintään kolmen vuoden ja enintään kuuden vuoden seuraamusuhkaa kantavien ja jo tehtyjen rikosten osalta harkinnanvaraa siitä, ilmoittaako se tällaisesta rikoksesta keskusrikospoliisille vai ei. Harkinnanvara olisi kuitenkin 3 momentissa mainittuihin arviointikriteereihin sidottua. Ilmoituksen yhteydessä luovutettavien rikosta koskevien tarpeellisten tietojen osalta viitataan edellä todettuun.

Pykälän 2 momentin 1 virkkeen mukaan suojelupoliisin olisi viipymättä ilmoitettava toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee, että hankkeilla on sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä. Toimivaltaisella viranomaisella tarkoitettaisiin esitutkintaviranomaisten lisäksi esimerkiksi hätäkeskusta. Toisin kuin yleensä, velvollisuutta ilmoittaa lainkohdassa tarkoitetusta rikoksesta olisi sidottu "viipymättä" tehtävään ilmoitukseen. Kyseinen virke asettaisi suojelupoliisille reagointivasteen osalta merkittävästi muita tiukemman velvoitteen ilmoittaa lainkohdassa tarkoitetusta rikoksesta. Käytännössä ilmoitusta tulisi tehdä niin pian kuin inhimillinen toiminta ja ilmoituksen tekemisen tapa sen mahdollistaisivat.

Momentin 2 virkkeen perusteella suojelupoliisi saisi luovuttaa tietoa toimivaltaisille viranomaisille tiedustelumenetelmän käytön yhteydessä ilmenevistä hankkeilla ja vielä estettävissä olevista rikoksista edellyttäen, että teosta seuraava rangaistusuhka on vähintään kaksi vuotta vankeutta. Tämän rangaistusuhkan alittavia tekoja koskisi sitä vastoin tiedonluovutuskielto. Toimivaltaiselle viranomaiselle luovutettava tieto voisi liittyä paitsi rikoksen estämiseen, myös sen paljastamiseen tai esimerkiksi esitutkinnan aloittamiskynnyksen selvittämiseen. Tiedonluovutuksen harkintaa ohjaavista kriteereistä säädettäisiin 3 momentissa. Ilmoituksen yhteydessä luovutettavien rikosta koskevien tarpeellisten tietojen osalta viitataan edellä 1 momentin yhteydessä mainittuun. Tässä yhteydessä tulisi huomioida erityisesti henkeen ja terveyteen kohdistuvien rikosten uhka. Lisäksi eräiden rikosten hengelle ja terveydelle muodostama uhkapotentiaali saattaisi puoltaa ilmoituksen tekemistä. Esimerkiksi yleisötapahtumaan tai yleiseen paikkaan kytkeytyvä väkivallan uhka, olisi painava peruste ilmoituksen tekemiselle. Kyse voisi olla tilanteesta, jossa henkilön käyttäytymisestä tehtyjen havaintojen perusteella muodostuisi perusteltu oletus oikeudettomasta hyökkäyksestä, joka kohdistuisi muihin paikalla oleviin ihmisiin.

Selvää on, että suojelupoliisi saisi 1 ja 2 momentissa tarkoitetusta ilmoituksesta huolimatta jatkaa käynnissä olevaa tiedonhankintaa tämän luvun perusteella, jos tiedustelumenetelmän käytön edellytykset olisivat edelleen olemassa. Tiedonhankinnan jatkamisesta 5 luvun 3 §:ssä mainitun rikoksen taikka valtiopetoksen, törkeän valtiopetoksen tai laittoman sotilaallisen toiminnan eli suojelupoliisin torjuntavastuulla olevien rikosten estämiseksi säädettäisiin 5 §:ssä.

Pykälän 3 momentin mukaan, kun harkittaisiin 1 momentissa tarkoitettua ilmoituksen siirtämistä tai 1 ja 2 momentissa tarkoitettua ilmoituksen tekemistä tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta tai sellaisen rikoksen estämisestä, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta, arvioinnissa olisi otettava huomioon rikoksen selvittämisen tai rikoksen estämisen merkitys yleisen ja yksityisen edun kannalta. Momenttiin koottaisiin ne kriteerit, joiden kautta ilmoituksen lykkäämistä ja harkinnanvaraisen ilmoituksen tekemistä jo tehdystä tai vielä estettävissä olevasta rikoksesta olisi arvioitava. Suojelupoliisin harkinta näissä toimissa ei siis olisi vapaata, vaan myös 3 momentissa tarkoitettuihin arviointikriteereihin sidottua. Tiedustelumenetelmien käyttötarkoituksesta johtuen olisi selvää, että harkinnanvaraisissa rikostiedon luovuttamistapauksissa keskeinen arviointikriteeri on luovuttamisen vaikutus kansalliseen turvallisuuteen. Ilmoituksen lykkäämistilanteessa suojelupoliisin olisi kuitenkin suhteutettava toisiinsa yhtäältä kansallisen turvallisuuden taikka hengen tai terveyden suojaamisintressi ja toisaalta rikoksen selvittämisintressi.

Pykälän 1 momentin mukaan suojelupoliisin päällikkö voisi siirtää ilmoitusta enintään vuodeksi kerrallaan. Jotta suojelupoliisin päällikkö pystyisi tosiasiallisesti arvioimaan rikoksen selvittämisen tai rikoksen estämisen merkitystä yleisen ja yksityisen edun kannalta, niin tämä saattaisi yksittäistapauksellisesti edellyttää keskusrikospoliisille tai paikallispoliisille suoritettavaa tiedustelua ennen päätöksen tekemistä. Tällä turvattaisiin mainittujen intressien kohdalla se, että ne tulisivat suojelupoliisin päällikön päätösharkinnassa mahdollisimman täysimääräisesti turvattua.

Silloin, kun kyse olisi harkinnanvaraisen ilmoituksen tekemisestä jo tehdystä tai vielä estettävissä olevasta rikoksesta, arvioinnissa tulisi keskittyä siihen, miten tehtävä ilmoitus vaikuttaisi rikoksen selvittämiseen tai estämiseen yleisen ja yksityisen edun kannalta. Arvioinnin lähtökohtana olisi yleinen ja yksityinen etu. Rikoksen estämis- ja selvittämisintressin painoarvo on yleisen edun kannalta sitä suurempi, mitä vakavammasta rikosepäilystä on kyse. Yleisen edun kannalta olisi otettava huomioon myös se, onko lykkääminen tai harkinnanvaraisen ilmoituk-

sen tekeminen jo tehdystä rikoksesta ylipäätään mahdollista ilman suurta todennäköisyyttä rikoksen selvittämättä jäämisestä. Rikoksen selvittäminen ei vaarantuisi ainakaan silloin, jos tieto itsessään muodostaisi olennaisen näytön tekijän syyllistymisestä rikokseen. Toisaalta olisi myös arvioitava aiheuttaako ilmoituksen tekeminen mahdollisesti haittaa yleiselle edulle ja ilmoittamisen haitat olisivat suuremmat kuin sillä saavutettavat hyödyt. Yksityisen edun kannalta merkittävää puolestaan olisi esimerkiksi se, jos ilmoittamisen arvioitaisiin mahdollistavan asianomistajan rikoksella saadun omaisuuden palauttaminen tai rikoksen johdosta tuomittavan menettämisseuraamuksen tai asianomistajalle tulevan vahingonkorvauksen täytäntöönpaneminen. Toisaalta yksityinen etu tarkoittaisi myös sen arvioimista aiheuttaako ilmoituksen tekeminen jollekin hengen ja terveyden vaaran, joka ei lähtökohtaisesti puoltaisi ilmoituksen tekemistä.

Pykälän 4 momentin mukaan 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. Esitutkinnan tasapuolisuusperiaatteen sekä jokaiselle kuuluvan oikeuden oikeudenmukaiseen oikeudenkäyntiin ja henkilökohtaiseen vapauteen kannalta on selvää, että pyyntöön saada syyttömyyttä tukevaa selvitystä on suhtauduttava esitutkinnassa sitä vakavammin, mitä suurempi on vaara, että henkilö pidätetään, vangitaan tai hän joutuu muun pakkokeinon kohteeksi tai joutuu syytteeseen tai tuomitaan rangaistukseen tai muuhun rikosoikeudelliseen seuraamukseen virheellisin perustein. Samoihin seikkoihin on viran puolesta kiinnitettävä huomiota myös silloin, kun suojelupoliisi harkitsee oma-aloitteista tiedonluovuttamista syyttömän tueksi. Suojelupoliisin oma-aloitteinen tiedonluovutus syyttömän tueksi voisi tulla kyseeseen lähinnä 5 momentin mukaisissa tilanteissa eli silloin, kun esitutkintaviranomainen on ilmoittanut suojelupoliisille sen tiedonhankinnan kohteena ollutta tai edelleen olevaa henkilöä koskevan esitutkinnan käynnistämisestä, esitutkintatoimenpiteen käyttämisestä taikka rikoksen estämiseen tähtäävän toimenpiteen käynnistämistä. Epäillyn pyyntö puolestaan voisi käytännössä tulla kyseeseen vain silloin, kun hän on saanut ilmoituksen tiedustelumenetelmän käytöstä.

Momentissa tarkoitetun vaaran tai vahingon ei välttämättä tulisi liittyä rikokseen, vaan kysymys saattaisi olla esimerkiksi onnettomuuden estämisestä. Mitä merkittävämmästä vaarasta hengelle, terveydelle tai vapaudelle olisi kyse, sitä korkeampi olisi kynnys olla tekemättä ilmoitus esimerkiksi toimivaltaiselle viranomaiselle. Ilmoitus voitaisiin tehdä myös yksityiselle henkilölle tai yhteisölle, jos tämä olisi tarpeen merkittävän ympäristö-, omaisuus- tai varallisuusvahingon vaaran estämiseksi.

Pykälän 5 momentin mukaan jos esitutkintaviranomainen käynnistää esitutkinnan tai ryhtyy esitutkintatoimenpiteen käyttämiseen taikka toimivaltainen viranomainen käynnistää rikoksen estämiseen tähtäävän toimenpiteen tässä pykälässä tarkoitetun ilmoituksen perusteella, esitutkintaviranomaisen tai toimivaltaisen viranomaisen on ennen esitutkinnan käynnistämistä tai esitutkintatoimenpiteen käyttämistä taikka rikoksen estämiseen tähtäävän toimenpiteen käynnistämistä ilmoitettava siitä suojelupoliisille. Momentin tarkoituksena on ylläpitää suojelupoliisin tilannekuvaa siitä, minkälaisiin toimiin esitutkintaviranomaiset tai muut toimivaltaiset viranomaiset ovat suojelupoliisin niille luovuttamien tietojen perusteella ryhtyneet sekä varmistaa tiedustelumenetelmän käytöstä ilmoittaminen 46 §:n 5 momentin tarkoittamissa tilanteissa. Viimeksi mainitun lainkohdan mukaan suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä ja paikkatiedustelusta on ilmoitettava tiedonhankinnan kohteelle, jos asiassa aloitetaan esitutkinta. Esitutkinnan käynnistämisestä säädetään esitutkintalain (805/2011) 3 luvun 3 §:ssä. Esitutkintatoimenpiteellä tarkoitetaan muun muassa kuulusteluja ja ryhmätunnistusta. Rikoksen estämiseen tähtääviä toimenpiteitä ovat muun muassa henkilön kiinniottaminen, sisäänpääsy kotirauhan tai julkisrauhan suojaamaan tilaan taikka paikan ja alueen eristäminen.

45 §. *Tiedustelutietojen hävittäminen.* Pykälän 1 momentin mukaan tiedustelumenetelmällä saatu tieto olisi hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi.

Momentti koskisi kaikkea tiedustelumenetelmällä saatua tietoa. Varsin pian tulisi käydä selväksi jo tiedustelumenetelmällä saadun tiedon sisällöstä johtuen tarvitaanko sitä kansallisen turvallisuuden suojaamiseksi vai voidaanko se hävittää.

Pykälän 2 momentin mukaan tieto voitaisiin kuitenkin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin, jos tämä on tarpeen 44 §:ssä tarkoitetuissa tapauksissa.

Tiedustelumenetelmällä saatu tieto, joka ei liity kansallisen turvallisuuden suojaamiseen, tulee lähtökohtaisesti hävittää. Tällöin saatetaan hävittää samalla 44 §:ssä tarkoitettua esimerkiksi törkeän rikoksen selvittämiseksi ja estämiseksi tarpeellista tai epäillyn syyttömyyttä tukevaa aineistoa. Sen vuoksi on tarpeen sallia poikkeaminen hävittämisvelvollisuudesta, jotta törkeiden rikosten selvittämiseksi ja estämiseksi tarpeellinen sekä syyttömyyttä tukeva aineisto olisi tarvittaessa käytettävissä.

Pykälän 3 momentin mukaan edellä 7 §:ssä tarkoitetut tukiasematiedot olisi hävitettävä, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi. Sääntely vastaisi 5 luvun 55 §:n 3 momentin sääntelyä sillä erotuksella, että tässä momentissa tiedon tarve liittyisi kansallisen turvallisuuden suojaamiseen.

Tietojen poistamisesta säädetään myös henkilötietojen käsittelystä poliisitoimessa annetussa laissa (761/2003).

46 §. *Kiiretilanteessa saadun tiedon hävittäminen.* Pykälän mukaan jos suojelupoliisin päällystöön kuuluva poliisimies olisi 7 §:n 1 momentissa, 8 §:n 1 momentissa, 11 §:n 1 momentissa, 12 §:n 1 momentissa, 13 §:n 1 momentissa, 14 §:n 1 momentissa tai 27 §:n 2 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, teknisen kuuntelun, teknisen katselun, henkilön teknisen seurannan, teknisen laitetarkkailun tai paikkatiedustelun 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. Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saataisiin käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

Kiirepäätöksen jälkeen tuomioistuimen antama kielteinen päätös tulee ilmoittaa tiedusteluvaltuutetulle kiirepäätösmenettelyn lainmukaisuuden tutkimiseksi. Kiirepäätöksellä saadun tiedon kohdalla on lähtökohtaisesti kyse laillisesti saadusta tiedosta. Mikäli tuomioistuin jälkikäteen katsoisi, ettei kiirepäätökselle ole ollut perusteita, niin mahdollisen menettelyvirheen vakavuudesta riippuen tämä saattaisi johtaa tilanteeseen, jossa tiedustelumenetelmällä saatua tietoa ei voitaisi hyödyntää syyllisyyttä tukevana selvityksen tai syyllisyyttä osoittavana näyttönä. Tuomioistuin voisi kielteisen päätöksen antaessaan lausua myös kiirepäätösmenettelyllä saatujen tietojen hyödynnettävyydestä rikoksen selvittämiseksi hankkimistapaan liittyvä oikeudenloukkauksen vakavuus huomioon ottaen. Yleisenä lähtökohtana punninnassa voidaan pitää yhtäältä asian selvittämisintressiä (rikoksen vakavuus) hyödyntämistä puoltavana näkökohtana ja toisaalta hyödyntämiskieltoa puoltavana näkökohtana ne epäedulliset vaikutukset, mitä hyödyntämisestä seuraisi. Hyödyntäminen saattaisi yhtäältä loukata epäillyn oikeusturvaa ja toi-

saalta auttaa aineellisen totuuden löytämisessä sekä palvella asianomistajan oikeuksien toteutumista. Yleisenä lähtökohtana voidaan pitää myös sitä, että kiirepäätöksellä saatua tietoa voitaisiin hyödyntää syytetyn syyttömyyden tukemiseksi.

Pykälän 2 momentissa säädettäisiin kiiretilanteessa jäljentämisellä saadun tiedon hävittämisestä. Kyse olisi analogisesti vastaavanlaisesta tilanteesta kuin 1 momentissa. Jos suojelupoliisin poliisimies tekisi kiirepäätöksen jäljentämisestä, mutta tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies katsoisi, että edellytyksiä toimenpiteelle ei ole ollut, niin jäljentämisellä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saataisiin kuitenkin käyttää samoin edellytyksin kuin tietoa saataisiin käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että hankkeilla on sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

47 §. *Tiedustelumenetelmän käytöstä ilmoittaminen.* Pykälän 1 momentin 1 virkkeen mukaan telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä tai viestiin kohdistuvasta lähetyksen jäljentämisestä olisi viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu. Kohteelle ilmoittamisesta olisi samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Momentissa lueteltaisiin ne tiedustelumenetelmät, joista ilmoitus tiedonhankinnan kohteelle on tehtävä. Kyse olisi sellaisista tiedustelumenetelmistä, joilla puututtaisiin tiedonhankinnan kohteena olevan henkilön luottamuksellisen viestin suojaan. Säännöksessä kytkettäisiin velvollisuus ilmoittaa tiedustelumenetelmän käytöstä tiedustelun kohteelle siihen ajankohtaan, kun tällainen tiedonhankinta on lopetettu. Tiedonhankinta on voitu lopettaa joko siksi, että sen tarkoitus kansallista turvallisuutta vakavasti uhkaavan siviilitiedustelun kohteena olevan toiminnan paljastamiseksi on saavutettu tai siksi, koska tiedonhankinta on osoittautunut tuloksettomaksi.

Ilmoituksen tulisi olla sillä tavoin yksilöity, että kohde voisi tarvittaessa pyrkiä selvittämään häneen kohdistetun tiedustelumenetelmän 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 viranomaisen tarvitsisi paljastaa. Ilmoitus voitaisiin tehdä kohteelle esimerkiksi kirjeitse viimeiseen tiedossa olevaan osoitteeseen. Muulle henkilölle kuin tiedonhankinnan kohteelle ei tarvitsisi ilmoittaa tiedustelumenetelmän käytöstä, vaikka hän olisi tosiasiallisesti joutunut toimenpiteen kohteeksi. Ilmoitusvelvollisuuden piiriin kuuluisivat näin ollen vain varsinaiset tiedonhankinnan kohteena olevat henkilöt eli ne henkilöt, joiden osalta vaatimus tai päätös tiedustelumenetelmän käyttämisestä olisi tehty.

Silloin, kun tiedustelumenetelmän käyttö on tosiasiallisesti lopetettu ennen luvan tai päätöksen voimassaolon päättymistä, eikä uutta lupaa ole haettu tai jatkopäätöstä tehty, tulisi ilmoitus kohteelle tehdä tosiasiallisesta lopettamishetkestä. Jos tiedonhankintaa jatkettaisiin jatkoluvan tai -päätöksen nojalla, tulisi ilmoitus tehdä joko tiedustelumenetelmän käytön tosiasiallisesta lopettamisesta taikka luvan tai päätöksen voimassaoloajan päättymisestä. Päätösten voimassaolon välillä voidaan hyväksyä muutaman päivän katkoksia, jotta tiedonhankintaa voidaan pitää yhdenjaksoisena.

Pykälän 1 momentin 2 virkkeen mukaan tiedustelumenetelmän käytöstä olisi kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta. Jos menetelmän käyttö on tosiasiallisesti lopetettu ennen luvan tai päätöksen voimassaolon päättymistä, eikä uutta lupaa ole haettu, laskettaisiin vuoden määräaika tosiasiallisesta lopettamishetkestä. Mikäli tiedonhankinta on päättynyt luvan tai päätöksen voimassaoloajan päättymiseen, laskettaisiin vuoden määräaika tästä päättymisestä. Takautuvasti käytettävissä tiedustelumenetelmissä määräaika laskettaisiin luvan tai päätöksen tekohetkestä, vaikka tietoja ei olisi vielä saatu.

Jos samaa tiedonhankinnan kohteena olevaa henkilöä koskien on tehty uusi päätös saman tiedustelumenetelmän käytöstä, laskettaisiin vuoden määräaika viimeisen samaa asiaa koskevan tiedonhankinnan tosiasiallisesta lopettamisesta taikka luvan tai päätöksen voimassaoloajan päättymisestä. Päätösten voimassaolon välillä voidaan hyväksyä muutaman päivän katkoksia, jotta tiedonhankintaa voidaan pitää yhdenjaksoisena.

Pykälän 2 momentin mukaan tuomioistuin voisi suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Ilmoituksen lykkäämisestä tai kokonaan tekemättä jättämisestä päättäisi tuomioistuin, vaikka kysymys olisi sellaisesta tiedustelumenetelmästä, josta on päättänyt suojelupoliisin päällystöön kuuluva poliisimies. Ehdotuksen mukaisesti ilmoitusta voitaisiin lykätä enintään kahdeksi vuodeksi kerrallaan. Uuden lykkäyksen myöntämisen 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. Lykkäämistä ja uudelleen lykkäämistä tulisi hakea ennen määräajan päättymistä.

Lykkäämisen mahdollistavana perusteena olisi ensinnäkin käynnissä olevan tiedustelumenetelmän käytön turvaaminen. Tiedonhankinta voisi liittyä mihin tahansa vireillä olevaan tiedusteluoperaatioon myös sotilastiedusteluoperaatioon. Lykkääminen olisi mahdollista myös kansallisen turvallisuuden varmistamiseksi. Kansallisen turvallisuuden varmistamisen käsitettä käsitellään 44 §:n perusteluissa. Lisäksi ilmoittamisen lykkääminen olisi mahdollista hengen tai terveyden suojaamiseksi. Lykkäämisen edellytyksenä olisi, että se on perusteltua. Kynnys lykkäämiselle ei siis olisi kovin korkea.

Ilmoitus saataisiin jättää tuomioistuimen päätöksellä kokonaan tekemättä vain silloin, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Kynnys kokonaan ilmoittamatta jättämiselle olisi puolestaan korkea, mitä kuvattaisiin ilmauksella "välttämätöntä".

Mikäli tuomioistuin ei myöntäisi lykkäystä tai ei hyväksyisi ilmoituksen kokonaan tekemättä jättämistä, vaatimuksen esittäjä saisi kannella päätöksestä Helsingin hovioikeudelle siten kuin 35 §:ssä säädetään.

Pykälän 3 momentin mukaan jos tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä olisi ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Tuntemattomaksi jääneelle tiedonhankinnan kohteelle ilmoitusta ei voitaisi luonnollisestikaan tehdä. Mikäli tiedonhankinnan kohteen henkilöllisyys myöhemmin selviäisi, tulisi ilmoitus kuitenkin tehdä. Tällaiset tilanteet saattaisivat myös muodostaa poikkeuksen pykälässä säädetyistä määräajoista, koska niitä ei joissakin tapauksissa kyetä noudattamaan. Jos henkilöllisyydeltään tunnettu tiedonhankinnan kohde olisi kateissa, suojelupoliisilta ei edellytettäisi kovin laajoja toimenpiteitä pelkästään ilmoituksen tekemiseksi. Riittävää olisi, että asiasta laaditaan etsintäkuulutus (esimerkiksi olinpaikkailmoitus) ilmoituksen antamista varten.

Pykälän 4 momentin mukaan kohteelle ilmoittamisesta olisi samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle. Kun tiedustelumenetelmän käyttö on perustunut tuomioistuimen lupaan, kohteelle ilmoittamisesta olisi samalla annettava tieto myös tuomioistuimelle. Lupaa edellyttävän tiedustelumenetelmän kohteelle ilmoittaminen olisi siten saatettava myös Helsingin käräjäoikeuden tietoon.

Pykälän 5 momentin mukaan jos suojelupoliisi jatkaisi tiedonhankintaa 5 §:n perusteella, noudatetaan mitä salaisen tiedonhankintakeinon käytöstä ilmoittamisesta 5 luvun 58 §:ssä säädetään. Tilanteessa, jossa tiedustelumenetelmän käyttönä alkanut tiedonhankinta jatkuisi salaisen tiedonhankintakeinon käyttönä, tehtäisiin ilmoitukset tiedonhankinnan kohteelle ja tuomioistuimelle samoin kuin päätökset ilmoituksen lykkäämisestä tai ilmoituksen kokonaan tekemättä jättämisestä poliisilain 5 luvun 58 §:n perusteella. Momentin tarkoittamissa tilanteissa tulisi ilmoittaa paitsi poliisilain 5 luvussa tarkoitetun keinon käytöstä, myös tiedustelumenetelmän käytöstä. Tiedustelumenetelmän käytöstä ilmoittamista arvioitaisiin tässä yhteydessä viimeksi mainitun pykälän nojalla.

Pykälän 6 momentin mukaan suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei olisi velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa. Ilmoitus paikkatiedustelusta tehtäisiin sille, joka on ollut kyseisen tiedustelumenetelmän käytön kohteena sekä tarvittaessa myös paikan omistajalle tai haltijalle. Säännöksessä tarkoitetusta jäljentämisestä ja lähetyksen jäljentämisestä ilmoitus tehtäisiin tiedonhankinnan kohteelle. Jos esitutkinta aloitettaisiin, noudatetaan, mitä pakkokeinolain 10 luvun 60 §:n 2–7 momentissa säädetään. Momentissa mainittujen tiedustelumenetelmien käytöstä ei sitä vastoin tarvitsisi lainkaan ilmoittaa, jos niiden kohteena olevassa asiassa ei aloitettaisi esitutkintaa.

Pykälän 7 momentissa säädettäisiin valtiolliselle toimijalle tehtävästä ilmoituksesta. Säännöksen mukaan tiedustelumenetelmän käytöstä ei olisi velvollisuutta ilmoittaa silloin, kun tiedonhankinnan kohteena on ollut 4 §:n 3 momentissa mainittu valtiollinen toimija. Vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa ja ilmoituksen tekeminen tulisi kyseeseen erittäin poikkeuksellisessa tapauksessa, jos tiedonhankinnan kohteena on ollut vieraan valtion viranomainen eli valtiollinen toimija. Säännöksen soveltamisalaan kuuluisivat myös valtiollisen toimijan välilliset toimijat.

Tiedustelumenetelmän käytöstä ei olisi ilmoitusvelvollisuutta ulkomaan tiedustelussa (39 §:n 3 momentti). Tämän lisäksi olisi tarpeen huomioida myös tilanteet, joissa tiedustelumenetelmää käytetään Suomen alueella valtiolliseen toimijaan. Sekä ulkomaan tiedustelussa että Suomen alueella tapahtuvassa valtiolliseen toimijaan kohdistuvassa tiedustelumenetelmän käytössä toimintaan liittyy lähes poikkeuksetta ulkopoliittisia ja mahdollisesti muita sensitiivisyyksiä, jolloin kohteena olleelle henkilölle ilmoittaminen ei ole perusteltua. Säännös ei kuitenkaan estäisi ilmoituksen tekemistä mitä kuvaa ilmaisu "ei ole velvollisuutta ilmoittaa".

Pykälän 8 momentin mukaan ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan mitä 34 §:ssä säädetään. Viittaus merkitsee käytännössä sitä, että myös ilmoitusasiat käsitellään Helsingin käräjäoikeudessa. Kuten tiedustelumenetelmää koskevan lupa-asian yhteydessä, myös ilmoitusasian käsittelyssä tulisi kiinnittää erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

48 §. *Pöytäkirja.* Pykälän mukaan tiedustelumenetelmän käytön lopettamisen jälkeen olisi laadittava ilman aiheetonta viivytystä pöytäkirja. Tiedustelumenetelmien käytön dokumentointi on välttämätöntä toiminnan oikeudellisen valvonnan mahdollistamiseksi. Toimenpiteiden kirjaamisesta valvontaa varten voitaisiin 62 §:n 1 momentin mukaan säätää tarkemmin valtioneuvoston asetuksella.

Nykyisin poliisilain 5 luvussa käytettävien salaisten tiedonhankintakeinojen pöytäkirjaamisesta säädetään esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta annetussa valtioneuvoston asetuksessa (122/2014). Asetuksen 3 luvun 1 §:n 1 momentin mukaan pakkokeinolain 10 luvun 1 §:ssä tarkoitetun salaisen pakkokeinon tai poliisilain (872/2011) 5 luvun 1 §:ssä tarkoitetun salaisen tiedonhankintakeinon käyttöä esittäneen tai siitä päättäneen taikka hänen määräämänsä esitutkintavirkamiehen on laadittava niiden käytön lopettamisen jälkeen ilman aiheetonta viivytystä, kuitenkin viimeistään 90 päivän kuluessa, pöytäkirja. Pykälän 2 momentin mukaan poliisilain 5 luvun 17 §:n 5 momentissa, 19 §:n 5 momentissa ja 21 §:n 4 momentissa tarkoitettu tekninen tarkkailu on kirjattava.

Myös tiedustelumenetelmien käytön jälkeen pöytäkirjaan kirjattavien toimenpiteiden kirjaamisesta on perusteltua säännellä valtioneuvoston asetuksella vastaavalla tavalla kuin esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta annetussa valtioneuvoston asetuksessa.

49 §. *Asianosaisjulkisuuden rajoittaminen eräissä tapauksissa.* Pykälän 1 momentin mukaan henkilöllä, jonka oikeutta tai velvollisuutta asia koskee, ei olisi viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 11 §:ssä säädetystä huolimatta oikeutta saada tietoa tässä luvussa tarkoitetun tiedustelumenetelmän käytöstä, ennen kuin 47 §:ssä tarkoitettu ilmoitus on tehty. Viimeksi mainitussa 47 §:ssä säädetään tiedustelumenetelmän käytöstä ilmoittamisesta. Asianosaisjulkisuuden rajoittaminen ennen tiedustelumenetelmän käytöstä tehtävää ilmoitusta on tärkeää siksi, että tiedustelumenetelmän käytön yhteydessä tuotetaan asiakirjoja, jotka koskevat valtion turvallisuutta eli seikkoja, joista tiedon antaminen olisi vastoin erittäin tärkeää yleistä etua.

Tiedustelutoiminnan valvonnassa annettavassa laissa säädettäisiin mahdollisuudesta tehdä tiedusteluvaltuutetulle kantelu (11 §). Kantelun voisi tehdä jokainen, joka katsoo, että tiedustelutoiminnassa on rikottu hänen oikeuksiaan tai menetelty muutoin lainvastaisesti. Tiedustelutoiminnan kohteena ollut tai henkilö, joka epäilisi, että häneen on kohdistettu tiedustelua, voisi pyytää tiedusteluvaltuutettua tutkimaan häneen kohdistuneen tiedustelumenetelmän käytön lainmukaisuuden (12 §).

Pykälän 2 momentin mukaan rekisteröidyn tarkastusoikeudesta säädetään poliisitoimessa annetussa laissa. Kyse olisi informatiivisesta viittauksesta säännöksessä tarkoitettuun lakiin, jonka 45 §:n 1 momentin 2 kohdan mukaan tarkastusoikeutta ei ole lainkaan suojelupoliisin toiminnallisen tietojärjestelmän tietoihin. Pykälän 2 momentissa säädetään tietosuojavaltuutetun tarkastusoikeudesta, jonka mukaan tietosuojavaltuutettu voi rekisteröidyn pyynnöstä tarkastaa suojelupoliisin tietojärjestelmässä olevien, rekisteröityä koskevien tietojen lainmukaisuuden.

50 §. *Tietojen saanti yksityiseltä yhteisöltä.* Pykälän mukaan suojelupoliisilla olisi suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä sellaisia tietoja, joiden yksittäistapauksessa voidaan olettaa olevan tarpeen sellaisen siviilitiedustelun kohteena olevan toiminnan selvittämisessä, joka vakavasti uhkaa kansallista turvallisuutta, ja jolla voidaan olettaa olevan merkitystä: 1) siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi, tavoittamiseksi tai yhteystietojen selvittämiseksi taikka tällaisen henkilön liikkumisen selvittämiseksi; 2) tiedustelumenetelmän käytön kohdentamiseksi siviilitiedustelun kohteena olevaan henkilöön; tai 3) siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön 3 §:ssä tarkoitettuun toimintaan oletettavasti kytkeytyvän taloudellisen toiminnan selvittämiseksi.

Pykälä vastaisi tarkoitukseltaan poliisilain 4 luvun 3 §:n 1 momentin sääntelyä. Tässä yhteydessä tietopyynnön tarkoituksena ei kuitenkaan olisi rikoksen estäminen tai selvittäminen, vaan tietopyyntö olisi sidottu 3 §:ssä tarkoitettuihin siviilitiedustelun kohteisiin, mikä ilmenee pykälän muotoilusta "siviilitiedustelun kohteena olevan toiminnan selvittämisessä".

Toiminnan selvittämistä koskevalla ilmaisulla ei tarkoitettaisi (rikoksen) selvittämistä esitutkintalain mukaisessa merkityksessä, vaan kyse olisi yksilöidyn kansallista turvallisuutta vakavasti uhkaavan toiminnan selvittämisestä. Selvittämisellä tarkoitettaisiin siten tietojen kokoamista keräämällä tietoa eri lähteistä ja pykälässä tarkoitettu tietopyyntö olisi yksi keino kerätä siviilitiedustelun kohteista merkityksellistä tietoa.

Pykälän todennäköisyyttä osoittavat ilmaisut "voidaan olettaa olevan tarpeen" ja "voidaan olettaa olevan merkitystä" olisivat niin sanottuja tuloksellisuusodotukseen rinnastettavia edellytyksiä. Näin ollen tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen tulisi ottaa tietopyyntöä koskeva kynnys huomioon sitä tehdessään. Vaikka tietopyynnön esittäjällä ei olisi tiedon luovuttajaa kohtaan perusteluvelvollisuutta, hänen tulisi perustaa tietopyyntöänsä koskeva harkintansa objektiivisiin seikkoihin ja kirjata se, 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 suojelupoliisille 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 suojelupoliisille.

Yrityksillä on runsaasti yrityssalaisuuden piiriin kuuluvia omalle elinkeinotoiminnalleen merkityksellisiä tietoja kuten tuotekehitystietoja. Pykälän perusteella yrityksellä ei olisi velvollisuutta luovuttaa suojelupoliisille tällaisia omalle yritystoiminnalleen tai sopimuskumppanilleen merkityksellisiä yrityssalaisuuden ytimeen kuuluvia tietoja, vaan tietopyynnössä olisi lähtökohtaisesti kyse asiakas-, työntekijä- tai muussa taloudellisessa suhteessa olevien tahoja yksilöivistä tiedoista.

Tietopyynnön yksittäistapauksellisuutta olisi arvioitava tiedonhankinnan kohteena olevan siviilitiedustelun kohteen kannalta. Näin ollen yksittäistapauksellisuus ei rajoittaisi tietopyyntöjen määrää saman kansallista turvallisuutta vakavasti uhkaavan toiminnan kohdalla. Yksittäistapauksellisuus voisi tarkoittaa tarvittaessa useampia tietopyyntöjä kyseistä uhkaa koskien, kunnes uhka olisi poistunut.

Pyynnön kohteena olevilla tiedoilla tulisi 1 kohdan mukaan perustellusti voida olettaa merkitystä siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi. Tällä tarkoitettaisiin sitä, että siviilitiedustelun kohteena oleva henkilö voitaisiin oletettavasti tunnistaa, tavoittaa 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 kertakäyttöliittymän ostoa ja sen ostajaa koskevan pyynnön osoittamista vähittäismyyntiliikkeelle. Pykälän 3 kohta kattaisi muun muassa pankkitiedustelut sekä muut luottolaitoksille tai rahavälitystoimijoille tehtävät tietopyynnöt, jotka mahdollistavat siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön 3 §:ssä tarkoitettuun toimintaan oletettavasti kytkeytyvän taloudellisen toiminnan, kuten henkilön tai oikeushenkilön saamien pankkisiirtojen lähteiden tunnistamisen tai tällaisessa oikeushenkilössä määräysvaltaa käyttävien tahojen, selvittämisen.

51 §. *Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin.* Pykälän mukaan teleyrityksen avustamisvelvollisuuteen sovellettaisiin mitä 5 luvun 61 §:ssä säädetään teleyrityksen avustamisvelvollisuudesta ja pääsystä eräisiin tiloihin.

52 §. *Korvaus teleyritykselle.* Pykälän mukaan teleyrityksen oikeudesta korvaukseen sovellettaisiin mitä 5 luvun 62 §:ssä säädetään korvauksesta teleyritykselle. Mainitun pykälän 1 momentin mukaan teleyrityksellä on oikeus saada valtion varoista korvaus tässä luvussa tarkoitetusta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista siten kuin sähköisen viestinnän palveluista annetun lain (917/2014) 299 §:ssä säädetään. Korvauksen maksamisesta päättää toimenpiteen suorittaneen poliisiviranomaisen yksikkö.

Sähköisen viestinnän palveluista annetun lain 299 §:n 1 momentin mukaan teleyrityksellä on oikeus saada valtion varoista korvaus yksinomaan viranomaisen avustamiseksi hankittujen järjestelmien, laitteistojen ja ohjelmistojen investoinneista ja ylläpidosta aiheutuneista välittömistä kustannuksista. Kustannusten korvaamisesta päättää tarvittaessa Viestintävirasto.

Mainitun pykälän perustelujen (HE 221/2013 vp) mukaan teleyritys saa korvauksen järjestelmien, laitteistojen ja ohjelmistojen ylläpidosta, kuten ohjelmistojen päivityksistä ja huollosta aiheutuvista kuluista. Sen sijaan järjestelmien, laitteistojen ja ohjelmistojen käytöstä aiheutuvia henkilöstökuluja ei korvata. Kyseisen muutoksen tavoitteena on ollut yhdenmukaistaa kustannusten korvaamista koskevaa sääntelyä. Kustannusten korvaamista koskevasta sääntelyratkaisusta ei ole ilmennyt tarvetta poiketa siviilitiedustelulainsäädännön valmistelun yhteydessä.

Sähköisen viestinnän palveluista annetun lain 299 §:n 2 momentissa säädetään oikeudesta vaatia oikaisua poliisiviranomaisen tekemään päätökseen. Pykälän 3 momentin mukaan hallinto-oikeuden on varattava Viestintävirastolle tilaisuus tulla kuulluksi.

53 §. *Teleyrityksen säilyttämien tietojen käyttäminen.* Pykälän mukaan sen lisäksi mitä sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentissa säädetään säilytettävien tietojen käyttämisestä, säilytettäviä tietoja saataisiin käyttää myös, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentissa säädetään, että pykälän 2 ja 3 momentissa tarkoitettuja tietoja saa käyttää ainoastaan pakkokeinolain 10 luvun 6 §:n 2 momentissa tarkoitettujen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi. Viimeksi mainitussa lainkohdassa säädetään televalvontaan oikeuttavien rikosten luettelosta. Kyseinen luettelo käsittää seuraavat rikokset: 1) rikos, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta; 2) teleosoitetta tai telepäätelaitetta käyttäen tehty rikos, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta; 3) teleosoitetta tai telepäätelaitetta käyttäen tehty, automaattiseen tietojenkäsittelyjärjestelmään kohdistunut luvaton käyttö; 4) seksikaupan kohteena olevan henkilön hyväksikäyttö, lapsen houkutteleminen seksuaalisiin tarkoituksiin ja parituksen; 5) huumausainerikos; 6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelu, kouluttautuminen terrorismirikoksen tekemistä varten, terroristiryhmän rahoittaminen tai matkustaminen terrorismirikoksen tekemistä varten; 7) törkeä tulliselvitysrikos; 8) törkeä laittoman saaliin kätkeminen; 9) panttivangin ottamisen valmistelu; taikka 10) törkeän ryöstön valmistelu.

Ehdotettavan pykälän mukaan vastaavia tietoja voitaisiin käyttää myös tiedon saamiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, joka on siviilitiedustelun kohteena (3 §). Kyse ei olisi siten uusien tietojen säilyttämisestä, vaan jo olemassa olevien tietojen hyödyntämisestä paitsi rikoksen selvittämiseksi ja syyteharkintaan saattamiseksi, myös kansallisen turvallisuuden suojaamiseksi. Tallennettujen tietojen määrä ei kasvaisi.

54 §. *Yhteistyö sotilastiedusteluviranomaisen kanssa.* Pykälän mukaan suojelupoliisin olisi toimittava yhteistyössä sotilastiedusteluviranomaisen kanssa tiedustelun tarkoituksenmukaiseksi hoitamiseksi sekä annettava sotilastiedusteluviranomaiselle tässä tarkoituksessa tarpeellisia tietoja sen estämättä mitä salassapitovelvollisuudesta säädetään.

Sääntelyn tarkoituksena olisi edistää suojelupoliisin ja sotilastiedusteluviranomaisen yhteistoimintaa siten, että niille säädetyt, samaan päämäärään liittyvät toimialakohtaiset ja rinnakkaiset tehtävät tulevat hoidetuiksi tarkoituksenmukaisesti, taloudellisesti ja joustavasti.

Keskeisiä yhteistyömuotoja olisivat yhteinen tiedustelu ja - analyysitoiminta, keskinäinen tietojen vaihtaminen, yhteisten tiedustelujärjestelmien kehittäminen, yhteisen tilannekuvan muodostaminen turvallisuusuhkista ja toimintaympäristön muutoksista, yhteiset toimintasuunnitelmat, keskinäinen virka-apu, koulutusyhteistyö ja virkamiesvaihto.

Yhteistoimintamuotoja olisivat myös yhteiset edustajat kansainvälisessä yhteistoiminnassa, henkilöstön yhteiskoulutus, tiedustelutoiminnan yhteensovittaminen, tiedonhankinnan kehittäminen, lomakkeiden ja tietojärjestelmien yhteensopivuuden kehittäminen, tilojen, kaluston, laitteiden ja varusteiden hankintojen yhteinen valmistelu sekä toiminnan ja sen tavoitteiden suunnittelun yhteensovittaminen.

Yhteistyövaatimuksen kautta varmistuttaisiin siitä, että siviili- ja sotilastiedusteluviranomaiset 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 tarkoituksenmukaisena sitä, etteivät tiedusteluviranomaiset voisi jakaa kalustoaan ja osaamistaan toiselle tiedusteluviranomaiselle. Tämä liittyisi erityisesti teletiedustelumenetelmien ja tietoliikennetiedustelun käyttämiseen.

55 §. *Yhteistyö muiden viranomaisten ja yhteisöjen kanssa*. Pykälässä säädettäisiin suojelupoliisin ja muiden kuin sotilastiedusteluviranomaisen välisestä yhteistyöstä.

Pykälän mukaan suojelupoliisin olisi tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi. Näin ollen myös muut viranomaiset voisivat tarvittaessa avustaa suojelupoliisia siviilitiedustelussa. Tämä tarkoittaisi yhteistyötä esimerkiksi keskusrikospoliisin, poliisilaitosten, Tullin, Rajavartiolaitoksen, Maahanmuuttoviraston tai Viestintäviraston kanssa.

Viranomaisen välisen yhteistyön toimivuudella on keskeinen merkitys siviilitiedustelun tavoitteiden toteutumisessa. Yhteistyön piiriin kuuluisi tietojärjestelmien kehittäminen, tilannekuvan muodostaminen turvallisuusuhkista ja toimintaympäristön muutoksista, yhteiset toimintasuunnitelmat, keskinäinen virka-apu ja koulutusyhteistyö.

Yhteistyön piiriin voisi kuulua myös viranomaisten välinen taktinen toiminta. Kyse voisi olla esimerkiksi tiedonhankinnan paljastumisen estämiseksi suoritettavista toimista.

Pykälän 2 momentin mukaan suojelupoliisi voisi tehtävänsä toteuttamiseksi toimia yhteistyössä yhteisöjen kanssa sekä luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä sellaisia tietoja, jos tietojen luovuttaminen olisi välttämätöntä kansallisen turvallisuuden suojaamiseksi.

Siviilitiedustelussa voi ilmetä tilanteita, joissa kansallisen turvallisuuden suojaamisen perusteella tietoja täytyy oma-aloitteisesti tai pyynnöstä välittää toiselle viranomaiselle. Sama koskee muutenkin tietojen antamista toisen viranomaisen hoidettaviksi kuuluvien tehtävien suorittamista varten. Kyse olisi muista kuin henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettujen tietojen luovuttamisesta, mistä säädettäisiin asianomaisessa laissa.

Ensinnäkin tietojen luovuttamisen tulisi kuulua suojelupoliisin tehtävään, josta säädetään poliisin hallinnosta annetun lain 10 §:ssä sekä osin tämän lain 1 luvun 1 §:ssä. Näin ollen suojelupoliisi tekisi ensivaiheen harkinnan tiedon luovuttamisesta omaan tehtäväkenttäänsä liittyen. Toiseksi tiedon luovuttamisen tulisi olla välttämätöntä. Tällä korostettaisiin sitä, että ilmaisukynnyksen on oltava korkea. Tietoja ei saa luovuttaa muissa kuin momentin asettamat edellytykset täyttävissä tapauksissa.

Suojelupoliisin ja yhteisöjen välinen yhteistyö voisi liittyä myös yritysten turvallisuuteen ja yritysvakoilun estämiseen.

Pykälän 3 momentin mukaan tietojen luovuttamisesta rikostorjuntaan säädettäisiin 44 §:ssä. Viittaus niin sanottuun palomuurisäännökseen olisi tarpeellinen, koska kansallisen turvallisuuden suojaaminen ei käsitä kuin marginaalisen osan rikoslakirikoksista. Näin ollen 44 §:ssä tarkoitettujen tietojen ilmoittaminen tapahtuisi kyseisen pykälän nojalla.

56 §. *Salaisen tiedonhankinnan yhteensovittaminen.* Pykälässä säädettäisiin suojelupoliisin, sotilastiedusteluviranomaisen, keskusrikospoliisin ja muun viranomaisen välisestä salaisen tiedonhankinnan koordinaatiosta. Kyseessä olisi erityissäännös suhteessa edellä esitettyihin yhteistyösäännöksiin nähden.

Salaista tiedonhankintaa suorittavien viranomaisten päällekkäiset tehtävät ja erityisesti päällekkäiset operaatiot voivat muodostaa vakavan työturvallisuusriskin, jos esimerkiksi eri salaisissa tiedonhankintatehtävissä viranomaiset toimivat toisistaan tietämättä.

Kun on useita viranomaisia, joilla on oikeus käyttää salaista tiedonhankintaa, niin tämä saattaa joissain tapauksissa aiheuttaa riskin sekä turvallisuusviranomaisten yleisten roolien että yksittäisten operaatioiden päällekkäisyydestä. Jotta tämänlaiset tilanteet pystyttäisiin ennalta estä-

mään ja torjumaan mahdolliset työtapaturmat, niin voi tapauskohtaisesti olla välttämätöntä, että kyseiset viranomaiset keskenään koordinoivat salaisen tiedonhankinnan käyttöä.

57 §. *Kansainvälinen yhteistyö.* Pykälässä säädettäisiin suojelupoliisin kansainvälisestä yhteistyöstä. Pykälän 1 momentin mukaan suojelupoliisi voisi tehdä yhteistyötä sekä toteuttaa tiedonhankintaa yhdessä ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa kansallisen turvallisuuden suojaamiseksi. Yhteistyöllä tarkoitettaisiin kaikkea kansainvälistä tiedustelu- ja turvallisuusviranomaisten välistä yhteistyötä suojelupoliisin ja muiden maiden vastaavien virastojen välillä. Yhteistyö voisi toteutua esimerkiksi tietojen vaihtona, teknisen tuen antamisena, koulutusyhteistyönä, virkamiesvaihtona, kansainvälisenä yhdyshenkilötoimintana tai muuna tiedusteluviranomaisten välisenä toimintana. Yhteisillä operaatioilla puolestaan tarkoitettaisiin yhteisiä tiedonhankintaoperaatioita, joissa voitaisiin käyttää tässä luvussa säädettyjä tiedustelumenetelmiä. Yhteisistä operaatioista säädettäisiin tarkemmin pykälän 2 ja 3 momenteissa sekä muiden kuin henkilötietojen vaihdosta 3 momentissa.

Pykälän 2 momentissa säädettäisiin tilanteesta, jossa suojelupoliisin poliisimies osallistuu suojelupoliisin ja ulkomaan tiedustelu- tai turvallisuusviranomaisen yhteiseen operaatioon toisen valtion alueella.

Jos yhteinen tiedonhankinta toteutettaisiin yhteistyössä sen valtion kanssa, jonka alueella tiedustelumenetelmiä olisi tarkoitus käyttää, on noudatettava kyseisen valtion toiminnalle asettamia rajoituksia. Tällöin suojelupoliisin poliisimies voisi osallistuessaan yhteiseen operaatioon toisessa valtiossa käyttää kyseisen valtion suostumuksella tässä luvussa tarkoitettuja tai niitä vastaavia tiedustelumenetelmiä. Tiedustelumenetelmiä voitaisiin tässä tapauksessa käyttää vain siinä laajuudessa ja sillä tavoin kuin kyseinen valtio tämän sallii. Säännös koskisi siis yhteistyötä kyseisen aluevaltion kanssa. Ilmaisun "yhteistyössä" voitaisiin katsoa kattavan myös sellaisen aluevaltion suostumukseen perustuvan yhteisen operaation, johon aluevaltio ei itse osallistu. Jos yhteinen operaatio sen sijaan suoritettaisiin kolmannen valtion alueella, niin suojelupoliisin käyttämiin tiedustelumenetelmiin sovellettaisiin ulkomaantiedustelusta säädettyä.

Suojelupoliisin poliisimies olisi ulkomailla myös yhteisessä operaatiossa toimiessaan suojelupoliisin ohjauksen sekä sisäisen että ulkoisen valvonnan alainen ja häntä koskettaisi samat oikeudet ja velvollisuudet kuin muussakin ulkomaantiedustelussa.

Pykälän 3 momentin 1. virkkeen mukaan suojelupoliisin päällikkö päättäisi kansainväliseen yhteistyöhön osallistumisesta ja tiedustelumenetelmien käytöstä. Toisin kuin yhteisoperaatioon osallistumista koskeva päätös, joka siis perustuisi yksin tähän pykälään, tiedustelumenetelmän käytön päättämiseen ulkomailla toteutettavien yhteisoperaatioiden tilanteissa sovellettaisiin 39 §:ssä säädettyä.

Päätös yhteiseen operaatioon osallistumisesta olisi perusteltava Suomen kansallisen turvallisuuden suojaamisella. Näin ollen toisen valtion kanssa kyseisen valtion alueella suoritettavalla yhteisoperaatiolla tulisi olla ainakin välillinen kosketuspinta Suomen kansallisen turvallisuuden suojaamiseksi. Tällainen tilanne voisi olla esimerkiksi silloin, kun toisen valtion alueella toimivan terroristiryhmän toiminnasta olisi tarpeen saada tietoa ja olisi oletettavaa, että kyseisen ryhmän toiminnan vaikutukset ulottuisivat tai tulisivat ulottumaan Suomen kansallisen turvallisuuden piiriin.

Kansainvälisen avun antamista ja pyytämistä koskevasta päätöksenteosta säädetään erikseen kansainvälisen avun antamisesta ja pyytämisestä annetussa laissa (418/2017).

Pykälän 3 momentin 2. virkkeessä säädettäisiin, että vieraan valtion toimivaltaisella virkamiehellä olisi suojelupoliisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä.

Toisin kuin 3 momentin 1. virkkeessä, tässä sallittaisiin suojelupoliisin päällikön päätöksellä, että toisen valtion virkamies osallistuu yhteiseen operaatioon Suomen alueella. Myös päätöksen siitä, että vieraan valtion virkamies voisi käyttää eräitä momentissa erikseen säädettyjä tiedustelumenetelmiä, tekisi suojelupoliisin päällikkö. Vieraan valtion virkamies voisi osallistua yhteistoimintaan Suomessa vain silloin, kun se olisi hänen lähettäjävaltionsa lainsäädännön sallimaa. Vieraan valtion virkamies toimisi yhteistoiminnassa suojelupoliisin vastuulla, määräysvallassa ja johdolla sekä Suomen lainsäädännön mukaisesti. Suomessa toimiessaan vieraan valtion virkamiehen tulee noudattaa niitä ohjeita ja määräyksiä, jotka suojelupoliisin poliisimies hänelle antaa sekä noudattaa niitä rajoituksia, jotka suojelupoliisi hänelle asettaa.

Vieraan valtion virkamiehelle voitaisiin suojelupoliisin päällikön päätöksellä antaa lupa käyttää suunnitelmallista tarkkailua (9 §), peiteltyä tiedonhankintaa (10 §), peitetoimintaa (18 §), valeostoa (20 §) ja tietolähteen ohjattua käyttöä (24 §). Kyseiset tiedustelumenetelmät merkitsevät vähäistä puuttumista perusoikeuksiin, eikä yhdelläkään niistä kajottaisi luottamuksellisen viestin salaisuuden suojaan. Vieraan valtion virkamies voisi käyttää näitä tiedustelumenetelmiä suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa, jolloin vastuu yhteisestä tiedonhankinnasta ja siinä käytettävistä tiedustelumenetelmistä olisi suojelupoliisilla. Suunnitelmallista tarkkailua voitaisiin tehdä niin reaalimaailmassa kuin tietoverkossakin. Erityisesti tietoverkossa tapahtuvassa tarkkailussa voitaisiin tarvita toisen valtion sellaisen virkamiehen apua, jolla olisi suojelupoliisilta puuttuva ominaisuus tai osaaminen, kuten kielitaito tai kulttuurin tuntemus, jota suojelupoliisin virkamiehillä ei ole. Vastaavanlainen yhteisoperaation tarve voi liittyä peiteltyyn tiedonhankintaan, peitetoimintaan, valeostoon ja tietolähteen ohjattuun käyttöön. Kyse olisi siitä, että vieraan valtion virkamies toimisi suojelupoliisin tiedonhankintaoperaatiossa avustavassa roolissa. Ulkomaisella virkamiehellä voi olla sellaista osaamista tai muita ominaisuuksia, joita suomalaisella virkamiehellä ei ole ja joita tarvittaisiin operaation onnistuneeksi toteuttamiseksi.

Pykälän 4 momentin mukaan suojelupoliisi voisi salassapitosäännösten estämättä luovuttaa tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua. Momentissa tarkoitetun tietojen luovuttamisen pitäisi ensinnäkin perustua suojelupoliisin tehtävään suojata kansallista turvallisuutta. Käytännössä kyse voisi olla tiedustelumenetelmien tekniikkaa ja taktiikkaa, haittaohjelmia koskevista tiedoista tai turvallisuusuhkia koskevista analyyseistä taikka muusta sellaisesta tiedosta, jonka luovuttaminen olisi Suomen intressien mukaista. Tiedon luovuttamisen tulisi toisaalta aina olla kansallisen edun mukaista. Tällaisen edun piiriin kuuluvat esimerkiksi tiedot Suomen poliittisista tai taloudellisista suhteista toisen valtion kanssa, sotilastiedustelua tai sotilaallista maanpuolustusta koskevat tiedot taikka tiedot kansainvälisen tiedusteluyhteistyön turvaamiseksi. Tietojen luovuttamisen hyväksyttävyyttä tulisi näin ollen arvioida yhtäältä kansallisen turvallisuuden suojaamisintressin ja toisaalta kansallisten etujen turvaamisintressin kannalta. Tässä kokonaisarvioinnissa olisi otettava huomioon myös luovutettavan tiedon ominaisuudet sekä tiedon vastaanottajana oleva taho.

Tiedon luovuttamisesta tulisi aina tehdä tarvittavat kirjaukset jälkikäteisen oikeudellisen valvonnan mahdollistamiseksi.

Pykälän 5 momentissa säädettäisiin, että henkilötietojen luovuttamiseen sovelletaan henkilötietojen käsittelystä poliisitoimessa annettua lakia (761/2003). Henkilötietojen luovuttamiseen kansainvälisessä yhteistyössä sovellettaisiin siten kyseistä lakia, eikä tämän pykälän 5 momenttia.

58 §. *Tiedustelutoiminnan yhteensovittaminen.* Pykälän 1 momentissa säädettäisiin tiedustelun yhteensovittamisesta. Pykälän mukaan tasavallan presidentti, valtioneuvoston kanslia, ulkoasiainministeriö, sisäministeriö ja puolustusministeriö sekä tarvittaessa muut ministeriöt ja viranomaiset sovittaisivat yhteen siviili- ja sotilastiedustelutoimintaa.

Ulko- ja turvallisuuspoliittisen ministerivaliokunnan tehtävänä on valmistelevasti käsitellä tärkeät ulko- ja turvallisuuspolitiikkaa ja muita Suomen suhteita ulkovaltoihin koskevat asiat, näihin liittyvät tärkeät sisäisen turvallisuuden asiat sekä tärkeät kokonaismaanpuolustusta koskevat asiat samoin kuin näiden asioiden yhteensovittamista koskevat kysymykset.

Momentissa mainitaan tasavallan presidentin ja valtioneuvoston organisaation lisäksi myös viranomaiset, minkä johdosta tiedustelutoiminnan valmisteleva yhteensovittaminen voisi tapahtua laajemmalla asiantuntijapohjalla esimerkiksi tiedustelun ja tilannekuvan koordinaatioryhmässä, johon kuuluu jäseninä muun muassa pääesikunnan tiedustelupäällikkö ja suojelupoliisin päällikkö. Heidän lisäkseen olisi mahdollista kutsua muiden ministeriöiden ja viranomaisten edustajia, jos tälle ilmenisi tarvetta.

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 tiedonhankintaprioriteettien osoittamisesta ja koordinoinnista sekä tiedustelutoiminnan tehtävien jakamisesta siviili- ja sotilastiedustelun välillä tiedustelun kohteita ja uhan luonnetta koskevan tarkoituksenmukaisuusharkinnan perusteella. Tämän harkinnan yhteydessä voitaisiin arvioida esimerkiksi muualla kuin Suomessa toteutettavaan siviili- ja sotilastiedusteluun mahdollisesti liittyviä ulkopoliittisia herkkyyksiä ja vaikutuksia Suomen kansainvälisiin suhteisiin. Tiedustelutoiminnan yhteensovittamisessa ei sitä vastoin olisi kyse tiedustelun valvonnasta tai operatiiviseen toimintaan, kuten tiedustelumenetelmän käyttämisestä päättämiseen, ulottuvasta ohjauksesta.

Pykälän 2 momentin mukaan, jos siviilitiedustelutoiminnalla arvioidaan olevan ulko- ja turvallisuuspoliittisia vaikutuksia, asia on valmistelevasti käsiteltävä 1 momentissa tarkoitettujen viranomaisten kesken. Myös nykyisin 1 momentissa tarkoitetut viranomaiset valmistelevat ulko- ja turvallisuuspoliittisesti merkittäviä asioita yhdessä ennen niiden viemistä ulko- ja turvallisuuspoliittisen ministerivaliokunnan käsiteltäväksi. Tehtävä ei kuitenkaan olisi ministerivaliokunnan tehtävän kanssa päällekkäinen, vaan momentissa tarkoitettu prosessi olisi valiokunnan käsittelyä edeltävä toimenpide ulko- ja turvallisuuspoliittisen ministerivaliokunnan käsittelyn sujuvoittamiseksi ja yhtäjaksoisen käsittelyn takaamiseksi.

Sotilastiedustelulain 17 §:ssä ehdotetaan säädettäväksi tiedustelutoiminnan yhteensovittamisesta samoin kuin tässä pykälässä.

59 §. *Siviilitiedustelun valvonta sisäasiainhallinnossa.* Pykälässä säädettäisiin suojelupoliisiin kohdistuvasta siviilitiedustelun sisäisestä valvonnasta. Pykälän mukaan tässä luvussa tarkoitettua tiedonhankintaa valvoisi suojelupoliisin päällikkö sekä sisäministeriö.

60 §. *Kertomuksen antaminen eduskunnan oikeusasiamiehelle ja tiedusteluvaltuutetulle*. Pykälän 1 momentin mukaan sisäministeriön olisi annettava eduskunnan oikeusasiamiehelle vuosittain kertomus tässä luvussa tarkoitettujen tiedustelumenetelmien ja siviilitiedustelun suojaamisen käytöstä ja valvonnasta. Tämä edellyttäisi sitä, että suojelupoliisi toimittaisi sisäministeriölle kertomuksen laatimiseksi tarvittavat tiedot ministeriön edellyttämällä tavalla.

Pykälän 2 momentissa olisi viittaussäännös tiedustelutoiminnan valvonnasta annettuun lakiin. Viittaussäännöksen lisääminen on perusteltua, koska tiedusteluvaltuutetun harjoittama laillisuusvalvonta ja eduskunnan harjoittama parlamentaarinen valvonta ovat keskeisimpiä tiedustelutoiminnan valvonnan elementtejä.

61 §. *Tiedusteluvaltuutetulle tehtävät ilmoitukset*. Pykälän 1 momentin mukaan suojelupoliisin olisi annettava tieto tiedusteluvaltuutetulle tämän luvun nojalla annetuista tuomioistuimen päätöksistä ja luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen.

Tiedustelutoiminnan luonteen vuoksi sekä tuomioistuimen tehtävän takia on tarkoituksenmukaista, että siviilitiedusteluviranomaisena toimiva suojelupoliisi tekisi ilmoituksen tiedusteluvaltuutetulle myönnetystä luvasta. Ilmoitusvelvollisuus pitäisi sisällään myös niin sanotuista kiirepäätöksistä tuomioistuimen tekemät kielteiset päätökset sekä 16 §:n 2 momentissa tarkoitetut tuomioistuimen antamat luvat ja kielteiset päätökset. Käytännössä tiedonantovelvollisuus tulisi täytettyä toimittamalla jäljennös tuomioistuimen antamasta päätöksestä tiedusteluvaltuutetulle. Samassa yhteydessä myös asiaa koskeva lupahakemus voitaisiin toimittaa tiedusteluvaltuutetulle.

Ilmoitus olisi myös merkittävässä osassa toteutettaessa tiedustelumenetelmien käytön ulkoista valvontaa. Tiedusteluvaltuutetulla olisi oltava ajantasainen tieto siitä, minkä tyyppisiä toimivaltuuksia suojelupoliisi siviilitiedustelussa käyttäisi. Tiedusteluvaltuutettu valvoisi muun muassa, että suojelupoliisi toimisi tuomioistuimen myöntämän lupapäätöksen edellyttämissä rajoissa.

Pykälän 2 momentissa säädettäisiin tiedusteluvaltuutetulle tehtävistä muista kuin 1 momentissa tarkoitetuista ilmoituksista. Suojelupoliisin olisi ilman aiheetonta viivytystä ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee: 1) muuta kuin 2 momentissa tarkoitettua tiedustelumenetelmää; 2) siviilitiedustelun suojaamista (36 §); 3) ilmaisukieltoa (38 §); 4) 44 §:n 1 momentissa tarkoitetun ilmoituksen siirtämistä.

Edellä 1 momentissa säädettyä ilmoitusmenettelyä tärkeämpää on, että tiedusteluvaltuutettu saisi tiedon muista kuin tuomioistuimen myöntämistä luvista. Riippumattoman oikeudellisen valvonnan mahdollistaminen tällaisissa asioissa on tosiasiallisesti merkittävää, koska tiedusteluviranomaisen itse tekemiin päätöksiin ei ole tehty ulkopuolista objektiivista arviota ennen tiedustelumenetelmän käyttöön ottoa – toisin kuin tuomioistuimen ollessa luvan myöntäjänä.

Pykälän 3 momentin mukaan tiedustelumenetelmää koskevan päätöksen ilmoittamisessa olisi kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

Tiedustelumenetelmien käyttö ja niistä tehtävät päätökset sisältävät tietoja, jotka ovat luonteeltaan hyvin arkaluonteisia salassa pidettäviä. Salassapitovelvollisuuden toteutumiseen ja tietoturvallisuuden varmistamiseen olisi pykälässä tarkoitettujen ilmoitusten tekemisessä kiinnitettävä erityistä huomiota. Tiedusteluvaltuutetulle tehtävän ilmoituksen tulisi tapahtua niin, ettei ilmoituksen tekemisestä aiheudu salassa pidettävän tiedon paljastumisriskiä. Ilmoituksen

kohteena olevia tietoja tulee käsitellä ainoastaan sellaisissa tiloissa, jotka on todettu tila- ja rakenneturvallisuudeltaan sellaisiksi, että niissä on turvallista käsitellä tietoja ilman paljastumisriskiä.

Jos ilmoitusvelvollisuus toteutetaan automaattisen tietojenkäsittelyn avulla, niin tiedonsiirtoyhteyden tulee olla sellainen, ettei se itsessään aiheuta riskiä salassa pidettävien tietojen paljastumiselle. Ainakin muiden kuin pykälän 1 momentissa tarkoitettujen ilmoitusten kohdalla olisi perusteltua, että ilmoituksen perusteena oleviin päätöksiin perehtyminen tapahtuisi tiedusteluviranomaisen tiloissa. Ilmoitus päätöksestä voisi tapahtua sellaisen viestintälaitteen välityksellä, joka teknisten ominaisuuksiensa puolesta mahdollistaisi sen, että tiedot olisivat ainoastaan tietosuojavaltuutetun saatavilla.

Ilmoitusmenettelyn ei itsessään tulisi muodostua sellaiseksi, että siitä aiheutuvat kustannukset olisivat selvässä epäsuhteessa tiedusteluvaltuutetulle tehtävän ilmoituksen tarkoituksen toteutumisen kanssa.

62 §. *Tarkemmat säännökset.* Pykälässä säädettäisiin niistä asioista, joista voitaisiin säätää valtioneuvoston asetuksella tai sisäministeriön asetuksella.

Pykälän 1 momentin mukaan valtioneuvoston asetuksella voitaisiin säätää: 1) tiedustelumenetelmien käytön ja niiden suojaamisen järjestämisestä; 2) toimenpiteiden kirjaamisesta valvontaa varten; 3) siviilitiedustelun valvontaa varten annettavista selvityksistä; 4) rikostorjuntaan luovutettavan tiedon siirtämistä koskevasta menettelystä ja siinä yhteydessä annettavista tarpeellisista tiedoista (44 §:n 1 momentti); 5) suojelupoliisin ja sotilastiedusteluviranomaisen välisen yhteistyön järjestämisestä (54 §); 6) suojelupoliisin ja muiden viranomaisten välisen yhteistyön järjestämisestä (55 §); 7) salaisen tiedonhankinnan yhteensovittamisen järjestämisestä (56 §); 8) tiedustelutoiminnan yhteensovittamisen järjestämisestä (58 §).

Siviili- ja sotilastiedustelulainsäädännön yhteydessä olisi tarpeen säätää ainakin 1–4 kohdissa tarkoitetuista asiakokonaisuuksista valtioneuvoston asetuksella jo ennen lain voimaantuloa.

Pykälän 2 momentin mukaan sisäministeriön asetuksella voitaisiin säätää: 1) siviilitiedustelun valvonnan järjestämisestä sisäasiainhallinnossa (59 §); 2) suojelupoliisin ja muun sisäasiainhallinnon välisen yhteistyön järjestämisestä; 3) suojelupoliisin kansainvälisen yhteistyön järjestämisestä (57 §).

Kaikissa asetuksenantovaltuussäännöksissä ilmenee, että ne on rajattu teknisiin tai menettelyllisiin seikkoihin. Esimerkiksi valtuussäännöksen 1 momentin 1–4 kohdat ovat asiallisesti vastaavansisältöiset poliisilain 5 luvun 65 §:n ja pakkokeinolain 10 luvun 67 §:n kanssa

Asioiden luonne huomioon ottaen säätäminen asetustasolla on perusteltua, koska kyse ei ole yksilön oikeuksista ja velvollisuuksista, jolloin asiasta tulisi säätää lailla, vaan viranomaisen sisäisen toiminnan tai viranomaisten välisen toiminnan järjestämisestä.

9 luku **Erinäiset säännökset**

8 §. *Liikkumis- ja oleskelurajoitukset.* Pykälään tehtäisiin tekninen tarkistus, jolla sisäasiainministeriö muutettaisiin sisäministeriöksi.

9 §. *Kansainvälinen yhteistoiminta.* Pykälän 2 momenttiin tehtäisiin tekninen tarkistus, jolla sisäasiainministeriö muutettaisiin sisäministeriöksi.

10 §. *Tarkemmat säännökset.* Pykälän 1 momenttiin tehtäisiin tekninen tarkistus, jolla sisäasiainministeriö muutettaisiin sisäministeriöksi.

1.2 Laki tietoliikennetiedustelusta siviilitiedustelussa

1 §. *Soveltamisala ja suhde muuhun lainsäädäntöön.* Pykälä koskisi lain soveltamisalaa ja lain suhdetta muuhun lainsäädäntöön.

Pykälän 1 momentissa todettaisiin laissa säädettävän tietoliikennetiedustelun käyttämisestä siviilitiedustelussa. Siviilitiedustelulla tarkoitettaisiin säädettäväksi ehdotettavan poliisilain 5 a luvun 1 §:n 1 momentin mukaan suojelupoliisin suorittamaa tiedustelua, jolla hankitaan tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Siviilitiedustelun kohteesta eli kansallista turvallisuutta vakavasti uhkaavista toiminnoista säädettäisiin poliisilain 5 a luvun 3 §:ssä ja tämän lain 3 §:ssä. Säännökset olisivat samasanaiset. Koska siviilitiedustelulla poliisilain 5 a luvun 1 §:n 1 momentin mukaan tarkoitettaisiin ainoastaan suojelupoliisin suorittamaa tiedustelua, seuraa tästä, että ainoastaan suojelupoliisi voisi käyttää tämän lain mukaista tietoliikennetiedustelua. Tämä seikka ilmenisi myös muun muassa 7, 9 ja 10 §:n säännöksistä.

Pykälän 2 momentti olisi luonteeltaan informatiivinen. Sen ensimmäisessä virkkeessä todettaisiin, että tietoliikennetiedustelun käyttämisestä sotilastiedustelussa ja tietoliikennetiedustelun teknisestä toteuttamisesta säädetään sotilastiedustelulaissa. Virkkeen tarkoituksena olisi kertoa, että tietoliikennetiedustelua koskevaa sääntelyä sisältyisi tämän lain ohella myös toiseen lakiin. Sotilastiedustelun käyttämän tietoliikennetiedustelun kohteet määräytyisivät sotilastiedustelulain mukaan ja ne olisivat osaksi toiset kuin tässä laissa. Toisaalta sotilastiedustelulaki sisältäisi myös sellaisia tietoliikennetiedustelun teknistä toteuttamista koskevia säännöksiä, jotka täydentävät tämän lain sääntelyä. Tämän lain 10 §:n mukaan puolustusvoimien tiedustelulaitos toimisi tietoliikennetiedustelua koskevien suojelupoliisin toimeksiantojen teknisenä toteuttajana. Teknisen toteuttajan roolissaan puolustusvoimien tiedustelulaitos soveltaisi paitsi edellä mainittua tämän lain 10 §:ää, myös sotilastiedustelulakiin sisältyviä teknistä toteuttamista koskevia säännöksiä. Tällaisia säännöksiä olisivat muun muassa sotilastiedustelulain 66, 72 ja 73 §.

Momentin toisessa virkkeessä todettaisiin, että siviilitiedustelussa käytettävästä telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta sekä televalvonnasta säädetään poliisilain 5 a luvussa. Tietoliikennetiedustelu muistuttaisi kyseisiä poliisilaissa säänneltäviä tiedustelumenetelmiä siltä osin, että siinäkin olisi kyse sähköiseen viestintään kohdistuvasta tiedustelusta. Erona olisi se, ettei tietoliikennetiedustelua näistä menetelmistä poiketen lähtökohtaisesti olisi tarkoitus kohdistaa mihinkään ennalta yksilöitävissä olevaan teleosoitteeseen tai telepäätelaitteeseen tietyn henkilön viestiyhteyksien seuraamiseksi. Se, tulisiko tiedon hankkimisessa käyttää tietoliikennetiedustelua vai poliisilain 5 a luvun menetelmiä, määräytyisi 6 §:n 2 momentin mukaan. Kyseinen säännös asettaisi tietoliikennetiedustelun edellytykseksi välttämättömyyden. Välttämättömyysedellytys pitäisi sisällään sen, että tietoliikennetiedustelua voidaan käyttää vain, jos tietoja ei voida hankkia tai niiden hankkiminen olisi kohtuuttoman vaikeaa muulla tavoin. Jos telepäätelaitteen tai teleosoitteen yksilöintitiedot olisivat siviilitiedusteluviranomaisen tiedossa eikä poliisilain 5 a luvun mukaisten teletiedustelumenetelmien käyttö muuten olisi erittäin vaikeaa, tietoliikennetiedustelun käytölle säädettäväksi ehdotettu välttämättömyysedellytys ei täyttyisi. Välttämättömyysedellytys ei kuitenkaan edellyttäisi vertailua ainoastaan mahdollisuuksiin hankkia tiedot edellä mainituilla teletiedustelumenetelmillä, vaan myös mahdollisuuksiin hankkia ne muilla poliisilain 5 a luvussa säädettäväksi ehdotetuilla menetelmillä.

Pykälän 3 momentissa todettaisiin se seikka, että tietoliikennetiedustelulla saatujen tietojen käsittelyä koskevia säännöksiä sisältyisi paitsi tähän lakiin, myös lakiin henkilötietojen käsittelystä poliisitoimessa (761/2003). Tähän lakiin ehdotetaan otettavaksi vain välttämättömät säännökset henkilötietojen käsittelystä. Tällaisia olisivat säännökset tietoliikennetiedustelun käyttöä rajoittavista tiedustelukielloista (ehdotettava lain 12 §), tietoliikennetiedustelussa kertyneiden tallenteiden ja asiakirjojen tarkastamisesta (13 §), tallenteiden tutkimisesta (14 §), velvollisuudesta hävittää viipymättä eräät tietoliikennetiedustelulla saadut tiedot (15 §) ja tietoliikennetiedustelulla saadun tiedon luovuttamisesta rikostorjuntaan (17 §). Ratkaisu olisi samankaltainen kuin esimerkiksi poliisilain nykyisessä 5 luvussa. Muilta kuin edellä mainituilta osin henkilötietojen käsittelystä säädettäisiin poliisin henkilötietolaissa, joka on poliisilain 1 luvun 1 §:ssä tarkoitettujen tehtävien suorittamiseksi tarpeellisten henkilötietojen automaattiseen käsittelyyn ja muuhun henkilötietojen käsittelyyn sovellettava yleislaki. Tietoliikennetiedustelulla hankittujen henkilötietojen käsittelystä säätämistä henkilötietojen käsittelystä poliisitoimessa annetussa laissa perustelisi se, että tällaisia tietoja on tarpeen verrata ja analysoida yhdessä muilla tiedustelumenetelmillä saatujen tietojen kanssa niiden relevanssin ja asiayhteyden ymmärtämiseksi. Tällaisen monilähdeanalyysin tuloksena muodostuvia tietoja ei voida pitää puhtaina tietoliikennetiedustelutietoina, jolloin myöskään ei ole tarkoituksenmukaista, että niiden käsittelystä säädettäisiin tietoliikennetiedustelulaissa.

2 §. *Määritelmät.* Pykälä sisältäisi laissa käytettyjen keskeisten käsitteiden määritelmät.

Pykälän 1 kohdan mukaan tietoliikennetiedustelulla tarkoitettaisiin Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä. Määritelmän olennaisia elementtejä olisivat ensinnäkin se, että tietoliikennetiedustelu kohdistuu Suomen rajan ylittävään tietoliikenteeseen, toiseksi se, että rajan ylittyminen tapahtuu viestintäverkossa ja kolmanneksi se, että tietoliikennetiedustelu on luonteeltaan tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa.

Tietoliikenteen Suomen rajan ylittymisellä tarkoitettaisiin sitä, että tietoliikenne tosiasiassa ylittää valtakunnan rajan siirtymällä suomalaisesta viestintäverkosta ulkomaiseen viestintäverkkoon tai päinvastoin. Tietoliikennetiedustelu toteutettaisiin teknisesti mahdollisimman lähellä niitä pisteitä, joissa Suomen viestintäverkko ja ulkomainen kiinteä verkko tai satelliittiverkko kytkeytyvät toisiinsa ja tietoliikenteen rajan ylittyminen siten tapahtuu. Toteuttamispiste olisi näin ollen lähtökohtaisesti niin lähellä rajan ylittävää linkkiä kuin mahdollista. Sijainti voisi kuitenkin olla etäämpänä linkistä, jos se olisi tarkoituksenmukaista jäljempänä 3 kohdassa määriteltävän tiedonsiirtäjän toiminnan kannalta.

Koska myös Suomen sisäiseksi tarkoitettu tietoliikenne voi internetin luonteesta johtuen sattumanvaraisesti reitittyä ulkomaisen viestintäverkon kautta, kuuluisi tällainenkin tietoliikenne periaatteessa määritelmän piiriin. Sen varmistamiseksi, että tietoliikennetiedustelulla ei tästä huolimatta hankittaisi tietoja asialliselta luonteeltaan kotimaisesta viestinnästä, ehdotetaan 12 §:ssä säädettäväksi kotimaista viestintää koskevasta tiedustelukiellosta ja 15 §:ssä sitä koskevasta hävittämisvelvollisuudesta.

Tietoliikenteen rajan ylittymisen olisi tapahduttava viestintäverkossa. Viestintäverkon käsite ehdotetaan määriteltävän pykälän 2 kohdassa tavalla, joka osaltaan rajaisi sitä, minkälaisissa järjestelmissä liikkuvaan tietoliikenteeseen tietoliikennetiedustelua voisi kohdistua.

Tietoliikennetiedustelun määritelmään kuuluisi se, että kyse on tietoliikenteen automaattiseen erotteluun perustuvasta teknisestä tiedonhankinnasta ja hankitun tiedon käsittelystä. Tältä osin määritelmän tarkoituksena olisi tehdä ero tietoliikennetiedustelun ja muiden viestintäverkossa

liikkuvaan tietoliikenteeseen kohdistuvien tiedonhankintakeinojen, ennen kaikkea telekuuntelun ja televalvonnan, välille. Telekuuntelussa ja -valvonnassa tiedon keruu voidaan toteuttaa mahdollisimman lähellä toimenpiteen kohteena olevaa yksittäistä teleosoitetta tai telepäätelaitetta. Tietoliikennetiedustelussa ei olisi kyse yksittäiseen telepäätelaitteeseen tai teleosoitteeseen kohdistuvasta tiedonhankinnasta lähellä toimenpiteen kohdelaitetta tai -osoitetta, vaan automatisoiduin menetelmin tapahtuvasta tietoliikenteen erottelusta sellaisessa kohdassa tietoverkkoa, jonka kautta voidaan olettaa kulkevan mahdollisimman suuri osa tiedustelun kohteena olevaa tietoliikennettä. Käytännössä erottelu toteutettaisiin vertailemalla tietoliikennettä hakuehdoiksi kutsuttaviin ennakkoon asetettuihin kriteereihin. Tietoliikennetiedustelun yhtenä tarkoituksena olisi tunnistaa yksittäisiä telepäätelaitteita ja teleosoitteita telekuuntelun tai -valvonnan toteuttamisen mahdollistamiseksi. Automatisoidun erottelun käytännön toteuttamisesta ehdotetaan säädettäväksi 4 §:ssä.

Määritelmän mukaan tietoliikennetiedustelu pitäisi sisällään paitsi automatisoituun erotteluun perustuvan teknisen tiedonhankinnan, myös hankitun tiedon käsittelyn. Hankitun tiedon käsittelyllä tarkoitettaisiin 5 §:ssä säädettäväksi ehdotettavaa automatisoidusti erotellun tiedon automaattista ja manuaalista jatkokäsittelyä.

Pykälän 2 kohdassa määriteltäisiin viestintäverkon käsite. Käsite on olennainen siksi, että pykälän 1 kohdan määritelmäsäännöksen mukaan tietoliikennetiedustelu voisi kohdistua vain sellaiseen tietoliikenteeseen, joka viestintäverkossa ylittää Suomen rajan. Viestintäverkolla tarkoitettaisiin, samoin kuin sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 39 kohdassa, toisiinsa liitetyistä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla. Olennaista määritelmän kannalta olisi ensinnäkin järjestelmän käyttötarkoitus viestien siirtoon tai jakeluun. Määritelmän sitomisesta järjestelmän käyttötarkoitukseen seuraisi, että tietoliikennetiedustelussa voitaisiin tiedustella myös sellaista viestintäverkossa liikkuvaa tietoliikennettä, jota mahdollisesti ei ole pidettävä viestintänä. Määritelmään kuuluisi toiseksi vaatimus järjestelmän sähkömagneettisesta teknisestä toteutustavasta sekä tämän toteutustavan sisäinen teknologianeutraalius. Määritelmä kattaisi järjestelmät, joissa siirto tai jakelu toteutetaan johtimella, radioaalloilla, optisesti tai millä hyvänsä muulla tavalla, kunhan tuo tapa on sähkömagneettinen.

Pykälän 3 kohdassa määriteltäisiin tiedonsiirtäjän käsite. Tiedonsiirtäjällä tarkoitettaisiin tahoa, joka omistaa tai hallitsee viestintäverkon sitä osaa, joka ylittää Suomen rajan. Määritelmällä on merkitystä sen varmistamiseksi, että tässä laissa ja sotilastiedustelulaissa säädettäväksi ehdotetut velvollisuudet myötävaikuttaa tietoliikennetiedustelun toteuttamiseen kohdentuvat oikeaan tahoon. Velvollisuuksissa olisi kyse ensinnäkin tämän lain 22§:ssä säädettäväksi ehdotetusta tiedonsiirtäjän velvollisuudesta antaa ilman aiheetonta viivästystä suojelupoliisille sellaiset hallussaan olevat tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi tietoliikennetiedustelun käyttöä koskevaa lupavaatimusta ja -päätöstä varten. Toiseksi kyse olisi velvollisuudesta, jonka asettamisella varmistettaisiin se, että rajan ylittävään viestintäverkon osaan eli käytännön tasolla tiedonsiirtoyhteyteen voidaan rakentaa niin sanottu liityntäpiste eli tietoliikennetiedustelun toteuttamispiste. Sotilastiedustelulain 94 §:ssä säädettäisiin tiedonsiirtäjän velvollisuudesta myötävaikuttaa tietoliikennetiedustelun edellyttämän liityntäpisteen toteuttamiseen antamalla puolustusvoimien tiedustelulaitokselle tätä tarkoitusta varten välttämättömät tiedot ja pääsy tiloihin, jossa liityntäpiste on määrä toteuttaa. Tiedonsiirtäjän velvollisuudesta myötävaikuttaa liitynnän rakentamiseen säädettäisiin sotilastiedustelulaissa siitä syystä, että asia liittyy läheisesti tietoliikennetiedustelun tekniseen toteuttamiseen. Liitynnän rakentamisen mahdollistava sääntely palvelisi kuitenkin myös siviilitietoliikennetiedustelun tarpeita.

Tiedonsiirtäjän käsitteen piiriin kuuluisivat sekä viestintäverkon rajan ylittävän osan omistaja että sellaisen osan haltija. Haltijalla tarkoitettaisiin sellaista koti- tai ulkomaista yritystä tai yhteisöä, joka tosiasiassa hallitsee viestintäverkon rajan ylittävää 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. Edellä mainitun rajoituksen johdosta voidaan arvioida, että tiedonsiirtäjän määritelmän piiriin kuuluisi tällä hetkellä enintään kymmenkunta yritystä. On syytä korostaa, että tiedonsiirtäjän määritelmä ei vastaisi sähköisen viestinnän palveluista annetun lain 3 §:n 36 kohdan mukaista viestinnän välittäjän määritelmää, vaan olisi sitä huomattavasti suppeampi.

3 §. *Tietoliikennetiedustelun kohteet.* Pykälässä säädettäisiin tyhjentävästi niistä tietoliikennetiedustelun kohteista, joista tieto tietoliikennetiedustelulla saataisiin hankkia. Tietoliikennetiedustelua ei saataisi käyttää tietojen hankkimiseksi mistään sellaisesta asiasta, ilmiöstä tai uhkasta, jota ei ole erikseen mainittu pykälässä.

Koska siviilitiedustelun kohteet, jotka ovat samat kuin tietoliikennetiedustelun kohteet ja niistä säädetään myös poliisilain 5 a luvun 3 §:ää vastaavasti, viitataan tämän pykälän perusteluiden osalta kyseisen poliisilain pykälän perusteluihin.

4 §. *Tietoliikennetiedustelun käytön edellytykset.* Pykälässä säädettäisiin tietoliikennetiedustelun käytön edellytyksistä.

Pykälän 1 momentin mukaan tietoliikennetiedustelun käytön edellytyksenä olisi, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Kyse olisi niin sanotusta perustellusta tuloksellisuusodotuksesta, jota sovellettaisiin kaikkeen tietoliikennetiedusteluun. Jos tietoliikennetiedustelulla ei voitaisi ylipäätään olettaa saatavan tietoja kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, eli tiedustelun ei voitaisi olettaa olevan tuloksellista, ei sitä saataisi käyttää.

Verrattaessa keskenään pykälän 1 momenttia ja toisaalta sen 2 momenttia voidaan havaita, että sellaiselle tietoliikennetiedustelulle, joka voidaan kohdistaa pelkästään vieraan valtion tietoliikenteeseen, ei asetettaisi muita edellytyksiä kuin se, että tiedustelu on tuloksellista. Tätä tiukempien edellytysten asettamista ei ole pidettävä perusteltuna, sillä valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 ja PeVL 9/2015). Näin ollen esimerkiksi vieraan valtion viranomaisorganisaation viestintä tai muu tietoliikenne ei nauti luottamuksellisen viestin salaisuuden suojaa.

Momentissa mainittaisiin vieraan valtion lisäksi vieraaseen valtioon rinnastuva taho, jonka merkityssisältöä käsitellään tarkemmin poliisilain 5 a luvun 4 §:n 4 momentin perusteluissa. Valtiollisen toimijan tietoliikenteeseen kohdistuvasta tiedustelusta sotilastiedustelussa säädettäisiin sotilastiedustelulain 66 ja 67 §:ssä.

Pelkän 1 momentin mukaisen tuloksellisuusodotuksen soveltaminen edellyttäisi käytännössä, että se vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenne, johon hakuehtoja käytetään, liikkuu viestintäverkossa muusta tietoliikenteestä erillään. Kyse olisi siis tilanteista, jois-

sa hakuehtojen avulla suoritettavan automaattisen vertailun piirissä olisi yksinomaan valtiollista tietoliikennettä esimerkiksi siksi, että se liikkuu sille varatussa viestintäverkon osassa. Jos sen sijaan vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenne olisi sillä tavalla sekoittunut muuhun tietoliikenteeseen, että hakuehtojen käyttö ulottuisi molempiin, tulisi 1 momentin mukaisen tuloksellisuusodotuksen ohella sovellettaviksi myös 2 momentissa säädettäväksi ehdotettu välttämättömyysedellytys.

Pykälän 2 momentin mukaan, jos tietoliikennetiedustelun hakuehtojen käyttö ei koskisi ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, olisi edellytyksenä lisäksi, että tietoliikennetiedustelun voidaan olettaa olevan välttämätöntä tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tietoliikennetiedustelulle asetettaisiin tältä osin tiukempi edellytys kuin poliisilain 5 a luvussa säädettäväksi ehdotetuille luottamuksellisen viestin salaisuuden suojaan puuttuville tiedustelumenetelmille. Ratkaisun taustalla on Euroopan ihmisoikeustuomioistuimen ratkaisu Szabo & Vissy v. Unkari, jonka mukaan ihmisoikeussopimuksen 8 artiklan mukaista "välttämätön demokraattisessa yhteiskunnassa" -edellytystä on tulkittava tietoliikennetiedustelun kaltaisen valvontateknologian yhteydessä siten, että se edellyttää "ehdotonta välttämättömyyttä" (strict necessity) kahdessa suhteessa. Menetelmän käytön tulee olla yleisellä tasolla ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi. Toiseksi menetelmän käytön tulee yksittäisen tiedusteluoperaation yhteydessä olla ehdottoman välttämätöntä olennaisen tärkeän tiedon (vital information) saamiseksi.

Tietoliikennetiedustelun käytön edellytykseksi ehdotettavalla välttämättömyydellä tarkoitettaisiin viimesijaisuutta eli 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 asettaman kriteeristön mukaisesti 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. Säännöksen soveltaminen edellyttäisi vertailua yhtäältä 5 a 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 vähäisemmän mahdollisuuden, että sivullista viestintää tulee tiedustelun piiriin. Näin ollen, jos telekuuntelun tai -valvonnan käyttö ei yksittäistapauksessa olisi mahdotonta tai huomattavan vaikeaa, tulisi niitä käyttää ensisijaisina keinoina suhteessa tietoliikennetiedusteluun.

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. Jos asetettaisiin vaatimus tietoliikennetiedustelulla hankittavan tiedon olennaisesta tärkeydestä, voitaisiin vaatimuksen katsoa viittaavan esimerkiksi siihen, että tiedon tulisi olla välttämätön jonkin kansallista turvallisuutta välittömästi uhkaavan vaaran torjumiseksi. 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 poliisilain 5 a luvussa tarkoitetun tiedustelumenetelmän käytön, mutta jonka ei vielä yksinään voida katsoa

olevan välttämätön uhkan torjumiseksi. Siviilitiedustelu olisi useista toisiaan täydentävistä tiedonhankintamenetelmistä muodostuva kokonaisuus, jonka puitteissa on erittäin vaikea ennakkoon arvottaa ja osoittaa kullakin yksittäisillä menetelmällä saatavan tiedon merkitys tiedonhankinnan kohteena olevaa toimintaa koskevan kokonaiskäsityksen kannalta.

5 §. *Tietoliikennetiedustelun kohdistaminen*. Pykälässä säädettäisiin tietoliikennetiedustelun kohdistamisesta eli siitä, millä tavalla kansallista turvallisuutta vakavasti uhkaavaan toimintaan liittyvä tietoliikenne alustavasti tunnistettaisiin ja ohjattaisiin 6 §:n mukaiseen jatkokäsittelyyn.

Pykälän 1 momentin mukaan tietoliikennetiedustelun kohdistaminen toteutettaisiin sellaisen tietoliikenteen automatisoidun erottelun avulla, joka perustuisi hakuehtojen käyttöön. Hakuehtoja käytettäisiin vain tietyssä osassa viestintäverkkoa kulkevaan tietoliikenteeseen. Tämä viestintäverkon osa olisi määritelty 7 §:n mukaisessa tuomioistuimen lupapäätöksessä tai, poikkeuksellisesti, 9 §:n mukaisessa suojelupoliisin päällikön väliaikaisessa kiirepäätöksessä. Kyseisessä viestintäverkon osassa kulkeva tietoliikennevirta peilattaisiin kulkemaan myös tiedustelujärjestelmän kautta, jolloin tiedustelujärjestelmä vertaisi tietoliikennettä järjestelmään ennakkoon syötettyihin hakuehtoihin. Vertailu suoritettaisiin tietoteknisesti, mistä johtuen kukaan luonnollinen henkilö ei näkisi tiedustelujärjestelmän läpi virtaavaa tietoliikennettä. Ainoastaan sellainen tietoliikenne, joka vastaa hakuehtoja, ohjautuisi tietoliikennetiedustelun seuraavana käsittelyvaiheena olevaan 6 §:n mukaiseen jatkokäsittelyyn. Muu kuin hakuehtoja vastaava tietoliikenne virtaisi tiedustelujärjestelmän läpi eikä se olisi enää myöhemmin palautettavissa tarkasteluun. Hakuehtojen käytön avulla toteutettava tietoliikenteen automatisoitu erottelu olisi tietoliikennetiedustelun teknistä toteuttamista, josta 10 §:n mukaan suojelupoliisinkin puolesta vastaisi puolustusvoimien tiedustelulaitos.

Pykälän 2 momentissa säädettäisiin hakuehtojen luonteesta. Säännöksestä ilmenevän pääsäännön mukaan hakuehto ei saisi kuvata viestin sisältöä. Viestin sisällöllä tarkoitettaisiin lähettäjän vastaanottajalle tarkoittamaa viestin semanttista sisältöä. Kiellon johdosta hakuehto ei saisi kuvata esimerkiksi viestivien henkilöiden käyttämiä ilmaisuja tai viestin sisältöön kuuluvia henkilöiden nimi- tai muita yksilöintitietoja. Sisältöä kuvaavan hakuehdon käyttökielto koskisi myös pilvipalveluun tallennettavan tai pilvipalvelusta noudettavan asiakirjan tai tiedoston sisältöä. Sisällöllisten hakuehtojen käyttökielto koskisi kaikkia muita tapauksia kuin niitä, joissa hakuehtoja verrataan pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen tai hakuehto kuvaa haitallisen tietokoneohjelman tai -käskyn sisältöä. Poikkeukset kiellosta liittyisivät sellaisiin tietoliikenteen lajeihin, joiden ei voida katsoa nauttivan luottamuksellisen viestin salaisuuden suojaa. Jos kyse sen sijaan olisi perusoikeussuojaa nauttivasta tietoliikenteestä, ei viestin sisältöä kuvaavien hakuehtojen käyttö olisi ylipäätään sallittua.

Tietoliikennetiedustelusta säätäneiden eurooppalaisten vertailuvaltioiden lainsäädännöissä ei ole asetettu yllä kuvatun kaltaisia rajoituksia tai esteitä käyttää sisällöllisiä hakuehtoja. Viestin sisältöä kuvaavien hakuehtojen käyttö on kyseisissä maissa sallittua. Sisällöllisten hakuehtojen käytölle ehdotettavat rajoitukset olisivat näin ollen omintakeinen suomalainen ratkaisu. Tarkoituksena olisi mahdollisimman pitkälle turvata sivullisen asemassa olevien henkilöiden nauttima luottamuksellisen viestin salaisuuden suojan ydinalue.

Sisällöllisten hakuehtojen käyttökiellosta johtuen hakuehdot saisivat kuvata ainoastaan viestinnän ohjaustietoja ja muita sellaisia tietoja, joiden ei voida katsoa kuuluvan lähettäjän vastaanottajalle tarkoittamaan viestin semanttiseen sisältöön. Ohjaustietoja ovat tietoverkolle taikka lähettävälle tai vastaanottavalle tietojärjestelmälle tarkoitetut ohjeet, komennot ja muut metatiedot, joilla vaikutetaan viestin kuljetukseen ja ohjaamiseen verkossa ja tietojärjestelmässä.

Tietoliikennetiedustelussa ohjaustieto erotettaisiin viestin sisällöstä verkkoliikenteen toimintaa kuvaavan OSI-viitemallin sovelluskerroksen tasolla. Kun erottaminen tapahtuisi sovelluskerroksen tasolla, luettaisiin ohjaustiedoksi myös sellainen tieto, jonka avulla viesti ohjataan tarkasti oikealle vastaanottajalle vastaanottavan laitteen viestintäohjelmistossa. Esimerkki tällaisesti tiedosta, jota ei sovelluskerrokselta asiaa tarkasteltaessa lueta viestin sisällöksi ja jota niin ollen olisi sallittua käyttää hakuehtona, olisi viestin lähettäjän tai vastaanottajan sähköpostiosoite.

Ohjaustiedon ja viestin sisältötiedon välinen rajanveto ei tietoliikennetiedustelussa kuitenkaan määrittyisi puhtaasti tietoteknisesti. Ratkaisevaa sen kannalta, katsotaanko hakuehto viestin sisältöä kuvaavaksi tiedoksi vai ohjaustiedoksi, olisi merkkijonon tarkoitus tietoliikennevirrassa eli se, esiintyykö hakuehdon kohde 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 viestin semanttisena sisältönä, jota hakuehto ei saisi kuvata. Sen sijaan hakuehtoina tulisivat kyseeseen sähköpostiosoitteet, sosiaalisen median palveluiden käyttäjätunnukset ja teleosoitteet. Hakuehto voisi myös olla rakenteinen siten, että se muodostuisi joukosta ohjaustietoja, esimerkiksi ip-osoitteen, kohdeportin ja jonkin kuljetuskerroksen tunnisteen yhdistelmästä. Lisäksi hakuehtoina voisivat olla IP-osoitealueet, autonomisten järjestelmien numerot (AS-numerot) ja domain-nimet. Koska myöskään esimerkiksi tietyn salaustekniikan tai aakkosmerkistön käyttö ei vielä sinänsä ilmaise mitään viestin merkityksellistä sisältöä, voitaisiin myös tällaisia hakuehtoja käyttää.

Momentin mukaan viestin varsinaista merkityssisältöä kuvaavia hakuehtoja saataisiin pääsäännöstä poiketen käyttää kahdessa tapauksessa. Molemmat poikkeukset perustuisivat ns. tiedonhankintalakityöryhmän mietinnössä (s. 64 ja s. 80) esitettyihin suosituksiin siitä, kuinka tietoliikennetiedustelun kohdistaminen voitaisiin järjestää. Näiden suositusten mukaisesti viestin sisältöä kuvaavan hakuehdon käyttö olisi sallittua vain silloin, kun kyse on sellaisesta tietoliikenteestä, jonka ei voida katsoa ylipäätään nauttivan luottamuksellisen viestin salaisuuden suojaa. Tällaisia tietoliikenteen lajeja ovat momentissa mainitut vieraan valtion tietoliikenne ja haittaohjelmaliikenne.

Poikkeuksista ensimmäinen liittyisi vieraan valtiotoimijan tai sellaiseen rinnastuvan tahon tietoliikenteeseen. 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 perustuslaillista luottamuksellisen viestin salaisuuden suojaa. Vieraaseen valtioon rinnastuvalla taholla tarkoitettaisiin valtionomaisen rakenteen omaavaa toimijaa, joka määrätyllä alueella käyttää omintakeista ja pysyvää valtaa. Myöskään tällaisen toimijan ei voida katsoa nauttivan perusoikeussuojaa.

Säännöksen mukaan, jos tietoliikennetiedustelu voidaan kohdistaa pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen, saataisiin hakuehtona käyttää viestin sisältöä kuvaavaa tietoa. Hakuehtona voisi tällöin olla viestin sisällöstä löytyvä merkkijono, esimerkiksi luonnollisen kielen sana tai lause.

Vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikennettä koskevan poikkeuksen soveltaminen tulisi kyseeseen vain niissä tapauksissa, joissa tiedustelujärjestelmään peilattavaan tietoliikennevirtaan ei voi päätyä luottamuksellisen viestinnän salaisuuden suojaa nauttivaa tietoliikennettä. Käytännössä tämä edellyttäisi, että se rajan ylittävän viestintäverkon osa, jonka sisältämä tietoliikenne peilataan tiedustelujärjestelmään hakuehtojen käyttöä varten, on varattu yksinomaan valtiollista tietoliikennettä varten.

Poikkeuksista toinen koskisi haitallista tietokoneohjelmaa tai käskyä. Tietokoneohjelman tai -käskyn haitallisuudella tarkoitettaisiin säännöksen yhteydessä ohjelman tai käskyn teknistä tietoturvallisuutta vaarantavaa luonnetta. Kyse olisi ohjelmasta tai käskystä, joka pyrkii anastamaan tietoa kohdejärjestelmästä, muuttamaan kohdejärjestelmän sisältämää tietoa oikeudetta tai haittaamaan kohdejärjestelmän toimintaa. Kohdejärjestelmäksi katsottaisiin mikä tahansa digitaalinen järjestelmä, myös itse verkko eli tietoliikennettä ohjaavat verkkolaitteet sekä reaalimaailman prosesseja ohjaavat laitteet.

Haitallisia tietokoneohjelmia ja -käskyjä kuvaavat poikkeussäännöksen sallimat sisällölliset hakuehdot olisivat käytännössä erilaisia teknisiä merkkijonoja eivätkä luonnollisen kielen sanoja tai ilmaisuja. Hakuehtojen erityisen luonteen vuoksi ei edellytettäisi vastaavasti kuin vieraan valtion tietoliikenteen sisältöä kuvaavien hakuehtojen osalta, että niitä ei saisi lainkaan verrata luottamuksellisen viestin salaisuuden suojaa nauttivaan tietoliikenteeseen. Haittaohjelman sisältöä kuvaavien hakuehtojen vertaaminen laajempaankin tietoliikennevirtaan olisi näin ollen sallittua. Ratkaisu olisi sekä teknisesti että asiallisesti sama kuin se, josta säädetään sähköisen viestinnän palveluista annetun lain (917/2014) toimenpiteitä tietoturvan toteuttamiseksi koskevassa 272 §:ssä. Kyseisen pykälän 1–2 momentin mukaan teleyrityksellä, yhteisötilaajalla ja lisäarvopalvelun tarjoajalla sekä niiden lukuun toimivalla on oikeus viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi ja estämiseksi muun muassa selvittää viestien sisältö automaattisesti. Käytännössä kyse on siitä, että säännöksessä tarkoitettu teleyritys, yhteisötilaaja tai muu vastaava taho vertaa hakuehtona käyttämäänsä haittaohjelmatunnistetta kaikkien käsittelemiensä viestien sisältöön.

Pykälän 3 momentissa säädettäisiin erityisestä kiellosta käyttää tietoliikennetiedustelun hakuehtona Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja. Jos telepäätelaitteen tai teleosoitteen haltija olisi Suomessa ja kyseisen telepäätelaitteen tai -osoitteen yksilöintitiedot suojelupoliisin tiedossa, olisi tiedonhankinta suoritettava poliisilain 5 a luvussa säädettäväksi ehdotettavien salaisten tiedonhankintamenetelmien - telekuuntelun, tietojen hankkimisen telekuuntelun sijasta tai televalvonnan - avulla, sikäli kuin niille säädettäväksi ehdotetut edellytykset täyttyvät. Tällä tavalla tiedonhankinnan vaikutus sivullisten tietoliikenteeseen pystyttäisiin minimoimaan.

6 §. *Automatisoidun erottelun avulla kerätyn tiedon jatkokäsittely.* Pykälässä säädettäisiin tiedusteluviranomaisen oikeudesta käsitellä automaattisesti ja manuaalisesti sellaista tietoa, joka 5 §:ssä tarkoitetulla tavalla olisi eroteltu automaattisesti tietoliikennevirrasta. Päinvastoin kuin 5 §:n mukainen toiminta, kerätyn tiedon jatkokäsittely ei olisi 10 §:ssä säädettäväksi ehdotettua tietoliikennetiedustelun teknistä toteuttamista, mistä johtuen sen suorittaisi siviilitiedusteluviranomaisena toimiva suojelupoliisi eikä puolustusvoimien tiedustelukeskus suojelupoliisin puolesta.

Automaattisella käsittelyllä tarkoitettaisiin sellaista erotellun tiedon analysointia, joka toteutetaan automaattisen tietojenkäsittelyn 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 supistaa manuaalisen käsittelyn kohteeksi otettavan tiedon määrää. Tietojärjestelmän avulla suoritettavat analysointi ja haut voisivat kohdistua 5 §:n nojalla kerättyyn tietoon sisältyviin tunnistamis- ja sijaintitietoihin ja muihin ohjaustietoihin sekä tiedon semanttiseen sisältöön.

Manuaalisella käsittelyllä tarkoitettaisiin erotellun tiedon aistinvaraista havainnointia luonnollisen henkilön toimesta. Koska manuaalisessa käsittelyssä samoin kuin edellä mainitussa au-

tomaattisessa käsittelyssä saataisiin selvittää muun muassa viestin sisältö, kuuluisi manuaaliseen käsittelyyn esimerkiksi se, että suojelupoliisin palveluksessa oleva virkamies selvittäisi käsiteltävänä olevan viestin tekstisisällön, tarkastelisi sen kuvaliitteitä, kuuntelisi ääntä tai antaisi viestisisällön syötteeksi ohjelmistolle, joka ajaisi viestin liitteenä olevaa suoritettavaa koodia laboratorio-olosuhteissa.

Automaattisessa ja manuaalisessa käsittelyssä saataisiin selvittää viestin sisältö ja muut luottamukselliset tiedot. Muilla luottamuksellisilla tiedoilla tarkoitettaisiin viestinnän tunnistamistietoja, välitystietoja ja sijaintitietoja. Poliisilain 5 luvun 8 §:n 1 momentin mukaan tunnistamistiedolla tarkoitetaan tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi. Sähköisen viestinnän palveluista annetussa laissa tunnistamistiedon käsite on, poliisilaista poiketen, korvattu välitystiedon käsitteellä. Sähköisen viestinnän palveluista annetun lain 3 §:n 40 kohdan mukaan välitystiedolla tarkoitetaan oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta ja radiolähettimen käyttäjästä sekä tietoa radiolähetyksen alkamisajankohdasta, kestosta ja lähetyspaikasta. Poliisilaissa käytetty tunnistamistiedon käsite ja sähköisen viestinnän palveluista annetussa laissa käytetty välitystiedon käsite eivät siis ole keskenään identtisiä. Ehdotettavan pykälän mukaisessa automaattisessa ja manuaalisessa käsittelyssä viestinnän luottamukselliset tiedot saataisiin kuitenkin selvittää siihen katsomatta, kuuluvatko ne tunnistamistiedon määritelmän, välitystiedon määritelmän vai molemman käsitteen määritelmän piiriin. Sijaintitiedolla tarkoitetaan sähköisen viestinnän palveluista annetun lain 3 §:n 18 kohdan mukaan viestintäverkosta tai päätelaitteesta saatavaa tietoa, joka ilmaisee liittymän tai päätelaitteen maantieteellisen sijainnin ja jota käytetään muuhun kuin viestin välittämiseen. Viestin sisällölle ei ole vakiintunutta määritelmää, mutta kysymystä viestin sisällön ja muiden luottamuksellisen viestin salaisuuden suojaa nauttivien tietojen välisestä rajanvedosta on käsitelty edellä 5 §:n perusteluiden yhteydessä. Tämän pykälän tulkinnan kannalta merkitystä ei kuitenkaan olisi sillä, kuinka tuo raja asettuu, sillä pykälän tarkoittama oikeus selvittää koskisi edellä todetusti kaikkia luottamuksellisen viestin salaisuuden piiriin kuuluvia tietoja. 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.

Pykälän tarkoittama oikeus selvittää viestin sisältö pitäisi myös sisällään oikeuden selvittää pilvipalveluun tallentamiseen liittyvän liikenteen sisältö, esimerkiksi pilvipalveluun tallennettavan tai sieltä noudettavan asiakirjan sisältö.

Jos automaattisen tai manuaalisen jatkokäsittelyn aikana kävisi ilmi, että käsittelyn kohteena olevaa tietoa koskee 12 §:n mukainen tiedustelukielto tai sitä ei tarvittaisi kansallisen turvallisuuden suojaamiseksi, tulisi se 15 §:n nojalla viipymättä hävittää.

7 §. *Tietoliikennetiedustelua koskeva tuomioistuimen lupa.* Pykälässä säädettäisiin tietoliikennetiedustelua koskevasta tuomioistuimen luvasta sekä tietoliikennetiedustelua koskevan vaatimuksen ja päätöksen sisällöstä.

Pykälän 1 momentin mukaan tietoliikennetiedustelusta päättäisi tuomioistuin suojelupoliisin päällikön kirjallisesta vaatimuksesta. Poliisilain 5 luvussa säädellyistä salaisista tiedonhankintakeinoista poiketen keinon käyttöä koskevalta vaatimukselta edellytettäisiin nimenomaisesti kirjallista muotoa. Kirjallisen vaatimuksen tekijänä voisi olla ainoastaan suojelupoliisin päällikkö, mikä myös olisi poikkeuksellinen ratkaisu suhteessa poliisilain 5 luvussa säädeltyihin salaisiin tiedonhankintamenetelmiin. Vaatimuksen tekijältä edellytettävää erityisen korkeaa

virka-asemaa voidaan perustella tietoliikennetiedustelun muista tiedonhankinta- ja tiedustelumenetelmistä poikkeavalla luonteella. Vaikka kirjallisen vaatimuksen tekijän edellytettäisiin olevan suojelupoliisin päällikkö, ei tästä seuraisi, että suojelupoliisin päällikön olisi oltava henkilökohtaisesti läsnä tuomioistuimessa sen käsitellessä vaatimusta. Vaatimusta käsiteltäessä läsnä voisi suojelupoliisin päällikön sijaan olla sellainen tämän määräämä toinen virkamies, joka on perehtynyt vaatimuksen kohteena olevaan asiaan.

Pykälän 2 momentissa säädettäisiin niistä seikoista, jotka suojelupoliisin päällikön vaatimuksessa tuomioistuimelle ja tuomioistuimen vaatimuksen johdosta tekemässä päätöksessä olisi mainittava.

Momentin 1 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tietoliikennetiedustelun kohteena oleva 3 §:ssä tarkoitettu kansallista turvallisuutta vakavasti uhkaava toiminta. Vaatimuksesta ja päätöksestä olisi näin ollen käytävä ilmi, mistä viitatun pykälän mukaisesta toiminnasta tai toiminnoista tietoliikennetiedustelulla olisi tarkoitus hankkia tietoa.

Momentin 2 kohdan mukaan vaatimuksesta ja päätöksestä olisi käytävä ilmi kansallista turvallisuutta vakavasti vaarantavan toiminnan tosiseikat. Suojelupoliisin edellytettäisiin tuomioistuimelle esittämässään vaatimuksessa tekevän 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 ja mikä taho tai ketkä henkilöt ovat toiminnan taustalla. Suojelupoliisin olisi tuomioistuinta tyydyttävällä tavalla osoitettava, että vaatimuksen kohteena oleva toiminta siitä tiedossa olevien konkreettisten tosiseikkojen perusteella vastaa vaatimuksen edellisessä kohdassa mainittua lain 3 §:ssä tarkoitettua uhkatyyppiä.

Momentin 3 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat. Vaatimuksessa ja päätöksessä olisi ensinnäkin perusteltava 4 §:n 1 momentissa tietoliikennetiedustelun edellytykseksi asetettu tuloksellisuus. Suojelupoliisin olisi vaatimuksessa tehtävä selkoa seikoista, joiden perusteella tietoliikennetiedustelulla voidaan ylipäätään olettaa saatavan tietoja siitä kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, jota vaatimus koskee. Jos vaatimus ei koskisi pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen kohdistuvaa tietoliikennetiedustelua, olisi siinä lisäksi tehtävä selkoa 4 §:n 2 momentissa edellytykseksi asetetun välttämättömyyden täyttymisestä. Vaatimuksessa ja samoin tuomioistuimen päätöksessä olisi tehtävä selkoa siitä, miksi niitä tietoja, jotka tietoliikennetiedustelulla olisi tarkoitus hankkia, ei voida hankkia muulla tavalla, tai miksi niiden hankkiminen muulla tavalla olisi oleellisesti vaikeampaa.

Momentin 4 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille. Tietoliikennetiedustelussa käytettäviä hakuehtoja ja esimerkkejä sellaisista on käsitelty edellä 5 §:n yksityiskohtaisissa perusteluissa. Hakuehtojen ohella tuomioistuimelle esitettävä vaatimus voisi kuitenkin koskea myös hakuehtojen luokkaa. Hakuehtojen luokalla ei hakuehdoista poiketen viitata yksittäiseen tekniseen tietoon, jota voidaan sellaisenaan käyttää tietoliikennevirtaan kohdistettavan automatisoidun erottelun vertailuehtona. Hakuehtojen luokalla tarkoitettaisiin tarkkarajaista suullista kuvausta tiedustelukysymyksen kannalta relevanteista hakuehdoista. Hakuehtojen luokan käyttöön voitaisiin hakea tuomioistuimelta lupa silloin, kun samaan riittävän 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 uu-

si lupamenettely hakuehtojen hyväksymiseksi, voisi tuomioistuimen lupa koskea hakuehdoista muodostuvan joukon sanallista kuvausta, jolloin uuden tiedon perusteella luotavat uudet yksittäiset hakuehdot kuuluisivat aiemmin haetun luvan piiriin.

Ruotsin signaalitiedustelulain 5 a §:ssä ja Sveitsin tiedustelulain 40 §:ssä säädetään hakuehtojen luokkien hyväksymisestä tietoliikennetiedustelun perustaksi vastaavalla tavalla kuin mitä tässä esitetään.

Hakuehtojen luokkana voisi olla esimerkiksi jonkin lupavaatimuksessa yksilöitävän henkilöryhmän viestiyhteyksien kuvaus. Ryhmään kuuluvia henkilöitä yhdistävänä tekijänä voisi olla esimerkiksi jäsenyys tietyssä terroristiryhmässä taikka toiminen tietyssä työtehtävässä sellaisessa vierasta valtiota edustavassa organisaatiossa, jonka toiminta uhkaa vakavasti Suomen kansallista turvallisuutta. Kun tietoliikennetiedustelun avulla saataisiin tietoon ryhmään kuuluvien henkilöiden käyttämiä teleosoiteavaruuksia ja muita ulkomaisia teleosoitteita, niitä voitaisiin käyttää hakuehtoina. Jotta henkilöryhmän viestiyhteydet voisivat tulla hyväksytyksi hakuehtojen luokkana, edellytettäisiin, että ryhmän jäsenyyden perusteet olisi määritelty vaatimuksessa riittävän tarkasti, ryhmän olisi osoitettu muodostavan vakavan uhkan kansalliselle turvallisuudelle ja vaatimus muutenkin täyttäisi tietoliikennetiedustelun edellytykset.

Hakuehtojen luokkana voisivat tulla kyseeseen myös tietoliikenneyhteydet tietyn hakemuksessa yksilöidyn riittävän suppean maantieteellisen alueen ja Suomen välillä. Kyseinen maantieteellinen alue voisi olla esimerkiksi tietyn terroristiryhmän komentopaikka, josta sen tiedetään ohjaavan Suomessa olevia jäseniään. Jotta tiettyyn maantieteelliseen alueeseen liittyvät viestiyhteydet voisivat tulla hyväksytyksi hakuehtojen luokkana, olisi tiedusteluviranomaisen kyettävä osoittamaan kyseisen alueen merkitys kansallista turvallisuutta vakavasti uhkaavan toiminnan 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 uhkan kannalta sivulliseen tietoliikenteeseen.

Edelleen hakuehtojen luokkina voisivat tulla kyseeseen esimerkiksi haittaohjelmakoodit, joita tietyn vieraan valtion tietty tiedustelupalvelu käyttää kybervakoilussaan, tai verkko-osoitteet, joita kyseinen tiedustelupalvelu käyttää kybervakoilunsa välikappaleena. Jos haittaohjelmakoodit tai verkko-osoitteet yksilöitäisiin vaatimuksessa, olisi niissä kyse hakuehdoista eikä niiden luokista. Tarve hakea lupaa kybervakoilussa käytettäviin haittaohjelmakoodeihin ja verkko-osoitteisiin hakuehtojen luokkina 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 tuomioistuin 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 tiedusteluviranomaiselle annettaisiin rajattu oikeus muotoilla tietoliikennetiedustelussa käytettävät konkreettiset hakuehdot itse, olisi tähän toimintaan tarve kohdistaa erityisen tarkkaa valvontaa. Valvonnan kohteena olisi se, että konkreettisten hakuehtojen määrittäminen tapahtuu tuomioistuimen päätöksessään hyväksymän hakuehtojen luokan puitteissa. Valvontaa koskeva sääntely esitetään otettavaksi lakiin tiedustelutoiminnan valvonnasta (/).

Lupavaatimuksessa ja päätöksessä olisi mainittava myös perustelut tietoliikennetiedustelussa käytettäville hakuehdoille tai hakuehtojen luokille. Hakuehdot olisivat, kuten edellä 4 §:n perusteluista käy ilmi, pääsääntöisesti teknisiä tietoja, joiden liityntä tietoliikennetiedustelun kohteena olevaan kansallista turvallisuutta vakavasti uhkaavaan toimintaan ei välttämättä näytä ilmeiseltä. Vaatimuksen esittäjän tulisi näin ollen perustella tuomioistuimelle, mikä on hakuehdon ja kansallista turvallisuutta vakavasti vaarantavan toiminnan 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 tiedusteluviranomaisen tehdä selkoa siitä, millä perusteilla ja minkälaista kansallista turvallisuutta vakavasti vaarantavaan toimintaan liittyvää tietoliikennettä oletetaan liikkuvan kyseisessä osoiteavaruudessa. Jos vaatimus koskisi hakuehtojen luokkaa, tulisi tiedusteluviranomaisen perustella se, mikä on valitun hakuehtojen luokan ja tietoliikennetiedustelulla selvitettävän kansallista turvallisuutta 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 lupavaatimuksessa ja päätöksessä olisi mainittava se viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja käytetään, sekä perustelut viestintäverkon osan valinnalle. Hakuehtoja ei saataisi käyttää koko rajan ylittävässä viestintäverkossa liikkuvaan tietoliikenteeseen, vaan niiden käyttö tulisi rajata niin suppeaan tietoliikennevirtaan kuin kussakin tapauksessa on välttämätöntä. Siviilitiedusteluviranomaisen velvollisuutena olisi lupavaatimuksessaan määritellä mahdollisimman täsmällisesti se rajan ylittävän viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja verrattaisiin. Vaatimuksessa ja päätöksessä edellytetty tieto viestintäverkon osasta selvitettäisiin tapauksesta riippuen joko sotilastiedustelulain 66 §:ssä säädettäväksi ehdotetulla viestinnän teknisten tietojen käsittelyä koskevan toimivaltuuden avulla tai tämän lain 22 §:ssä tiedonsiirtäjille säädettäväksi ehdotetun tietojenantovelvollisuuden avulla. Yleisimmin viestintäverkon osan selvittämisessä käytettäisiin edellä mainittujen selvittämiskeinojen yhdistelmää.

Sotilastiedustelulain 66 §:ssä säädettäväksi ehdotettu viestinnän teknisten tietojen käsittely olisi ensisijaisesti tarkoitettu menetelmäksi selvittää suhteellisen staattisten tietoliikennevirtojen reitittyminen rajan ylittävässä viestintäverkossa. Sen mahdollistamiseksi, että myös siviilitiedustelussa voidaan käyttää hyväksi kyseisen säännöksen mukaista toimintaa, otettaisiin tämän lain 10 §:n 2 momentiksi säännös, jonka mukaan suojelupoliisi saa antaa puolustusvoimien tiedustelulaitokselle toimeksiantoja viestinnän teknisten tietojen käsittelemiseksi. Sotilastiedustelulain 67 §:n mukaisen luvan viestinnän teknisten tietojen käsittelemiseksi tuomioistuimesta hakisi tuolloin suojelupoliisinkin puolesta puolustusvoimien tiedustelulaitos.

Tämän lain 22 §:ssä säädettäväksi ehdotetun tiedonsiirtäjän tietojenantovelvollisuuden puitteissa saatavat tiedot olisivat puolestaan tarpeen erityisesti sen selvittämiseksi, missä viestin-

täverkon osassa muun kuin staattisen tietoliikenteen voidaan olettaa ylittävän Suomen raja. Pykälä velvoittaisi tiedonsiirtäjän antamaan suojelupoliisin yksilöidystä pyynnöstä sellaiset hallussaan olevat tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi tietoliikennetiedustelun lupavaatimusta ja -päätöstä varten. Koska tiedonsiirtäjien tiedot siitä, minkälaista tietoliikennettä niiden omistamissa tai hallitsemissa rajat ylittävissä viestintäverkoissa kulkee, ovat verrattain ylimalkaiset, voi tapauskohtaisesti olla, että lupavaatimuksessa pystytään vain sulkemaan pois sellaiset viestintäverkon osat, joissa vaatimuksen perusteena olevaan kansallista turvallisuutta vakavasti uhkaavaan toimintaan liittyvän tietoliikenteen ei ainakaan voida olettaa kulkevan. Vaatimus voisi tästä johtuen koskea verrattain laajaakin viestintäverkon osaa.

Kahden edellä mainitun menetelmän erityisistä käyttöaloista huolimatta viestintäverkon osan selvittämisessä käytettäisiin käytännössä useimmin niiden yhdistelmää. Staattisen tietoliikenteen rajan yli reitittymistä selvitettäessä tiedonsiirtäjiltä saatavat tiedot olisivat alkutilanteessa välttämättömiä, jotta sotilastiedustelulain 66 §:ssä tarkoitettua toimivaltuutta voitaisiin käyttää mahdollisimman kohdennetusti ja rationaalisesti. Muun kuin staattisen tietoliikenteen reitittymistä selvitettäessä ne tiedot, jotka olisi saatu tiedonsiirtäjältä, olisi voitava todentaa sotilastiedustelulain 66 §:ssä tarkoitetun toiminnan avulla. Lisäksi tämä toiminta voisi tuottaa sellaista uutta poissulkevaa tietoa, jota tiedonsiirtäjällä ei ollut hallussaan. Poissulkevan tiedon käyttö mahdollistaisi sen, että tietoliikennetiedustelun hakuehtoja ei käytettäisi laajemmassa osassa rajan ylittävää viestintäverkkoa liikkuvaan tietoliikenteeseen kuin on välttämätöntä.

Vaatimuksessa ja päätöksessä olisi mainittava perustelut sille viestintäverkon osalle, jossa liikkuvaan tietoliikenteeseen hakuehtoja on tarkoitus käyttää. Siviilitiedusteluviranomaisen edellytettäisiin näin ollen tekevän vaatimuksessaan selkoa siitä, miksi ja millä perusteilla kansallista turvallisuutta vakavasti uhkaavaan toimintaan liittyvän tietoliikenteen voidaan olettaa kulkevan siinä tietoverkon osassa, jota vaatimus koskee.

Momentin 6 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella. Kohdan perusteluiden osalta viitataan poliisilain 5 a luvun 6 §:n 4 kohdan perusteluihin.

Momentin 7 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava tietoliikennetiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Kohdan perusteluiden osalta viitataan poliisilain 5 a luvun 6 §:n 5 kohdan perusteluihin.

Momentin 8 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava mahdolliset tietoliikennetiedustelun käytölle asetettavat rajoitukset ja ehdot. Jos tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, ne olisi syytä kirjata jo siihen. Rajoituksia ja ehtoja voitaisiin asettaa esimerkiksi sille, kuinka tiedusteluviranomainen saa muodostaa hakuehtoja niiden hakuehtojen luokkien puitteissa, joihin tuomioistuin myöntää luvan.

Pykälän 3 momentissa säädettäisiin tietoliikennetiedustelua koskevan luvan enimmäisvoimassaoloajasta. Tietoliikennetiedustelua koskevan luvan enimmäisvoimassaoloaika olisi kuusi kuukautta. Vastaavasta enimmäisvoimassaoloajasta säädetään Ruotsin signaalitiedustelulain 5 a §:ssä ja Sveitsin tiedustelulain 40 §:ssä. Tietoliikennetiedustelua koskevan luvan enimmäisvoimassaoloaika olisi myös sama kuin poliisilain 5 a luvussa säänneltyjä tiedustelumenetelmiä koskevien lupien ja päätösten. Säännöksessä ehdotettu kuuden kuukauden lupa-aika ei automaattisesti tarkoittaisi sitä, että lupa voitaisiin aina hakea kuudeksi kuukaudeksi tai että se tulisi myöntää kuuden kuukauden määräajaksi. Suhteellisuus- ja vähimmän haitan periaatteen mukaista harkintaa edellyttäisi säännöksessä oleva ilmaisu "enintään kuudeksi kuukaudeksi

kerrallaan". Siksi lupaa hakiessa sekä sitä myönnettäessä tulisi harkita tietoliikennetiedustelun käytön ajallisen keston tarpeellisuutta tapauskohtaisesti.

Pykälän 4 momentin mukaan tietoliikennetiedustelu olisi lopetettava ennen luvassa mainitun määräajan päättymistä, jos tietoliikennetiedustelun tarkoitus on saavutettu tai sen edellytyksiä ei enää ole. Säännöksellä korostettaisiin sitä, ettei tietoliikennetiedustelua missään olosuhteissa saisi käyttää kauemmin kuin on tarpeen, vaikka tuomioistuimen myöntämä lupa sinänsä olisikin vielä voimassa.

8 §. *Menettely tuomioistuimessa.* Pykälän mukaan tietoliikennetiedustelua koskevan lupa-asian käsittelemisessä ja ratkaisemisessa tuomioistuimessa noudatettaisiin, mitä poliisilain 5 a luvun 35 §:ssä säädetään tiedustelumenetelmää koskevan lupa-asian käsittelemisestä.

Pykälän perusteluiden osalta viitataan poliisilain 5 a luvun edellä mainitun pykälän perusteluihin.

9 §. *Kiiretilanteen päätösmenettely.* Pykälässä säädettäisiin tietoliikennetiedustelua koskevasta poikkeuksellisesta kiiretilanteen päätösmenettelystä, jossa päätöksen tietoliikennetiedustelun aloittamisesta tekisi suojelupoliisin päällikkö. Asia olisi saatettava tuomioistuimen ratkaistavaksi heti kun se on mahdollista, kuitenkin viimeistään 24 tuntia tietoliikennetiedustelun alkamisesta. Tietoliikennetiedustelu olisi lopetettava välittömästi, jos tuomioistuin asian ratkaistessaan katsoo, etteivät tietoliikennetiedustelulle 4 §:ssä säädettäväksi ehdotetut edellytykset täyttyneet.

Ehdotettava pykälä on muotoiltu käyttäen pääasiallisina esikuvina poliisilain 5 luvun 10 §:n 2 momentin ja 12 §:n 1 momentin sekä pakkokeinolain 10 luvun 9 §:n 1 momentin ja 11 §:n 1 momentin säännöksiä, joiden mukaan pidättämiseen oikeutettu virkamies voi kiiretapauksissa päättää väliaikaisesti televalvonnasta ja tukiasematietojen hankkimisesta siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Tietoliikennetiedustelun osalta vastaavankaltaisesta kiiretilanteen päätösmenettelystä säädetään Ruotsin signaalitiedustelulain 5 b §:ssä. Edellä mainituista poliisi- ja pakkokeinolain säännöksistä poiketen ehdotetaan, että toimivalta tehdä tietoliikennetiedustelua koskeva väliaikainen kiirepäätös kuuluisi suojelupoliisin organisaatiossa yksin suojelupoliisin päällikölle.

Yleisperusteluista ilmenevällä tavalla Euroopan ihmisoikeustuomioistuin on ratkaisukäytännössään katsonut, että erityissäännökset kiiretilanteiden päätöksentekomenettelystä voivat olla hyväksyttäviä, jos kansallisesta laista selvästi ilmenee, että sellaista päätöksentekomenettelyä voidaan käyttää vain poikkeuksellisissa tapauksissa ja välttämättömien syiden ollessa käsillä. Poliisi- ja pakkokeinolakien sekä Ruotsin signaalitiedustelulain edellä viitattujen säännösten tavoin kiiremenettelyn käytön edellytykseksi ehdotetaan asetettavan, että tietoliikennetiedustelua koskeva asia ei siedä viivytystä. Tarve tietoliikennetiedustelun käyttämiseen voi joskus syntyä niin nopeasti, että luvan hakemisesta 7 §:n mukaisessa menettelyssä aiheutuva viivästys vakavasti vaarantaisi kansallisen turvallisuuden. Kyse voi olla esimerkiksi kansainväliseen terrorismiin liittyvästä välittömästä ja vakavasta uhkatilanteesta. Kiiremenettelyn käytön edellytys täyttyisi myös silloin, kun välitöntä uhkatilannetta ei sinänsä ole, mutta luvan hakemisesta aiheutuva viivästys johtaisi tietoliikennetiedustelulla saatavissa olevan aineiston peruuttamattomaan menetykseen. Tietoliikennetiedustelun monivaiheisuudesta johtuen voidaan arvioida, että kiiremenettelyn käytön edellytykset täyttyisivät sen osalta selvästi harvemmin kuin esimerkiksi televalvonnan osalta. Tietoliikenteen automatisoidussa erottelussa käytettävien hakuehtojen muotoilu esimerkiksi on siinä määrin aikaa vievä prosessi, että lupa tietoliikennetiedusteluun yleensä olisi mahdollista hakea tuomioistuimelta ennen kuin hakuehdot sisältävä

kiirepäätös olisi valmis toimitettavaksi päätöksen teknisestä toteuttamisesta vastaavalle viranomaiselle.

Tietoliikennetiedustelua koskeva kiirepäätös olisi tehtävä kirjallisesti. Vaatimuksella varmistettaisiin se, että tuomioistuin myöhemmin asiaa käsitellessään voisi todeta, täyttyivätkö tietoliikennetiedustelulle asetetut edellytykset sinä ajankohtana, kun kiirepäätös tehtiin. Kiirepäätöksen kirjallista muotoa koskevalla vaatimuksella taattaisiin samoin se, että päätökseen ja sen teko-olosuhteisiin voitaisiin kohdistaa riittävän tehokasta jälkikäteisestä laillisuusvalvontaa. Vaatimus kirjallisesta muodosta koskisi jokaista niistä 9 kohdasta, jotka sisältyisivät 7 §:n 2 momenttiin.

Tietoliikennetiedustelua koskeva asia olisi saatettava tuomioistuimen ratkaistavaksi heti kun se on mahdollista, kuitenkin viimeistään 24 tuntia tietoliikennetiedustelun alkamisesta. Asia tulisi saattaa tuomioistuimen käsiteltäväksi siitä huolimatta, että tietoliikennetiedustelun käyttö lopetetaan 24 tunnin kuluessa sen käytön aloittamisesta. Muuten hyvin lyhytaikaisella tiedonhankinnalla voitaisiin kiertää päätöksentekomenettelylle asetettaviksi ehdotettuja vaatimuksia ja 2 momentissa säädettäväksi ehdotettua tietojen hävittämisvelvollisuutta.

Pykälän 2 momentissa säädettäisiin tuomioistuimen ratkaisun vaikutuksista silloin kun tuomioistuin toteaisi, että 1 momentin mukaisessa menettelyssä päätetyn tietoliikennetiedustelun edellytykset kokonaan tai osittain puuttuivat.

Momentin ensimmäisen virkkeen mukaan tietoliikennetiedustelu olisi välittömästi lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä, jos tuomioistuin katsoo, että 4 §:n mukaisia edellytyksiä tietoliikennetiedustelulle ei ole ollut. Viitatussa pykälässä ehdotetaan säädettäväksi tietoliikennetiedustelulle asetettavista tuloksellisuus- ja välttämättömyysedellytyksistä. Jos tuomioistuin katsoisi, että kiiremenettelyä noudattaen tehty päätös ei ole täyttänyt tietoliikennetiedustelun edellytyksiä, voidaan kiirepäätös katsoa siinä määrin perustavanlaatuisella tavalla virheelliseksi, että tietoliikennetiedustelun käyttö kokonaisuudessaan on lopetettava ja sillä saatu aineisto ja tehdyt muistiinpanot koko laajuudessaan hävitettävä.

Momentin toisessa virkkeessä sääntelyn kohteena olisivat tilanteet, joissa tuomioistuin muusta syystä kuin 4 §:ssä tarkoitettujen edellytysten puuttumisen johdosta katsoo kiirepäätöksen virheelliseksi. Muu virheellisyys voi joissain tilanteissa olla laadultaan niin vakava, että se rinnastuisi 4 §:ssä tarkoitettujen edellytysten puuttumiseen, mutta toisissa tilanteissa taas sillä tavoin lievää tai osittaista, että tietoliikennetiedustelun kokonaan lopettamista voitaisiin pitää kohtuuttomana. Ehdotetussa sääntelyssä on pyritty huomioimaan se, että kiirepäätösmenettely käytännössä tulisi kyseeseen erityisen vakavissa tilanteissa tiedon saamiseksi välittömästi uhkaavista vaaroista, ja että tällaisissa tilanteissa tehtyihin päätöksiin saattaa sisältyä vähäisempiä virheitä.

Jos tietoliikennetiedustelun käyttöä koskeva kiirepäätös olisi vakavasti virheellinen esimerkiksi sen vuoksi, että tietoliikennetiedustelun kohteena ollut toiminta ei vastaa mitään 3 §:ssä säädettäväksi ehdotettua toimintaa tai tästä toiminnasta tiedossa olevat konkreettiset tosiseikat ovat riittämättömät tietoliikennetiedustelua koskevan päätöksen tekemiseksi, rinnastuisi virheen vakavuus siihen, että tietoliikennetiedustelulle 4 §:ssä säädetyt edellytykset ovat puuttuneet. Tällöin tietoliikennetiedustelu olisi tuomioistuimen päätöksen mukaisesti kokonaan lopetettava ja sillä saatu aineisto ja tehdyt muistiinpanot koko laajuudessaan hävitettävä. Osittaiseksi virheellisyydeksi voitaisiin katsoa esimerkiksi se, että jokin tai jotkin kiirepäätöksessä mainituista hakuehdoista eivät olisi olleet riittävän tarkkoja tai riittävästi vastanneet tiedonhankinnan kohteena olevaa uhkaavaa toimintaa, vaikka toiset hakuehdot ovatkin olleet moit-

teettomia. Jos tuomioistuin ratkaisisi asian tällä tavalla, olisi virheellisten hakuehtojen käyttö välittömästi lopetettava sekä niiden käytön avulla saatu aineisto ja käytön johdosta tehdyt muistiinpanot viipymättä hävitettävä. Muilta osin tietoliikennetiedustelu voisi tuomioistuimen ratkaisun sallimassa laajuudessa jatkua ja sillä saadut tiedot saataisiin säilyttää. Tietoliikennetiedustelun osittaista lopettamista ja sillä saatujen tietojen vastaavanlaajuista hävittämistä koskeva tilanne voisi olla käsillä myös silloin, kun tietoliikennetiedustelun käyttöä koskevassa kiirepäätöksessä mainitut viestintäverkon osat, joihin tietoliikennetiedustelu kohdistetaan, on yksilöity joiltain osin oikein ja toisilta osin väärin.

Momentin kolmannen virkkeen mukaan tuomioistuimen kumoamalla kiirepäätöksellä saatu tieto saataisiin kuitenkin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin poliisilain 5 a luvun 45 §:n 1 momentissa säädetyin edellytyksin. Tieto olisi viitatun säännöksen mukaan hävitettävä viipymättä sen jälkeen, kun olisi käynyt ilmi, ettei sitä tarvita näihin tarkoituksiin. Mainittuun poliisilain 5 a luvun 45 §:n 2 momentin säännöksessä viitattaisiin myös poliisilain 5 a luvun 46 §:ään, joka koskisi kyseisen luvun mukaisten tiedustelumenetelmien käytöllä kiiretilanteessa saadun tiedon hävittämistä. Edellytykset väärällä kiirepäätöksellä saadun tiedon käytölle olisivat näin ollen samat yhtäältä silloin, kun tieto on saatu tietoliikennetiedustelulla, ja toisaalta silloin, kun tieto on saatu poliisilain 5 a luvussa tarkoitetuilla tiedustelumenetelmillä.

10 §. *Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa.* Pykälässä säädettäisiin tietoliikennetiedustelun teknisestä toteuttamisesta. Tietoliikennetiedustelun tekninen toteuttaminen tapahtuisi suojelupoliisin toimeksiannosta ja puolustusvoimien tiedustelulaitoksen toimesta. Tekninen toteuttaminen pitäisi sisällään yhtäältä sotilastiedustelulain 66 §:n mukaiset toimenpiteet, joihin puolustusvoimien tiedustelulaitos hakisi suojelupoliisin puolesta luvan, ja toisaalta tämän lain 5 §:n mukaiset toimenpiteet, joihin luvan tuomioistuimelta hakisi suojelupoliisi tai joista suojelupoliisin päällikkö poikkeuksellisessa kiiretilanteessa voisi tehdä väliaikaisen päätöksen. Tekniseen toteuttamiseen kuuluisi myös se, että puolustusvoimien tiedustelulaitos toimittaisi toimeksiannon johdosta hankkimansa tiedot toimeksiantajana olevalle suojelupoliisille.

Pykälän 1 momentin mukaan tietoliikennetiedustelun teknisenä toteuttajana toimisi puolustusvoimien tiedustelulaitos. Puolustusvoimien tiedustelulaitoksen osoittaminen tekniseksi toteuttajaksi perustuisi tiedonhankintalakityöryhmän esitykseen. Tiedonhankintalakityöryhmän loppumietinnössä todetun mukaisesti ei olisi tarkoituksenmukaista, että tiedustelutietoa tarvitsevat viranomaiset harjoittaisivat tietoliikennetiedustelua kukin erikseen, vaan toiminnan yhdenmukaisuudelle ja salassa pidettävyydelle asetetut vaatimukset, toiminnan edellyttämä erikoistuminen ja tekninen osaaminen sekä toiminnan lainmukaisuuden valvontaan liittyvät näkökohdat perustelisivat sitä, että yksi viranomainen toteuttaa tietoliikennetiedustelun teknisesti kaikkien viranomaisten puolesta.

Pykälän 2 momentissa säädettäisiin niin sanottuun teknisten tietojen käsittelyyn liittyvästä toimeksiantomenettelystä. Teknisten tietojen käsittely olisi menetelmä, jonka avulla voitaisiin selvittää tuomioistuimelle myöhemmin esitettävää tietoliikennetiedustelun lupavaatimusta varten se viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja olisi tarpeen käyttää. Teknisten tietojen käsittelystä säädettäisiin sotilastiedustelulain 66 §:ssä ja sitä koskevasta lupamenettelystä sotilastiedustelulain 67 §:ssä. Ensin mainitun säännöksen 1 momentin mukaan puolustusvoimien tiedustelulaitos saisi viestintäverkon tietoliikenteestä hetkellisesti kerätä ja tallentaa viestinnän teknisiä tietoja sekä automaattisen tietojenkäsittelyn avulla käsitellä niitä tilastollista analyysiä varten. Tässä tilastollisessa analysoinnissa selvitettäisiin se, missä osassa viestintäverkkoa uhkaavaan toimintaan liittyvä tietoliikenne todennäköisimmin liikkuu. Sotilastiedustelulain 67 §:n mukaan teknisten tietojen käsittelystä päättäisi tuomioistuin puolus-

tusvoimien tiedustelulaitoksen tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti koulutetun virkamiehen vaatimuksesta. Pykälässä säädettäisiin myös niistä tiedoista, joiden on käytävä ilmi tuomioistuimelle esitettävästä vaatimuksesta ja tuomioistuimen päätöksestä.

Toimeksiantomenettelyllä mahdollistettaisiin se, että viestintäverkon osan selvittämiseksi tarpeellista sotilastiedustelulain toimivaltuutta voitaisiin hyödyntää myös siviilitiedustelun hyväksi. Säännöksen mukaan suojelupoliisi voisi antaa puolustusvoimien tiedustelulaitokselle teknisten tietojen käsittelyä koskevan toimeksiannon, minkä jälkeen puolustusvoimien tiedustelulaitos hakisi sanottuun toimenpiteeseen tuomioistuimelta luvan. Saatuaan tuomioistuimelta luvan ja toteutettuaan luvan mukaiset toimenpiteet, puolustusvoimien tiedustelulaitos toimittaisi tilastollisen analyysinsa tuloksen suojelupoliisin käyttöön.

Teknisten tietojen käsittelyä koskevan toimeksiannon antamisen yhteydessä suojelupoliisin tulisi toimittaa puolustusvoimien tiedustelulaitokselle tiedot, jotka ovat tarpeen toimeksiannon mahdollisimman kohdennettua ja rationaalista toteuttamista varten. Tällaisia tietoja olisivat muun muassa alustava kuvaus niistä hakuehdoista, joita myöhemmässä tietoliikennetiedustelussa olisi tarkoitus käyttää, sekä tieto siitä maantieteellisestä alueesta, josta tietoliikennetiedustelulla selvitettävään toimintaan liittyvä tietoliikenne on lähtöisin. Lisäksi suojelupoliisin tulisi toimittaa puolustusvoimien tiedustelulaitokselle sellaiset asian kannalta olennaiset tiedot, jotka se olisi saanut tiedonsiirtäjältä tai -siirtäjiltä näille 22 §:ssä säädettäväksi ehdotetun tietojenantovelvollisuuden nojalla. Tällaisilla tiedonsiirtäjiltä saaduilla tiedoilla olisi poissulkeva merkitys, sillä niiden avulla teknisten tietojen käsittelyyn kuuluva hetkellinen näytteenotto voitaisiin rajata koskemaan vain sitä osaa viestintäverkosta, jossa tietoliikennetiedustelun kannalta olennainen tietoliikenne voi liikkua. Sotilastiedustelulain 67 §:n 2 momentin mukaan teknisten tietojen käsittelyä koskevasta tuomioistuimelle esitettävästä lupavaatimuksesta olisi käytävä ilmi ne viestintäverkon osat, joista teknisiä tietoja on määrä hetkellisesti kerätä.

Sotilastiedustelulain 67 §:n tarkoittaman luvan teknisten tietojen käsittelyyn hakisi suojelupoliisin puolesta puolustusvoimien tiedustelulaitos. Syynä ehdotettuun menettelyyn on se, että säännöksen 2 momentin mukaan lupavaatimuksesta tulisi käydä ilmi eräitä sellaisia teknisten tietojen käsittelyn organisointiin ja toteuttamiseen liittyviä tietoja, joista paras tieto on juuri puolustusvoimien tiedustelulaitoksella. Tällaisia olisivat lupavaatimuksessa esitettävät tieto toimintaa johtavasta sotilastiedustelun virkamiehestä sekä suunnitelma siitä, miten vaatimuksen kohteena oleva toiminta on määrä sotilastiedusteluviranomaisen toimesta toteuttaa.

Toteutettuaan tuomioistuimen luvan mukaisen teknisten tietojen käsittelyn suojelupoliisin puolesta, puolustusvoimien tiedustelulaitos toimittaisi käsittelyn puitteissa laatimansa tilastollisen analyysin tuloksen suojelupoliisin käyttöön. Tilastollisen analyysin tulos kertoisi sen, mihin viestintäverkon osaan suojelupoliisin tulisi seuraavassa vaiheessa hakea tämän lain 7 §:n mukaista lupaa tietoliikennetiedusteluun.

Pykälän 3 momentin ensimmäisen virkkeen mukaan suojelupoliisi toimittaisi 7 tai 9 §:ssä tarkoitetun tietoliikennetiedustelun käyttöä koskevan päätöksen puolustusvoimien tiedustelulaitokselle, joka suorittaisi 5 §:n mukaiset toimenpiteet suojelupoliisin puolesta. Viitatussa 5 §:ssä ehdotetaan säädettäväksi tietoliikennetiedustelun kohdistamisesta, jonka teknisluontoinen suorittaminen näin ollen olisi puolustusvoimien tiedustelulaitoksen tehtävä. Käytännössä kohdistaminen suoritettaisiin siten, että puolustusvoimien tiedustelulaitos syöttäisi tietoliikennetiedustelussa käytettävään tekniseen järjestelmään tuomioistuimen lupapäätöksen tai suojelupoliisin päällikön kiirepäätöksen mukaiset hakuehdot. Konkreettiset hakuehdot eivät kuitenkaan kaikissa tapauksissa ilmenisi päätöksestä, sillä ehdotetun 7 §:n 3 momentin 4 kohdan mukaan päätöksessä voitaisiin hakuehtojen käytön ohella tai sijasta hyväksyä myös hakuehto-

jen luokkien käyttö. Tietoliikennetiedustelun tekninen toteuttaminen ei pitäisi sisällään oikeutta kehittää ja täsmentää hakuehtoja päätöksessä hyväksyttyjen hakuehtojen luokkien puitteissa, vaan hakuehtojen konkretisointi olisi yksin toimeksiantajan eli suojelupoliisin tehtävä. Tekninen toteuttaja ei näin ollen olisi myöskään oikeudellisessa vastuussa siitä, että hakuehdot on muodostettu oikein, vaan ainoastaan siitä, että ne on syötetty tietoliikenteen suodattamisessa käytettävään tekniseen järjestelmään toimeksiannon mukaisesti.

Puolustusvoimien tiedustelulaitoksen suorittamassa automatisoidussa suodatuksessa muusta tietoliikenteestä eroteltaisiin hakuehtoja vastaava ja siten selvitettävänä olevan uhan kannalta lähtökohtaisesti merkityksellinen tietoliikenteen osa. Puolustusvoimien tiedustelulaitos ottaisi tietoliikenteen tämän osan haltuunsa sen suojelupoliisille toimittamista varten. Puolustusvoimien tiedustelulaitoksella ei olisi teknisen toteuttamisen puitteissa oikeutta käsitellä haltuun otettua tietoliikennettä automaattisesti tai manuaalisesti siten kuin 6 §:ssä ehdotetaan säädettävän, vaan oikeus toimeksiannon johdosta haltuun otetun tietoliikenteen jatkokäsittelyyn olisi ainoastaan toimeksiantajalla. Teknisen toteuttamisen puhtaasti teknistä luonnetta ilmentäisi osaltaan myös sotilastiedustelulain ehdotetun 73 §:n 3 momentti, jonka mukaan puolustusvoimien tiedustelulaitos ei saisi tietoliikennetiedustelun teknisessä toteuttamisessa selvittää viestin sisältöä.

Momentin jälkimmäisen virkkeen mukaan puolustusvoimien tiedustelulaitos toimittaisi toimeksiannon toteuttamisella keräämänsä tiedot toimeksiantajalle eli suojelupoliisille. Tietoliikennetiedustelun teknisellä toteuttamisella kerättyjen tietojen haltuunotto olisi väliaikainen toimi, jonka tarkoituksena olisi ainoastaan mahdollistaa niiden toimittaminen tietojen käsittelystä vastaavalle viranomaiselle. Puolustusvoimien tiedustelulaitoksella ei olisi oikeutta muuten kuin väliaikaisesti tallentaa näitä tietoja, jotka siten poistuisivat sen tietojärjestelmistä niiden suojelupoliisille toimittamisen myötä. Momentissa ei otettaisi kantaa siihen, millä konkreettisella tavalla puolustusvoimien tiedustelulaitos toimittaisi tiedot suojelupoliisille. Pääsääntöisesti toimittaminen tapahtuisi salatun tiedonsiirtoyhteyden avulla, mutta säännös sallisi myös sen, että tiedot toimitetaan muulla riittävän tietoturvallisella tavalla.

Pykälän 4 momentin mukaan suojelupoliisin muuhun yhteistyöhön sotilastiedusteluviranomaisen kanssa sovellettaisiin poliisilain 5 a luvun 54 §:ää. Muulla yhteistyöllä tarkoitettaisiin muuta tietoliikennetiedusteluun liittyvää yhteistyötä kuin 1-3 momenteissa säänneltäväksi ehdotettua suojelupoliisin toimeksiannosta tapahtuvaa puolustusvoimien tiedustelulaitoksen suorittamaa tietoliikennetiedustelun teknistä toteuttamista. Koska tässä momentissa mainittaisiin 1-3 momenteista poiketen yhteistyötahona sotilastiedusteluviranomainen, olisi momentin tarkoittamaa yhteistyötä mahdollista tehdä muunkin sotilastiedusteluviranomaisen kuin puolustusvoimien tiedustelulaitoksen kanssa. Sotilastiedustelulain ehdotetun 8 §:n mukaan sotilastiedusteluviranomaisia olisivat pääesikunta ja puolustusvoimien tiedustelulaitos.

Momentissa viitatun poliisilain 5 a luvun ehdotetun 54 §:n 1 momentin mukaan suojelupoliisin olisi toimittava yhteistyössä sotilastiedusteluviranomaisen kanssa tiedustelun tarkoituksenmukaiseksi hoitamiseksi sekä annettava sotilastiedusteluviranomaiselle tässä tarkoituksessa tarpeellisia tietoja sen estämättä mitä salassapitovelvollisuudesta säädetään. Pykälän 2 momentin mukaan valtioneuvoston asetuksella voitaisiin antaa tarkempia säännöksiä suojelupoliisin ja sotilastiedusteluviranomaisen välisestä yhteistyöstä.

Koska nyt kyseessä olevan momentin sisältö muodostuisi viittauksesta poliisilain 5 a luvun edellä mainittuun pykälään, viitataan momentin perusteluiden osalta yllä sanotun lisäksi poliisilain kyseisen pykälän perusteluihin.

11 §. *Määräaikojen laskeminen.* Pykälässä säädettäisiin laissa tarkoitettujen määräaikojen laskemisesta.

Koska pykälä asiallisesti vastaisi poliisilain 5 luvun voimassa olevan 49 §:n ja poliisilain ehdotettavan 5 a luvun 40 §:n sääntelyä, viitataan pykälän perusteluiden osalta kyseisten poliisilain pykälien perusteluihin.

12 §. *Tiedustelukielto.* Pykälässä säädettäisiin kiellosta kohdistaa tietoliikennetiedustelua tietyn tyyppisiin viesteihin ja tietoihin.

Pykälän mukainen tiedustelukielto koskisi ensinnäkin sellaisia viestejä, joiden lähettäjä ja vastaanottaja ovat fyysisesti Suomessa sillä hetkellä kun viestintä tapahtuu. Tietoliikennetiedustelu ei olisi keino seurata kotimaisia uhkia, vaan sen tarkoituksena olisi hankkia tietoa kansalliseen turvallisuuteen kohdistuvista vakavista ulkoisista uhkista eli uhkista, joiden alkuperä on Suomen ulkopuolella. Tästä syystä tietoliikennetiedustelu kohdistuisi, 2 §:n määritelmäsäännöksen mukaisesti, ainoastaan sellaiseen tietoliikenteeseen, joka ylittää Suomen rajan viestintäverkossa. Kotimaista viestintää koskevan erikseen säädettävän tiedustelukiellon tarpeellisuus liittyy siihen, ettei se seikka, että tietoliikenne fyysisesti ylittää Suomen rajan, ole tae tietoliikenteen tosiasiallisesti kansainvälisestä luonteesta. Internet on rakennettu siten, että verkon vika- tai ruuhkatilanteissa kotimaisten osapuolten välinen tietoliikenne saattaa reitittyä ulkomaisen verkkolaitteen kautta. Tällöin tietoliikenne näyttää siirtojärjestelmäkerrokselta tarkasteltuna rajat ylittävältä tietoliikenteeltä, vaikka kyse tosiasiallisesti on kotimaisesta tietoliikenteestä. Tiedustelukiellon tarkoituksena olisi varmistaa se, että tietoliikennetiedustelua ei kohdisteta Suomessa viestintätapahtuman hetkellä olleiden osapuolten välisiin viesteihin, jotka teknisten olosuhteiden vuoksi reitittyvät lähettäjältä vastaanottajalle ulkomaan kautta.

Mahdollista sinänsä on, että myös kotimaassa oleskelevien osapuolten välisiin viesteihin sisältyy tiedustelun kannalta merkittävää tietoa kansalliseen turvallisuuteen kohdistuvista vakavista ulkoisista uhkista. Tietoliikennetiedustelun muista tiedustelumenetelmistä poikkeavan luonteen vuoksi sen käyttöalaa kuitenkin olisi tarpeen rajata eri tavoin sen varmistamiseksi, että luottamuksellisen viestin salaisuuteen puuttuminen olisi hyväksyttävää ja mahdollisimman vähäistä. Koska kotimaisella viestinnällä voidaan arvioida olevan aidosti kansainvälistä viestintää vähäisempi merkitys tiedon saamiseksi niistä uhkista, joista ehdotetaan säädettäväksi 3 §:ssä, on perusteltua rajata kotimainen viestintä kokonaan tietoliikennetiedustelun käyttöalan ulkopuolelle. Tiedustelutarkoituksessa tapahtuvan kotimaisten viestien sisällön ja muiden tietojen selvittämisen tulisi tietoliikennetiedustelun sijasta perustua poliisilain 5 a luvussa säädettyihin menetelmiin, muun muassa telekuunteluun ja -valvontaan. Vastaavankaltaisesta kotimaisiin viesteihin kohdistuvasta tiedustelukiellosta säädetään esimerkiksi Ruotsin signaalitiedustelulain 2 a §:ssä ja Sveitsin tiedustelulain 38 §:n 2 momentissa.

Kotimaista viestintää koskevan tiedustelukiellon noudattamisen varmistamiseksi lain 15 §:ässä 1 momentin 1 kohdassa ehdotetaan säädettäväksi velvollisuudesta hävittää tällainen viestintä viipymättä. Hävittämisvelvollisuudesta säätämisen välttämättömyys johtuu siitä, että kotimaisen viestinnän luotettava tunnistaminen ja sen erottaminen aidosti kansainvälisestä viestinnästä ei yleensä ole mahdollista teknisin menetelmin tapahtuvassa tietoliikenteen automatisoidussa erottelussa. Automatisoidussa erottelussa käytettävien hakuehtojen muotoilulla voidaan jossain määrin vähentää todennäköisyyttä, että automaattisesti kerätyn tiedon joukkoon päätyy kotimaisten osapuolten välisiä viestejä. Hakuehtoja ei kuitenkaan ole mahdollista muodostaa siten, että ne kaikissa tapauksissa voisivat tehdä eron aidosti kansainvälisen viestin ja toisaalta sellaisen kotimaisten osapuolten välisen viestin, joka reitittyy ulkomaan kautta, välille. Edellä sanotusta johtuen kotimaista viestintää koskevan tiedustelukiellon olennaisena sisältönä olisi velvollisuus kaikin käytettävissä olevin keinoin estää se, että automatisoidusti

erotellun tietoliikenteen joukkoon päätyy kotimaista viestintää, kielto käyttää tällaista viestintää mitenkään hyväksi sekä velvollisuus hävittää se heti kun sen tosiasiallinen luonne on käynyt ilmi.

Kotimaisia viestejä koskevan tiedustelukiellon ohella pykälässä ehdotetaan säädettäväksi kiellosta kohdistaa tietoliikennetiedustelua tietoon, josta lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 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 tai 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. Oikeudenkäymiskaaren 22 §:n 2 momentin sisältämä viittaus 11 §:n 2 ja 3 momentteihin ei tässä soveltuisi, koska oikeudenkäymiskaaren 11 §:ään liittyvästä nimenomaisesta tiedustelukiellosta ei muutenkaan esitetä säädettäväksi.

Ehdotettavilla oikeudenkäymiskaareen liittyvillä tiedustelukielloilla on yhtymäkohtia, mutta myös merkittäviä eroja poliisilain 5 luvun 50 §:ssä ja pakkokeinolain 10 luvun 52 §:ssä säädettyihin kuuntelu- ja katselukieltoihin. Kyseisten kieltojen mukaan poliisi ei saa kohdistaa tiettyjä tele- ja teknisen tiedonhankinnan keinoja muun muassa rikoksesta epäillyn ja hänen oikeudenkäyntiavustajansa väliseen viestiin, rikoksesta epäillyn ja oikeudenkäymiskaaressa tarkoitetun papin väliseen viestiin, rikoksen johdosta vapautensa menettäneen epäillyn ja lääkärin, sairaanhoitajan, psykologin tai sosiaalityöntekijän väliseen viestiin eikä yleensä myös-

kään rikoksesta epäillyn ja yleisön saataville toimitetun viestin laatijan tai julkaisijan taikka ohjelmatoimittajan väliseen viestiin. Poliisi- ja pakkokeinolakien rikostorjuntamenetelmiin liittyvät kiellot koskevat näin ollen kaikkea tele- tai muuta vastaavaa viestintää rikoksesta epäillyn ja häneen oikeudenkäymiskaaressa tarkoitetussa suhteessa olevan henkilön välillä katsomatta siihen, onko osapuolten välisen yksittäisen viestin sisältö sellainen, että se on oikeudenkäymiskaaren todistamiskieltojen tai oikeuksien olla todistamatta piirissä.

Poliisi- ja pakkokeinolaeissa säännellyistä salaisista tiedonhankinta- ja pakkokeinoista poiketen tietoliikennetiedustelua ei kohdistettaisi rikoksesta epäiltyyn tai oletettuun tulevaan rikoksentekijään. Tietoliikennetiedustelussa tiedustelukiellon alaa ei näin ollen voida tarkoituksenmukaisella tavalla määrittää käyttäen lähtökohtana rikoksesta epäillyn ja oikeudenkäymiskaaressa tarkoitetun ammattihenkilön välistä viestiyhteyttä. Tietoliikennetiedustelussa ei yleensä olisi ylipäätään kyse jonkin tietyn ennakkoon yksilöidyn henkilön viestiyhteyksien seuraamisesta, vaan uhkien tunnistamisesta käyttämällä hakuehtoja tietoliikenteen automatisoidussa erottelussa. Tietoliikennetiedustelun tiedustelukieltoa ei voida määrittää siten, että se koskisi kohdehenkilön yhteyksiä tietyn aseman omaaviin henkilöihin, sillä samanlaista täsmällistä kohdehenkilöä kuin esimerkiksi telekuuntelussa ei monesti olisi edes olemassa. Tästä johtuen ehdotetaan, että tietoliikennetiedustelun tiedustelukielto koskisi ainoastaan niitä nimenomaisia tietoja, joista säännöksessä viitatut ammattihenkilöt ovat oikeudenkäymiskaaren nojalla velvoitettuja tai oikeutettuja olemaan todistamatta.

Oikeudenkäymiskaaressa tarkoitetun ammattihenkilön ja toisen osapuolen välinen yksittäinen viesti voi sisältää sekä todistamiskiellon tai oikeuden olla todistamatta alaisia tietoja että muita tietoja. Tiedustelukielto koskisi edellä sanotun mukaisesti ainoastaan ensiksi mainittuja tietoja. Viestin sisältämiin muihin tietoihin voitaisiin kohdistaa tiedustelua ja ne voitaisiin tallentaa, jos niillä on merkitystä sen uhan selvittämisessä, jota varten tietoliikennetiedusteluun on myönnetty lupa. Jos tiedoilla ei ole merkitystä uhan selvittämisessä, olisi ne hävitettävä. Velvollisuus hävittää epäolennaiset tiedot perustuisi tämän lain 15 §:n 1 momentin 3 kohdan nimenomaiseen säännökseen.

Säännöksessä mainittaisiin tiedon lähettäjän ja vastaanottajan, eli kahden- tai monenvälisen viestinnän osapuolten, ohella erikseen tiedon tallentaja. Tallentajalla viitattaisiin henkilöön, joka tallentaa pilvipalveluun dataa, esimerkiksi asiakirjan. Jos tällaisen pilvipalveluun tallennettavan asiakirjan sisältö kuuluisi jonkin säännöksessä mainitun todistamiskiellon tai oikeuden olla todistamatta piiriin, nauttisi se tiedustelukiellon nojalla suojaa tiedustelulta.

Nyt kyseessä olevan tiedustelukiellon noudattaminen siten, että tietoliikenteestä ei lainkaan kerättäisi kiellon piiriin kuuluvia tietoja, on teknisesti mahdotonta. Tietoliikennetiedustelun ensimmäinen vaihe perustuisi tietoliikenteen automatisoituun erotteluun, jossa käytettäisiin hakuehtoja. Hakuehdot eivät saisi, 4 §:n 2 momentissa säädettäväksi ehdotettavia poikkeuksia lukuun ottamatta, koskea viestin sisältöä. Koska tiedustelukiellon soveltuvuus määräytyisi tiedon sisällön perusteella, voitaisiin tiedon kuuluminen tiedustelukiellon piiriin käytännössä havaita vasta viestin sisällön manuaalisen selvittämisen yhteydessä. Ongelma ei sinänsä ole uusi eikä se liity ainoastaan tietoliikennetiedusteluun. Myöskään poliisi- ja pakkokeinolakien mukaisten kuuntelu- ja katselukieltojen sananmukainen noudattaminen ei ole aina mahdollista, sillä viestin kuuluminen kuuntelukiellon piiriin saattaa käydä ilmi vasta telekuuntelun aikana (pakkokeinolain 10 luvun 52 §:n 2 momentti ja siihen viittaava poliisilain 5 luvun 50 §). Edellä sanotusta johtuen lain 15 §:ssä ehdotetaan säädettäväksi tietojen hävittämisvelvollisuudesta, jolla varmistettaisiin se, että tiedustelukiellon alaisen tiedon käsittely viipymättä lopetettaisiin ja tieto välittömästi hävitettäisiin kun sen luonne tuollaisena tietona on käynyt ilmi.

13 §. *Tallenteiden ja asiakirjojen tarkastaminen.* Pykälän mukaan suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen olisi ilman aiheetonta viivytystä tarkastettava tietoliikennetiedustelun käytössä kertyneet tallenteet ja asiakirjat.

Koska pykälä asiallisesti vastaisi poliisilain 5 luvun voimassa olevan 51 §:n ja ehdotettavaa poliisilain 5 a luvun 42 §:n sääntelyä, viitataan pykälän perusteluiden osalta poliisilain kyseisten pykälien perusteluihin.

14 §. *Tallenteiden tutkiminen.* Pykälän mukaan tietoliikennetiedustelun käytössä kertyneitä tallenteita saisi tutkia vain tuomioistuin ja suojelupoliisin päällystöön kuuluva poliisimies. Suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saisi tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

Koska pykälä asiallisesti vastaisi poliisilain 5 luvun voimassa olevan 52 §:n ja ehdotettavan 5 a luvun 43 §:n sääntelyä, viitataan pykälän perusteluiden osalta poliisilain kyseisten pykälien perusteluihin.

15 §. *Tietojen hävittäminen.* Pykälässä säädettäisiin velvollisuudesta hävittää viipymättä eräät tietoliikennetiedustelun avulla hankitut tiedot. Hävittämisvelvollisuus koskisi yhtäältä 12 §:ssä säädettäväksi ehdotetun tiedustelukiellon piiriin kuuluvia tietoja ja toisaalta tietoja, joita ei tarvita kansallisen turvallisuuden suojaamiseksi. Velvollisuus hävittää tiedustelukiellon alaiset tiedot ja siitä johtuva kielto käyttää niitä millään tavalla hyväksi olisivat ehdottomia eikä niistä olisi lupa poiketa. Velvollisuus hävittää kansallisen turvallisuuden suojaamisen kannalta epäolennaiset tiedot sen sijaan ei olisi ehdoton, vaan siitä olisi mahdollista poiketa pykälässä yksilöidyistä syistä.

Pykälän 1 momentin 1 kohdan mukaan tietoliikennetiedustelulla saatu tieto olisi hävitettävä viipymättä, jos käy ilmi, että viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui. Velvollisuus täydentäisi 12 §:ssä säädettäväksi ehdotettua tiedustelukieltoa. Mainitun pykälän mukaan tietoliikennetiedustelua ei saisi kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa ("kotimainen viesti"). Siltä osin kuin tällaisia tiedustelukiellon alaisia viestejä kuitenkin seuloutuisi käsittelyyn, olisi ne nyt kyseessä olevan säännöksen nojalla hävitettävä viipymättä kun niiden luonne kotimaisina viesteinä on käynyt ilmi.

Hävittämisvelvollisuuden käytännön merkitystä korostaa se, että 12 §:n mukaisen kotimaista viestintää koskevan tiedustelukiellon täydellinen noudattaminen ei ole teknisesti mahdollista. Viesti saattaa reitittyä vastaanottajalleen ulkomaan kautta eli Suomen rajan ylittäen, vaikka sekä viestin lähettäjä että sen vastaanottaja tosiasiassa ovat Suomessa. Tietoliikenteen automatisoidussa erottelussa käytettävien hakuehtojen muotoilulla voidaan jossain määrin vähentää riskiä, että tällaisia kotimaisia viestejä sisältyy kerättyyn aineistoon. Riski ei kuitenkaan yleensä ole kokonaan poistettavissa, mistä johtuen 5 §:ssä tarkoitetun manuaalisenkin käsittelyn kohteeksi voi joutua myös kotimaisia viestejä. Manuaalisessa käsittelyssä viestin kotimainen luonne voi käydä ilmi jo viestin ohjaus- ja välitystietojen tarkastelussa, missä tapauksessa viesti olisi viipymättä hävitettävä sen sisältöä selvittämättä. Joissain tapauksissa viestin kotimainen luonne voidaan havaita vasta sen sisältöä manuaalisesti selvitettäessä, jolloin sisällön selvittäminen olisi välittömästi lopetettava ja viesti viipymättä hävitettävä.

Momentin 2 kohdan mukaan tietoliikennetiedustelulla saatu tieto, josta lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta 12 §:ssä tarkoitetulla tavalla, olisi hävitettävä viipymättä. Hävittämisvelvollisuus koskisi 12 §:n sisältämän viittauksen mukaisesti oikeudenkäymiskaaren 17 luvun 13, 14, 16 ja 20 §:n sekä 22 §:n 2

momentin tarkoittamia tietoja, joista kyseisissä säännöksissä tarkoitetut ammattihenkilöt ovat velvoitettuja tai oikeutettuja olemaan todistamatta. Hävittämisvelvollisuus ei koskisi kaikkea kyseisten ammattihenkilöiden viestintää, vaan hävittämisvelvollisuuden olemassaolon ratkaisisi tiedon sisältö. Vaikka ammattihenkilön viestintään sisältyvän tiedon hävittämiseen ei olisikaan velvollisuutta tämän kohdan perusteella, voisi velvollisuus olla olemassa edellä käsitellyn momentin 1 kohdan tai jäljempänä käsiteltävän 3 kohdan nojalla.

Säännöksessä mainittaisiin tiedon lähettäjän ja vastaanottajan, eli kahden- tai monenvälisen viestinnän osapuolten, ohella erikseen tiedon tallentaja. Tallentajalla viitattaisiin henkilöön, joka tallentaa pilvipalveluun dataa, esimerkiksi asiakirjan. Jos tällaisen pilvipalveluun tallennettavan asiakirjan sisältö kuuluisi jonkin säännöksessä tarkoitetun todistamiskiellon tai oikeuden olla todistamatta piiriin, olisi se hävitettävä.

Tieto olisi hävitettävä viipymättä kun on käynyt ilmi, että sitä koskee oikeudenkäymiskaareen liittyvä tiedustelukielto. Edellä 12 §:n yksityiskohtaisissa perusteluissa selostetuista syistä asia voidaan pääsääntöisesti havaita vasta 6 §:ssä säädettäväksi ehdotetun sisällön selvittämisen yhteydessä. Velvollisuudella viipymättä hävittämiseen tarkoitettaisiin tällaisissa tilanteissa sitä, että todistamiskiellon tai todistamattajättämisoikeuden alaisen tiedon sisällön tarkempi selvittäminen olisi välittömästi lopetettava ja tieto sekä sitä koskevat mahdolliset muistiinpanot heti hävitettävä.

Momentin 3 kohdan mukaan tietoliikennetiedustelulla saatu tieto olisi hävitettävä viipymättä, jos käy ilmi, ettei sitä tarvita kansallisen turvallisuuden suojaamiseksi. Säännöksen tarkoittama hävittämisvelvollisuus koskisi niin ollen tietoa, joka on epäolennaista kansallisen turvallisuuden suojaamisen kannalta.

Tietoliikennetiedustelulla saatu tieto voinee joissain tapauksissa koskea jotain muuta tietoliikennetiedustelun kohteena olevaa kansallista turvallisuutta vakavasti uhkaavaa toimintaa kuin sitä, mitä varten lupa tietoliikennetiedusteluun on myönnetty. Kyse voi olla esimerkiksi siitä, että lupa tietoliikennetiedusteluun on myönnetty tiedon hankkimiseksi terrorismiin liittyvästä uhkasta, mutta luvan nojalla toteutetun tietoliikennetiedustelun avulla saadaan terrorismin ohella tai sijasta tietoa joukkotuhoaseista. Jos tällaisella luvallisen tietoliikennetiedustelun oheistuotteena saadulla tiedolla on merkitystä kansallisen turvallisuuden suojaamiseksi, ei velvollisuutta sen hävittämiseen olisi.

Koska säännös vastaisi ehdotettavaa poliisilain 5 a luvun 45 §:n 1 momenttia, viitataan muilta osin kyseisen säännöksen perusteluihin.

Pykälän 2 momentin mukaan edellä 1 momentin 3 kohdassa tarkoitettu tieto voitaisiin kuitenkin poliisilain 5 a luvun 44 §:ssä säädetyin edellytyksin luovuttaa rikostorjuntaan ja poliisilain 5 a luvun 45 §:n 2 momentissa säädetyin edellytyksin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin. Kyse olisi hävittämisvelvollisuudesta ja siihen liittyvästä tiedon käyttökiellosta tietyin edellytyksin poikkeamista koskevasta säännöksestä. Ehdotettavasta säännöksestä ilmenevällä tavalla hävittämisvelvollisuudesta ja käyttökiellosta poikkeaminen tulisi kyseeseen vain silloin, kun hävittämisvelvollisuuden perusteena on pykälän 1 momentin 3 kohdan mukaisesti se, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi. Jos hävittämisvelvollisuus sen sijaan johtuu siitä, että kyse on kotimaisesta viestinnästä (1 momentin 1 kohta) tai kyse on todistamiskiellon taikka oikeuden olla todistamatta piiriin kuuluvasta tiedosta (1 momentin 2 kohta), ei hävittämisvelvollisuudesta ja siitä seuraavasta käyttökiellosta poikkeaminen nyt kyseessä olevan 2 momentin nojalla tai muutenkaan olisi mahdollista.

Koska ehdotettavan momentin sisältö muodostuu siinä viitattujen poliisilain 5 a luvun 45 §:n ja 45 §:n 2 momentin perusteella, viitataan muilta osin kyseisten säännösten perusteluihin.

Pykälän 3 momentin mukaan tietojen hävittämisestä vastaisi tietoliikennetiedustelun tekninen toteuttaja tai, jos se on ehtinyt toimittaa tiedot toimeksiantajalle, toimeksiantaja. Säännöksellä varmistettaisiin se, että viestit tai tiedot hävitetään heti ensi vaiheessa sen viranomaisen toimesta, joka on havainnut, että viestejä tai tietoja koskee pykälässä säädettäväksi ehdotettu velvollisuus.

Tietoliikennetiedustelun teknisenä toteuttajana toimisi 10 §:n 1 momentin mukaan puolustusvoimien tiedustelulaitos. Teknisenä toteuttajana toimiessaan puolustusvoimien tiedustelulaitos välittäisi suojelupoliisin toimeksiannon perusteella keräämänsä tietoliikenteen suojelupoliisille sellaisenaan. Sillä ei itsellään olisi oikeutta selvittää viestien sisältöä eikä myöskään tarkastella kerättävän tietoliikenteen muita tietoja sen enempää kuin toimeksiannon tekninen toteuttaminen edellyttäisi. Teknisessä toteuttamisessa ei tästä johtuen liene yleensä mahdollista tehdä havaintoa siitä, että toimeksiannon johdosta kerättyyn tietoliikenteeseen sisältyy hävittämisvelvollisuuden piiriin kuuluvia viestejä tai tietoja. Viestien ja tietojen tällainen luonne voitaneen pääsääntöisesti havaita vasta 6 §:n mukaisessa automatisoidusti erotellun tietoliikenteen jatkokäsittelyssä, jonka suorittaisi suojelupoliisi. Käytännössä voidaan siis arvioida hyvin poikkeukselliseksi, että viestit ja tiedot hävitettäisiin puolustusvoimien tiedustelulaitoksen toimesta niitä suojelupoliisille toimittamatta.

Viestien ja tietojen hävittämisen tarkoituksena olisi varmistaa se, ettei niitä voitaisi millään tavalla käyttää hyväksi tiedusteluviranomaisen toiminnassa. Viestien ja tietojen hävittämisestä ei kuitenkaan seuraisi, että niistä ei jäisi mitään merkintöjä asiakirjoihin. Laillisuusvalvonnallisista ja oikeusturvasyistä olisi välttämätöntä, että jokainen hävitystapahtuma ja sen peruste dokumentoitaisiin riittävällä tavalla. Siitä, millä tavalla ja tarkkuudella viestien ja tietojen hävittäminen kirjattaisiin, säädettäisiin 23 §:n mukaisesti valtioneuvoston asetuksella.

16 §. *Haitallista tietokoneohjelmaa tai käskyä koskevien tietojen luovuttaminen viranomaiselle, yritykselle tai yhteisölle.* Pykälässä säädettäisiin suojelupoliisin oikeudesta salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankittu tieto haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi.

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 yksityisiin tahoihin, olisi yhteiskunnan kokonaissuojautumisen kannalta tärkeää, että hyökkäyksissä käytettäviä haittaohjelmia koskevia tietoja voitaisiin mahdollisimman laajasti luovuttaa hyökkäysten potentiaalisille kohteille. Tietojen luovutusoikeudesta säätämällä voitaisiin osaltaan turvata tiedon saajan mahdollisuuksia ryhtyä huolehtimaan tietoturvastaan sellaisilla toimenpiteillä, joista säädetään sähköisen viestinnän palveluista annetun lain 272 §:ssä. Kyseisen säännöksen mukaiset toimenpiteet voivat pitää sisällään muun muassa viestin sisällön automaattisen selvittämisen, viestien välittämisen ja vastaanottamisen automaattisen estämisen tai rajoittamisen sekä tietoturvaa vaarantavien haitallisten tietokoneohjelmien automaattisen poistamisen viesteistä.

Pykälän 1 momentin 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 haittaohjelmaa tai -käskyä käyttävä taho tiedon julkiseksi tulemisen myötä voisi tehdä johtopäätöksiä viranomaisten kyvystä 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 kansalliseen turvallisuuteen liittyvät syyt voisivat estää tiedon luovuttamisen, vaikka tiedon saaminen sinänsä olisi viranomaisen, yrityksen tai yhteisön kannalta tarpeen, jotta se voisi turvata etunsa. On selvää, että kansalliseen turvallisuuteen liittyvät syyt voisivat vain poikkeuksellisesti muodostaa esteen tiedon luovuttamiselle viranomaistaholle, sillä kansallisen turvallisuuden suojaamiseksi olisi yleensä päinvastoin välttämätöntä, että viranomainen saisi tällaisen tiedon. Intressipunninnalla olisi suurempi merkitys silloin, kun tiedon saajana olisi yksityinen taho. Vaikka kynnys tiedon luovuttamiselle yksityisellekin taholle olisi syytä asettaa matalaksi, on syytä korostaa, ettei säännöksen tarkoituksena olisi siirtää vastuuta yritysten ja yhteisöjen tietoturvasta huolehtimisesta suojelupoliisille. Säännöksen tarkoituksena olisi mahdollistaa se, että suojelupoliisi osaltaan voisi tukea yritysten ja yhteisöjen toimenpiteitä tietoverkkohyökkäyksiltä suojautumiseksi.

Haitallista tietokoneohjelmaa tai -käskyä koskevan tiedon luovuttamiselle olisi kaksi vaihtoehtoista perustetta: kansallisen turvallisuuden suojaaminen ja tiedon saajan etujen turvaaminen. Perusteet tiedon luovuttamiselle voisivat yhtyä tapauksissa, joissa tiedon saajana olisi viranomainen tai esimerkiksi yhteiskunnan elintärkeän infrastruktuurin ylläpitämisen tai koko kansantalouden kannalta merkittävä yritys tai yhteisö. Perusteiden vaihtoehtoisuudesta seuraisi kuitenkin, että tieto voitaisiin edellä kuvatun harkinnan rajoissa luovuttaa siihen katsomatta, onko yrityksellä tai yhteisöllä tällaista merkitystä vai ei.

Pykälän 2 momentin mukaan yrityksen tai yhteisön palveluksessa olevan vaitiolovelvollisuuteen sovellettaisiin, mitä viranomaisten toiminnan julkisuudesta annetun lain 23§:n 2 momentissa säädetään. Viitatun lainkohdan toisen virkkeen mukaan vaitiolovelvollisuus on sillä, jolle viranomainen on ilmoittanut julkisuus- tai salassapito-olettaman sisältävän salassapitosäännöksen osoittamissa rajoissa tietoja, jotka ovat yleisöltä salassa pidettäviä. Yrityksen tai yhteisön palveluksessa olevan vaitiolovelvollisuudesta seuraisi julkisuuslain 23 §:n 1 momentin mukaan, että henkilö ei saisi paljastaa asiakirjan salassa pidettävää sisältöä tai tietoa, joka asiakirjaan merkittynä olisi salassa pidettävä, eikä muutakaan toimessaan tietoonsa saamaa seikkaa, josta lailla on säädetty vaitiolovelvollisuus. Vaitiolovelvollisuuden piiriin kuuluvaa tietoa ei saisi paljastaa senkään jälkeen, kun toiminta yrityksen tai yhteisön palveluksessa on päättynyt.

17 §. *Tiedon luovuttaminen rikostorjuntaan.* Pykälän mukaan tietoliikennetiedustelulla saadun tiedon rikostorjuntaan luovuttamiseen sovellettaisiin poliisilain 5 a luvun 44 §:ää.

Pykälän perusteluiden osalta viitataan poliisilain kyseisen ehdotettavan pykälän perusteluihin.

18 §. *Asianosaisjulkisuuden rajoittaminen eräissä tapauksissa.* Pykälässä säädettäisiin asianosaisen tiedonsaantioikeuden rajoittamisesta tietoliikennetiedustelun käyttöä koskevissa asioissa.

Koska pykälä asiallisesti vastaisi poliisilain ehdotettavan 5 a luvun 49 §:n sääntelyä, viitataan pykälän perusteluiden osalta kyseisen poliisilain pykälän perusteluihin.

19 §. *Pöytäkirja.* Pykälän mukaan tiedustelumenetelmän käytön lopettamisen jälkeen olisi laadittava ilman aiheetonta viivytystä pöytäkirja.

Koska pykälä asiallisesti vastaisi poliisilain 5 luvun voimassa olevan 59 §:n ja poliisilain ehdotettavan 5 a luvun 48 §:n sääntelyä, viitataan pykälän perusteluiden osalta poliisilain kyseisten pykälien perusteluihin.

20 §. *Tietoliikennetiedustelun käytöstä ilmoittaminen.* Pykälässä säädettäisiin tietoliikennetiedustelun käytöstä ilmoittamisesta. Yleisperusteluista ilmenevällä tavalla Euroopan ihmisoikeustuomioistuin on lukuisissa ratkaisuissaan ottanut kantaa kysymykseen siitä, tuleeko ja missä tilanteissa tiedonhankinnan kohdehenkilöllä olla oikeus saada viranomaiselta tieto häneen kohdistetusta tiedonhankintatoimenpiteestä, esimerkiksi tietoliikennetiedustelusta. EIT on ratkaisukäytännössään korostanut, että tiedonhankinnan kohdehenkilöllä on oltava käytössään tehokkaat oikeusturvakeinot mahdollisesti lainvastaista viranomaistiedonhankintaa vastaan. Valitus- tai kantelumahdollisuuden käytön edellytyksenä on ihmisoikeustuomioistuimen toteamalla tavalla yleensä se, että henkilö saa viranomaiselta tiedon häneen kohdistetusta salaisesta tiedonhankinnasta sen jälkeen kun salaisen tiedonhankintamenetelmän käyttö on päättynyt. EIT:n ratkaisukäytännön mukaan 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. Kuitenkin myös järjestelmä, joka ei edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin oikeus kannella viranomaisen salaisesta tiedonhankinnasta on tullut kansallisessa lainsäädännössä säätää sillä tavalla yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisen saattaneen puuttua luottamuksellisen viestintänsä nauttimaan suojaan (EIT Kennedy v. Yhdistynyt Kuningaskunta).

Ehdotettavassa pykälässä velvollisuus ilmoittaa tietoliikennetiedustelusta rajattaisiin tapauksiin, joissa tietoliikennetiedustelun voidaan katsoa puuttuneen luottamuksellisen viestin salaisuuteen verrattain syvällisesti. Pykälän mukaisen rajatun ilmoittamisvelvollisuuden vastapainoksi tiedustelutoiminnan valvontaa koskevan lain 22 §:ssä ehdotetaan säädettäväksi yleisestä oikeudesta tehdä tietoliikennetiedustelua koskeva tutkimispyyntö tiedustelun oikeudelliselle valvontaviranomaiselle. Pykälässä säädettäväksi ehdotettava ilmoittamisvelvollisuus olisi laajempi kuin esimerkiksi Ruotsissa, jossa ilmoittamisvelvollisuus on signaalitiedustelulain 11 a §:n nojalla olemassa vain silloin, kun signaalitiedustelussa on käytetty johonkin tiettyyn luonnolliseen henkilöön välittömästi liittyviä hakuehtoja.

Pykälän ensimmäisen virkkeen mukaan, jos 6 §:ssä tarkoitetussa automatisoidusti erotellun tiedon jatkokäsittelyssä olisi manuaalisesti selvitetty tietyn Suomessa olevan henkilön luottamuksellisen viestin tai tallentaman tiedon sisältö, ilmoitettaisiin hänelle tietoliikennetiedustelusta noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan olisi, jos tietoliikennetiedustelulla saatu tieto olisi hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

Automatisoidun erottelun avulla kerättyä tietoa saataisiin 5 §:n mukaan käsitellä automaattisesti ja manuaalisesti. Automaattisessa ja manuaalisessa käsittelyssä puolestaan saataisiin selvittää viestin sisältö ja muut luottamukselliset tiedot. Nyt kyseessä olevassa pykälässä edellytettäisiin kohteelle ilmoittamista silloin, kun käsittely olisi ollut manuaalista ja siinä olisi selvitetty luottamuksellisen viestin tai tallennetun tiedon sisältö. Koska vieraan valtion tai sellaiseen rinnastuvan tahon viestintä ehdotetun 4 §:n perusteluissa todetulla tavalla ei nauti luottamuksellisen viestin salaisuuden suojaa, ei säännös perustaisi velvollisuutta ilmoittaa tietoliikennetiedustelusta tällaisen viestinnän osapuolelle. Säännös ei myöskään perustaisi velvollisuutta ilmoittaa tietoliikennetiedustelusta sellaiselle luottamuksellisen viestin salaisuuden suojaa sinänsä nauttivalle henkilölle, joka on muualla kuin Suomessa. Ilmoittamisvelvollisuus olisi näissä tapauksissa monesti muutenkin tehoton kohteen henkilöllisyyttä koskevan epätietoisuuden vuoksi tai siksi, että henkilöllisyydeltään sinänsä tunnetun kohteen olinpaikka ei olisi tiedossa tai kohtuullisella työllä selvitettävissä.

Luottamuksellisen viestin sisällön ohella säännöksessä mainittaisiin erikseen tallennetun tiedon sisältö. Tallennetulla tiedolla viitattaisiin pilvipalveluun tallennettuun tietoon.

Silloin kun velvollisuus ilmoittaa tietoliikennetiedustelusta olisi olemassa, sovellettaisiin ilmoittamiseen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Sellaisen tietoliikennetiedustelun, jossa selvitetään luottamuksellisen viestin sisältö, voidaan katsoa sekä teknisessä mielessä että perusoikeuspuuttumisen syvyyden puolesta läheisesti rinnastuvan telekuunteluun. Siksi ehdotetaan, että velvollisuudesta ilmoittaa edellä mainitusta kahdesta menetelmästä säädettäisiin yhdenmukaisesti. Kun tietoliikennetiedustelusta ilmoittamiseen sovellettaisiin telekuuntelusta ilmoittamista, seuraisi tästä, että tietoliikennetiedustelun käytöstä olisi viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus olisi saavutettu. Tuomioistuin voisi kuitenkin suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta päättää, että ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se olisi perusteltua käynnissä olevan tiedonhankinnan turvaamiseksi, kansallisen turvallisuuden tai valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saataisiin tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se olisi välttämätöntä kansallisen turvallisuuden tai valtion turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Jos tiedonhankinnan kohteen henkilöllisyys ei olisi tiedossa määräajan tai lykkäyksen päättyessä, tiedonhankintakeinon käytöstä olisi ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä. Kohteelle ilmoittamisesta olisi samalla annettava kirjallisesti tieto tietoliikennetiedusteluun luvan myöntäneelle tuomioistuimelle. Jos suojelupoliisi kuitenkin jatkaisi tiedonhankintaa poliisilain ehdotetun 5 a luvun 5 §:n perusteella, noudatettaisiin, mitä salaisen tiedonhankintakeinon käytöstä ilmoittamisesta 5 luvun 58 §:ssä säädetään. Tietoliikennetiedustelusta ilmoittamista koskevan asian käsittelyssä tuomioistuimessa noudatettaisiin mitä poliisilain ehdotetun 5 a luvun 35 §:ssä säädettäisiin.

Edellä sanotun lisäksi viitataan siihen, mitä poliisilain ehdotetun 5 a luvun 47 §:n perusteluissa todetaan.

Pykälän toisen virkkeen mukaan velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan olisi, jos tietoliikennetiedustelulla saatu tieto olisi hävitetty 8 §:n 2 momentin tai 15 §:n perusteella. Kyse olisi poikkeuksesta siihen, mistä ensimmäisessä virkkeessä olisi säädetty. Näin ollen, jos manuaalisessa käsittelyssä olisi selvitetty tietyn Suomessa olevan henkilön viestin sisältö, mutta samassa yhteydessä olisi havaittu, että kyse on hävittämisvelvollisuuden alaan kuuluvasta tiedosta, ja tuo tieto olisi hävittämisvelvollisuuden mukaisesti viipymättä hävitetty, ei velvollisuutta ilmoittamiseen olisi. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei tällaisissa tapauksissa voitane pitää perusteltuna, sillä sen henkilön luottamuksellisen viestin sisältö, jolle ilmoitus olisi muuten tehtävä, olisi hävitetty tiedusteluviranomaisen hallusta.

21 §. *Tietoliikennetiedustelun edellyttämän kytkennän toteuttaminen*. Pykälän mukaan tietoliikennetiedustelun edellyttämän kytkennän toteuttamisessa siviilitiedustelua varten noudatettaisiin, mitä sotilastiedustelulain 72 §:ssä säädetään. Kytkennän toteuttamista koskeva substanssisääntely sisältyisi sotilastiedustelulakiin sen vuoksi, että se läheisesti liittyy tietoliikennetiedustelun tekniseen toteuttamiseen, josta vastaisi puolustusvoimien tiedustelulaitos. Sotilastiedustelulakiin viittaavan säännöksen avulla varmistettaisiin se, että kytkennän toteuttajalla olisi velvollisuus suorittaa sille kuuluvat toimenpiteet siihen katsomatta, palvelevatko ne siviili- vai sotilastiedusteluviranomaisen tietoliikennetiedustelua.

Pykälässä viitatun sotilastiedustelulain 72 §:n mukaan tiedustelun kytkennän suorittaja panisi täytäntöön sotilastiedustelulain 5 luvussa tarkoitetut luvat ja luovuttaisi luvassa mainitussa viestintäverkon osassa liikkuvan tietoliikenteen edelleen puolustusvoimien tiedustelulaitokselle. Pykälän tarkoittamaksi kytkennän suorittajaksi osoitettaisiin sotilastiedustelulain 9 §:ssä Suomen Erillisverkot Oy. Viittauksesta sotilastiedustelulain 72 §:ään seuraisi, että Suomen Erillisverkot Oy:llä olisi velvollisuus suorittaa kytkentä ja luovuttaa tietoliikenne puolustusvoimien tiedustelulaitokselle myös silloin, kun kyse on tämän lain 7 tai 9 §:n tarkoittaman päätöksen täytäntöönpanosta.

Pykälän perusteluiden osalta viitataan muilta osin sotilastiedustelulain 72 §:n perusteluihin.

22 §. *Tiedonsiirtäjän tietojenantovelvollisuus.* Pykälässä säädettäisiin tiedonsiirtäjän velvollisuudesta antaa suojelupoliisille tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen päällystöön kuuluvan suojelupoliisin poliisimiehen yksilöidystä pyynnöstä hallussaan olevat Suomen rajan ylittävän viestintäverkon rakenteeseen ja siinä kulkevan tietoliikenteen reitittymiseen liittyvät tekniset tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi tietoliikennetiedustelun käyttöä koskevaa lupavaatimusta ja -päätöstä varten.

Kyseinen velvollisuus liittyy tuomioistuimen lupaa koskevan 7 §:n 2 momentin 5 kohdan sääntelyyn, jonka mukaan suojelupoliisin olisi tuomioistuimelle esittämässään lupavaatimuksessa yksilöitävä se viestintäverkon osa, jossa kulkevaan tietoliikenteeseen tietoliikennetiedustelun automaattisia hakuehtoja verrattaisiin. Jotta viestintäverkon osa voitaisiin lupavaatimusta varten yksilöidä, olisi välttämätöntä, että suojelupoliisi saisi yksilöintiä edistäviä tietoja niiltä tahoilta, joilla sellaisia liiketoimintaansa liittyvistä syistä on hallussaan. Tietojen antamisvelvollisuudesta säätämällä voitaisiin ehkäistä se, että 5 §:ssä säädettäväksi ehdotettava tietoliikennetiedustelun hakuehtoperusteinen vertailu tulisi kohdistumaan tietoliikenteeseen laajemmin kuin on välttämätöntä tietoliikennetiedustelun kohteena olevan kansallista turvallisuutta vakavasti uhkaavan toiminnan selvittämiseksi. Jos tiedonsiirtäjän hallussa olevat tiedot osoittaisivat, että selvitettävänä olevaa uhkaavaa toimintaa koskeva tietoliikenne ei voi liikkua jossain tietyssä viestintäverkon osassa esimerkiksi sen vuoksi, että se on varattu jonkin selvitettävänä olevan uhkan kannalta epäolennaisen asiakasorganisaation käyttöön, ei tuo viestintäverkon osa voisi olla tietoliikennetiedustelua koskevan lupavaatimuksen piirissä.

Pykälän tarkoittaman tiedonantovelvollisuuden piiriin kuuluvat tiedot koskisivat ennen kaikkea sitä, mitkä asiakasorganisaatiot ovat varanneet tiedonsiirtäjältä siirtokapasiteettia käyttöönsä ja mitä tiedonsiirtäjän hallitsemia rajan ylittävän viestintäverkon osia tällaiset varaukset koskevat. Pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja myös muista mahdollisista seikoista, jotka vaikuttavat tietoliikenteen reitittymistodennäköisyyteen sen ylittäessä Suomen rajan tiedonsiirtäjän omistamassa tai sen hallinnassa olevassa viestintäverkon osassa. On syytä korostaa, että pykälä velvoittaisi tiedonsiirtäjän antamaan tietoja vain siltä kapasiteettia varanneista asiakasorganisaatioista, ei sen sijaan viestintätapahtumien osapuolena olevista kuluttaja-asiakkaistaan. Pykälä ei muutenkaan perustaisi suojelupoliisille oikeutta hankkia tai saada tietoja yksittäisistä viestintätapahtumista tai niiden osapuolina olevista henkilöistä.

Tiedonsiirtäjä olisi velvoitettu antamaan tiedot suojelupoliisin yksilöidystä pyynnöstä. Pyynnön yksilöimistä koskevalla vaatimuksella tarkoitettaisiin sitä, että suojelupoliisin olisi pyynnön yhteydessä annettava riittävät tiedot, jotta tiedonsiirtäjä voisi arvioida, mitkä sen hallussa olevat tiedot ovat tarpeen pyynnön täyttämiseksi. Pyyntö ei voisi koskea epäämäräistä rajoittamatonta tietojoukkoa, vaan suojelupoliisin olisi pyynnössä rajattava kohteena olevaa asiaa.

Pykälä velvoittaisi tiedonsiirtäjän antamaan suojelupoliisille sellaiset tiedot, jotka ovat viestintäverkon osan yksilöimiseksi tarpeellisia. Tietojen tarpeellisuutta koskeva vaatimus sisältäisi sen, että tiedonsiirtäjän olisi annettava suojelupoliisille kaikki sellaiset tiedot, joilla voi olla viestintäverkon osan mahdollisimman tarkan yksilöimisen kannalta merkitystä. Toiselta puolen tietojen tarpeellisuudelle asetettavasta vaatimuksesta seuraisi, ettei tiedonsiirtäjä olisi velvoitettu antamaan suojelupoliisille mitään sellaisia hallussaan olevia tietoja, joilla ei voi olla edellä mainitun asian kannalta merkitystä. Tiedonsiirtäjän pykälässä tarkoitetun velvollisuuden nojalla antamat tiedot eivät liittyisi yksittäisiin henkilöihin liittyvien välitystietojen hankkimiseen, vaan kyse olisi nimenomaan tietyn viestintäverkon osan tunnistamisesta.

Tiedonsiirtäjän velvollisuus antaa tietoja koskisi ainoastaan sellaisia tietoja, jotka sillä on valmiiksi hallussaan. Säädettäväksi ehdotettava tietojenantovelvollisuus ei näin ollen velvoittaisi tiedonsiirtäjiä hankkimaan uusia tietoja suojelupoliisia varten.

Tiedonsiirtäjä olisi vaitiolovelvollinen suojelupoliisin pyynnöstä ja siihen antamastaan vastauksesta viranomaisten toiminnan julkisuudesta annetun lain 23 §:n 2 momentin ja 24 §:n 1 momentin 5 ja 9 kohtien nojalla.

23 §. *Korvaus tiedonsiirtäjälle.* Pykälässä säädettäisiin tiedonsiirtäjälle tietojen antamisesta aiheutuneiden kustannusten korvaamisesta, korvauspäätöksen tekijästä sekä muutoksenhausta.

Pykälän 1 momentin mukaan tiedonsiirtäjällä olisi oikeus saada valtion varoista korvaus 22 §:ssä tarkoitetusta tietojen antamisesta aiheutuneista välittömistä kustannuksista. Momentissa tarkoitetut välittömät kustannukset olisivat pääasiassa työvoimakustannuksia. Välittömiä kustannuksia voisivat myös olla tietoja koostettaessa mahdollisesti hyödynnettävien teknisten laitteistojen ynnä muiden apuvälineiden käytöstä aiheutuvat kustannukset. Korvauksen maksamisesta päättäisi suojelupoliisi. Suojelupoliisi ratkaisisi näin ollen sen, mitkä kustannukset ovat välittömiä ja tulevat korvattavaksi. Suojelupoliisi myös määrittäisi korvauksen suuruuden.

Pykälän 2 momentin mukaan suojelupoliisin päätökseen saisi vaatia oikaisua siten kuin hallintolaissa (434/2003) säädetään. Oikaisuvaatimukseen annettuun päätökseen saisi hakea muutosta valittamalla hallinto-oikeuteen siten kuin hallintolainkäyttölaissa (586/1996) säädetään. Hallinto-oikeuden päätökseen saisi hakea muutosta valittamalla vain, jos korkein hallinto-oikeus myöntää valitusluvan. Momentin sääntely vastaisi pakkokeinolain 10 luvun 64 §:n 2 momentin, poliisilain 5 luvun 62 §:n 2 momentin ja poliisilain ehdotetun 5 a luvun 51 §:n

sääntelyä koskien muutoksenhakua poliisiyksikön päätökseen kustannusten korvaamisesta teleyritykselle muun muassa tietojen antamisesta teleyritykselle aiheutuneista kustannuksista.

24 §. *Tietoliikennetiedustelun valvonta sisäasiainhallinnossa.* Pykälässä säädettäisiin tietoliikennetiedustelun käytön oikeudellisesta valvonnasta sisäasianhallinnossa. Pykälä asiallisesti vastaisi poliisilain 5 a luvun 59 §:ään ehdotettavaa sääntelyä.

25 §. *Tietoliikennetiedustelun ulkoinen valvonta.* Pykälässä säädettäisiin tietoliikennetiedustelun käytön ulkoisesta valvonnasta. Pykälä asiallisesti vastaisi poliisilain 5 a luvun 60 §:ään ehdotettavaa sääntelyä.

26 §. *Tiedusteluvaltuutetulle tehtävät ilmoitukset*. Pykälän mukaan suojelupoliisin olisi annettava tieto tiedusteluvaltuutetulle tämän lain nojalla annetuista tuomioistuimen luvista ja päätöksistä mahdollisimman pian tehdyn päätöksen jälkeen. Pykälä asiallisesti vastaisi poliisilain 5 a luvun 61 §:n 1 momenttiin ehdotettavaa sääntelyä.

27 §. *Tarkemmat säännökset.* Pykälässä säädettäisiin tietoliikennetiedustelun käytön järjestämistä ja valvontaa sekä toimenpiteiden kirjaamista ja valvontaa varten annettavia selvityksiä koskevasta asetuksenantovaltuudesta. Asiallisesti samansisältöinen asetuksenantovaltuutta koskeva säännös on nykyisin poliisilain 5 luvun 65 §:ssä, jossa se koskee kyseisen luvun mukaisten salaisten tiedonhankintakeinojen käytön järjestämistä ja valvontaa sekä toimenpiteiden kirjaamista ja valvontaa varten annettavia selvityksiä. Asetuksenantovaltuussäännös ehdotetaan myös otettavaksi poliisilain 5 a luvun 62 §:ksi, jossa se koskisi kyseisessä luvussa säädettäväksi ehdotettuja tiedustelumenetelmiä sekä muuta toimintaa. Nyt kyseessä olevan pykälän perusteluiden osalta viitataan jälkimmäisen edellä mainitun poliisilain 5 a luvun pykälän perusteluihin siltä osin, kun kyse on tiedustelumenetelmän käytön järjestämistä ja valvontaa sekä toimenpiteiden kirjaamista ja valvontaa varten annettavia selvityksiä.

1.3 Laki poliisin hallinnosta annetun lain muuttamisesta

10 §. *Suojelupoliisi.* Poliisilain 1 luvun 1 §:n 1 momenttia ehdotetaan muutettavaksi niin, että poliisin tehtäväksi säädettäisiin kansallisen turvallisuuden suojaaminen. Tämä pykälä saatettaisiin yhteismitalliseksi poliisilain 1 luvun 1 §:n 1 momentin kanssa ja siinä täsmennettäisiin, että kansallisen turvallisuuden suojaamista koskeva tehtävä poliisin organisaatiossa ensisijaisesti kuuluisi suojelupoliisille.

Voimassa olevan poliisin hallinnosta annetun lain 10 §:n 1 momentin ensimmäisen virkkeen 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. Toisen virkkeen mukaan suojelupoliisin tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi.

Momentin ensimmäistä virkettä ehdotetaan muutettavaksi ensinnäkin siten, että siihen lisättäisiin suojelupoliisin tehtäväksi hankkia sellaista tietoa, joka on tarpeen kansallisen turvallisuuden suojaamiseksi. Muutoksella täsmennettäisiin suojelupoliisin tehtävää tiedonhankinnallisempaan ja tiedustelullisempaan suuntaan nykyisen ennalta estävän tehtävän ohella. Lisäksi virkkeessä käytettävä käsite torjua ehdotetaan korvattavaksi ilmaisulla havaita, estää ja paljastaa, koska käsitteen torjua voidaan katsoa kattavan myös rikosten selvittämisen. Rikosten selvittämistehtävä ehdotetaan tässä esityksessä poistettavaksi suojelupoliisilta. Virkkeen loppuosasta ehdotetaan samasta syystä poistettavaksi maininta siitä, että suojelupoliisi suorittaa rikosten tutkintaa. Virkettä muutettaisiin myös niin, että siihen lisättäisiin käsite toiminnat siinä

nykyisin mainittujen hankkeiden ja rikosten lisäksi. Säännökseen lisättävällä käsitteellä viitattaisiin poliisilain 5 a luvun 3 §:ssä sekä siviilitietoliikennetiedustelulain 3 §:ssä tarkoitettuun kansallista turvallisuutta vakavasti uhkaavaan toimintaan. Lisäksi virkettä ehdotettaisiin muutettavaksi siten, että siinä käytetty käsite vaarantaa muutettaisiin käsitteeksi uhata. Tämä olisi perusteltua, koska edellä viitatuissa poliisilain 5 a luvun 3 §:ssä sekä siviilitietoliikennetiedustelulain 3 §:ssä käytetään ilmaisua uhkaava toiminta.

Momentin toista virkettä muutetaan siten, että siinä käytetty käsite valtakunnan turvallisuus korvattaisiin nykyaikaisemmalla käsitteellä yhteiskunnan turvallisuus. Virkettä muutettaisiin myös niin, että siihen lisättäisiin havaitseminen estämisen lisäksi. Tämänkin lisäyksen tarkoituksena olisi ilmentää suojelupoliisin tiedonhankinnallista tehtävää ennalta estämistehtävän ohella. Virkettä ehdotetaan muutettavaksi myös siten, että käsite vaarantava muutetaan käsitteeksi uhkaava samalla tavoin kuin ensimmäisessä virkkeessä.

Pykälän 2 momentin mukaan sisäministeriö määräisi Poliisihallitusta kuultuaan tarvittaessa tarkemmin suojelupoliisin ja muiden poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä. Momentin muutos liittyy 1 momentissa ehdotettuun muutokseen koskien esitutkintatoimivaltuuksien poistamista. Sisäministeriö ei siten enää päättäisi asiaryhmistä, jotka kuuluvat suojelupoliisin tutkittaviksi. Sisäministeriö kuitenkin päättäisi suojelupoliisin ja muiden poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä. Vaikka suojelupoliisilta ehdotetaan poistettavaksi esitutkinta- ja pakkokeinotoimivaltuudet, niin suojelupoliisi voisi osallistua edelleenkin tarpeen mukaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa. Tämä tehtävä liittyisi poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä päättämiseen. Koska suojelupoliisilla ei kuitenkaan olisi varsinaisia esitutkintaan liittyviä tutkintatehtäviä, niin maininta tutkintajärjestelyistä päättämisestä poistettaisiin momentin lopusta.

15 a §. *Poliisivaltuudet.* Pykälään lisättäisiin uusi 3 momentti, jossa todettaisiin, että 1 momentissa säädetyn lisäksi suojelupoliisin virkamiehellä olisi oikeus käyttää poliisilain 5 a luvussa tarkoitettuja tiedustelumenetelmiä kansallisen turvallisuuden suojaamiseksi sen mukaan kuin mainitussa luvussa säädetään.

Ilmauksella "sen lisäksi mitä 1 momentissa säädetään " tarkoitettaisiin, että ainoastaan suojelupoliisin palveluksessa olevalla virkamiehellä olisi oikeus käyttää 5 a luvussa tarkoitettuja toimivaltuuksia. Tämä ilmenee myös poliisilakiehdotuksen 5 a luvusta sekä sen perusteluista. Lähtökohtaisesti 5 a luvun toimivaltuuksia käyttäisi suojelupoliisissa virkasuhteessa oleva poliisimies, mutta joissain tilanteissa myös muu kuin poliisimies voi joutua avustamaan tai osin käyttämään tiettyjä toimivaltuuksia. Siksi on poliisimiehen sijasta perustelua puhua suojelupoliisin virkamiehestä.

Momentissa tarkoitettujen toimivaltuuksien käyttämistä ei olisi alueellisesti rajattu samalla tavalla kuin 1 momentissa, jonka mukaan poliisimiehellä on tehtäväänsä suorittaessaan koko maassa poliisilaissa tai muussa laissa säädetyt valtuudet. Näin ollen suojelupoliisin virkamiehellä olisi erikseen säädetyissä tilanteissa oikeus käyttää kyseisiä toimivaltuuksia myös ulkomaan tiedustelussa kuitenkin sen mukaan kuin poliisilain 5 a luvussa säädetään.

Pykälään lisättävä 2 momentti olisi erityissäännös 1 momenttiin nähden.

1.4 Laki henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

5 §. *Suojelupoliisin toiminnallinen tietojärjestelmä.* Pykälän 2 momenttia muutettaisiin niin, että suojelupoliisin toiminnallinen tietojärjestelmä voisi sisältää myös tietoja, joita olisi tar-

peen käsitellä kansallisen turvallisuuden suojaamiseksi tai rikosten paljastamiseksi tai selvittämiseksi.

Suojelupoliisin on tehtävänsä hoitamista varten ylläpidettävä suojelupoliisin toiminnallista tietojärjestelmää, johon talletetaan suojelupoliisin tehtävän kannalta tarpeellinen tieto ja siten myös eri toimivaltuuksilla saadut tiedot. Ehdotetuilla poliisilain 5 a luvun sekä lain tietoliikennetiedustelusta siviilitiedustelussa mukaisilla toimivaltuuksilla saadut henkilötiedot talletettaisiin suojelupoliisin toiminnalliseen tietojärjestelmään. Suojelupoliisin toiminnallista tietojärjestelmää koskevaa pykälää ehdotetaan muutettavaksi siten, että pykälästä ilmenee muutettavan poliisilain 1 luvun 1 §:n 1 momentin mukaisesti kansallisen turvallisuuden suojaaminen sekä lisätään siihen samasta syystä perusteeksi myös rikosten paljastaminen.

13 §. *Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä.* Pykälän 2, 4, 15 ja 16 kohtia ehdotetaan muutettavaksi niin, että niihin lisättäisiin "kansallisen turvallisuuden suojaamiseksi". Ehdotus liittyisi poliisilain 1 luvun 1 §:n 1 momenttiin ehdotettavaan muutokseen poliisin tehtävissä.

Pykälän 2 kohtaa muutettaisiin lisäksi niin, että siihen lisättäisiin "rikosten paljastamiseksi". Tämä muutos olisi tekninen, sillä poliisin tehtävänä rikoksen paljastaminen on ollut jo vuoden 2014 alusta lähtien.

45 §. *Tarkastusoikeuden rajoittaminen.* Pykälän 1 momentin 5 kohtaa ehdotetaan muutettavaksi niin, että tarkastusoikeutta ei poliisilain 5 luvun ja pakkokeinolain 10 luvun lisäksi olisi tietoihin, jotka olisi saatu poliisilain 4 luvun 3 §:ssä, 5 a luvussa tai siviilitiedustelusta tietoliikennetiedustelusta annetussa laissa tarkoitettuja toimivaltuuksia käyttäen. Lisäksi pykälästä poistettaisiin viittaus kumottuun sähköisen viestinnän tietosuojalakiin.

Tietojen lainmukaisuuden tarkastamisella ei tarkoitettaisi niiden alkuperäisen hankkimisen lainmukaisuuden tai tarkoituksenmukaisuuden, vaan niiden käsittelyn lainmukaisuuden tarkastamista. Rekisteröidyn tietojen käsittelyn lainmukaisuuden voi pyytää tarkistettavaksi tietosuojavaltuutetun toimesta pykälän 2 momentissa säädetyllä tavalla.

1.5 Laki esitutkintalain muuttamisesta

2 luku **Esitutkintaan osalliset**

1 §. *Viranomaiset esitutkinnassa.* Pykälän 1 momenttia muutettaisiin niin, että siihen lisättäisiin virke, jonka mukaan suojelupoliisi ei olisi kuitenkaan esitutkintaviranomainen.

Suojelupoliisin esitutkintatoimivaltuuksien rajoittaminen liittyisi suojelupoliisin tiedustelullisten toimivaltuuksien lisääntymiseen. Nykyisin suojelupoliisi voi käyttää rikoksen estämiseksi ja paljastamiseksi poliisilain 5 luvussa tarkoitettuja salaisia tiedonhankintakeinoja ja rikoksen selvittämiseksi pakkokeinolain 10 luvussa säädettyjä salaisia pakkokeinoja. Yleisperusteluissa esitetyn mukaisesti tulisi oikeudenmukaisen oikeudenkäynnin turvaamiseksi harkita suojelupoliisin esitutkintatehtävien ja -toimivaltuuksien rajoittamista. Esitutkintatoimivallan rajoittaminen ei kuitenkaan estäisi suojelupoliisin mahdollisuutta osallistua tarpeen mukaan esitutkintaviranomaisen suorittamaan esitutkintaan asiantuntijaviranomaisen ominaisuudessa.

1.6 Laki rikoslain muuttamisesta

12 luku **Maanpetosrikoksista**

12 §. *Rajoitussäännös*. Pykälässä säädettäisiin siitä, ettei rikoslain 12 luvussa tarkoitettuna rikoksena pidetä poliisilain (872/2011) 5 a luvun, tietoliikennetiedustelusta siviilitiedustelussa annetun lain (/) tai sotilastiedustelusta annetun lain (/) mukaista tiedustelumenetelmien käyttämistä. Tällä tarkoitettaisiin sitä, että toimiessaan tiedustelulainsäädännön mukaisesti tiedustelumenetelmää käyttävä virkamies ja tiedustelun kohteena oleva henkilö eivät syyllisty rikoslain 12 luvussa tarkoitettuun tekoon. Esimerkiksi peitetoiminnassa sitä suorittava virkamies saattaa joutua tilanteisiin, joissa hänen menettelynsä täyttää rikoksen tunnusmerkistön ja joissa menettelystä seuraisi ilman rajoitussäännöstä rikosoikeudellinen vastuu. Oikeuskäytännön varaan ei voida jättää sitä, miten tiedustelulainsäädännön mukaisesti käytettävä peitetoiminta tai muu tiedustelumenetelmä suhtautuu rikoslain 12 luvun säännöksiin.

1.7 Laki pakkokeinolain muuttamisesta

2 luku Kiinniottaminen, pidättäminen ja vangitseminen

9 §. *Pidättämiseen oikeutettu virkamies.* Pykälän 1 momentin 1 kohtaa muutettaisiin niin, että siitä poistettaisiin suojelupoliisin päällikkö, esitutkintatehtäviin määrätty apulaispäällikkö, esitutkintatehtäviin määrätty osastopäällikkö, esitutkintatehtäviin määrätty ylitarkastaja ja tarkastaja. Kyseiset virkamiehet eivät olisi enää pidättämiseen oikeutettuja virkamiehiä. Muutos liittyisi edellä esitutkintalain yhteydessä ehdotettuun muutokseen.

10 luku Salaiset pakkokeinot

3 §. *Telekuuntelu ja sen edellytykset*. Pykälän 1 momentin ensimmäisessä virkkeessä ehdotetaan muutettavaksi telekuuntelun määritelmää, koska voimassa olevan lain määritelmässä viitataan kumottuun viestintämarkkinalakiin.

Ehdotettavan määritelmän mukaan telekuuntelulla tarkoitettaisiin sähköisen viestinnän palveluista annetun lain 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 8 §:ssä tarkoitettujen tunnistamistietojen selvittämiseksi. Telekuuntelua saataisiin kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jonka voidaan perustellusti olettaa syyllistyvän 2 momentissa mainittuun rikokseen.

Muutoksen tarkoituksena ei ole asiallisesti muuttaa telekuuntelun määritelmää tai sen soveltamisalaa, vaan muutos olisi tekninen.

6 §. *Televalvonta ja sen edellytykset*. Pykälän 1 momentissa ehdotetaan tarkistettavaksi televalvonnan määritelmää, koska voimassa olevan lain määritelmässä viitataan kumottuun sähköisen viestinnän tietosuojalakiin sekä viittausketjun kautta telekuuntelun määritelmäsäännöksessä (3 §) olevaan viestintämarkkinalakiin, joka on kumottu.

Ehdotettavan määritelmän mukaan televalvonnalla tarkoitettaisiin tunnistamistietojen hankkimista viestistä, joka on lähetetty 3 §: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 tarkoitettaisiin sähköisen viestinnän palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun tilaajaan tai mainitun pykälän 30 kohdassa tarkoitettuun käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

Muutoksen tarkoituksena ei ole asiallisesti muuttaa televalvonnan määritelmää tai sen soveltamisalaa, vaan muutos olisi tekninen.

39 §. *Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset.* Pykälän mukaan tietolähdetoiminnalla tarkoitettaisiin muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun viranomaisen ulkopuoliselta henkilöltä (tietolähde).

Voimassa olevassa laissa tietolähde voi olla ainoastaan poliisin ja muun esitutkintaviranomaisen ulkopuolinen henkilö. Käytännössä on esiintynyt tulkinnanvaraisuutta sen suhteen, onko muu kuin esitutkintaviranomaisen palveluksessa olevan virkamies rekisteröitävä tietolähteeksi. Siksi määritelmää ehdotetaan täsmennettäväksi mainitulla tavalla, ja tietolähde olisi poliisiviranomaisen ja muun viranomaisen ulkopuolinen henkilö.

1.8 Laki oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain muuttamisesta

5 §. *Oikeudenkäyntiä koskevien perustietojen julkiseksi tulemisen ajankohta.* Poliisilakiin (872/2011) ehdotettavaksi lisättävässä 5 a luvussa ja sotilastiedustelusta annetun lain 4 luvussa säädettäisiin muun muassa telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta, televalvonnasta ja tukiasematietojen hankkimisesta. Tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa ja sotilastiedustelusta annetun lain 5 luvussa puolestaan säädettäisiin tietoliikennetiedustelusta. Ottaen huomioon, että esimerkiksi näiden tiedustelumenetelmien käyttö edellyttää tuomioistuimen lupaa, tulisi tieto tällaisen asian käsittelystä tuomioistuimessa helposti julki ennen siviili- tai sotilastiedustelun tavoitteiden saavuttamista, jollei oikeudenkäyntiä koskevien perustietojen julkiseksi tulemisen ajankohdasta säädetä toisin kuin oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain 4 §:ssä edellytetään. Viimeksi mainitun lainkohdan mukaan tiedot asiaa käsittelevästä tuomioistuimesta, asian yksilöidystä laadusta, asian käsittelyn vaiheista sekä suullisen käsittelyn ajankohdasta ja käsittelypaikasta sekä asianosaisen yksilöimiseksi tarpeelliset tiedot ovat heti julkisia.

Näiden syiden vuoksi oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain 5 §:n 2 momenttia ehdotetaan täydennettäväksi niin, että siinä mainittaisiin pakkokeinolain 10 luvussa, poliisilain 5 luvussa ja rikostorjunnasta Tullissa annetussa laissa tarkoitetun salaisen tiedonhankintakeinon lisäksi myös poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa ja sotilastiedustelusta annetussa laissa tarkoitetun tiedustelumenetelmän osalta, että perustiedot asiassa tulisivat julkiseksi vasta, kun tiedustelumenetelmän käytöstä on viimeistään ilmoitettava tiedonhankinnan kohteelle. Poliisilain 5 a luvun 46 §:ssä, tietoliikennetiedustelusta siviilitiedustelussa annetun lain 20 §:ssä ja sotilastiedustelusta annetun lain 87 §:ssä säädettäisiin kohteelle ilmoittamisesta. Jos ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä poliisilain 5 a luvun 46 §:n 2 momentin tai sotilastiedustelusta annetun lain 87 §:n 4 momentin nojalla, myöskään oikeudenkäynnin perustiedot eivät tulisi julkisiksi.

Momenttia tarkistettaisiin lisäksi niin, että jos henkilölle ilmoitetaan tiedustelumenetelmän käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, perustiedot tulevat julkiseksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Momentin sääntely siitä, että tuomioistuimella on harkintavalta oikeudenkäynnin perustietojen julkiseksi tulon ajankohdan aikaistamisessa, muttei sen myöhentämisessä, ulotettaisiin koskemaan myös tiedustelumenetelmän käyttöä.

Tullilain (1466/1994) 20 f § on kumottu lailla tullilain muuttamisesta 624/2015. Tullin osalta salaisista tiedonhankintakeinoista säädetään nykyään rikostorjunnasta Tullissa annetussa laissa. Momentissa oleva viittaus tullilain 20 f §:ään muutettaisiin sen vuoksi viittaukseksi rikostorjunnasta Tullissa annetun lain 3 lukuun.

12 §. *Asianosaisen oikeus tiedonsaantiin.* Momentin 3 kohtaa ehdotetaan täydennettäväksi niin, että asianosaisella ei olisi oikeutta saada tietoja oikeudenkäyntiasiakirjoista poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa tai sotilastiedustelusta annetussa laissa tarkoitettua tiedustelumenetelmää koskevassa asiassa, jossa tiedonhankinnan kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla. Nämä asiat rajattaisiin momentissa mainittujen salaista tiedonhankintakeinoa koskevien asioiden tavoin asianosaisen tiedonsaantioikeuden ulkopuolelle ajallisesti, kunnes ne tulevat julkiseksi oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain 16 §:n 4 momentin nojalla.

16 §. *Pakkokeinoasioiden julkisuus.* Pakkokeinoasioiden julkisuutta koskevassa pykälässä säädetään eräiden pakkokeinoasioiden osalta erityissäännöksiä käsittelyn, oikeudenkäyntiasiakirjojen ja ratkaisun julkisuudesta. Pakkokeinoasiaryhmää koskevat erityissäännökset on koottu tähän pykälään, koska keskeisiä pakkokeinoja on säännönmukaisesti käsiteltävä suullisessa käsittelyssä. Niin sanottua diaarijulkisuutta koskeva erityissäännös puolestaan tulisi sijoitettavaksi 5 §:n tarkistettuun 2 momenttiin, koska diaarijulkisuutta koskevat säännökset tulevat yleensä sovellettaviksi eri yhteydessä kuin muuta oikeudenkäynnin julkisuutta koskevat säännökset.

Tiedustelumenetelmän käytössä on kyse asioista, jotka ratkaistaan kuulematta sen kohteena olevaa henkilöä. Tämän vuoksi on välttämätöntä, ettei myöskään yleisöllä ole pääsyä mahdollisiin asian käsittelyä koskeviin istuntoihin tai saada tietoa istunnoissa annetuista ratkaisuista ja niiden sisältämistä asiakirjoista. Muussa tapauksessa tiedustelumenetelmän käytöltä menisi koko tarkoitus. Tämän vuoksi pykälän 4 momenttia ehdotetaan tarkistettavaksi siten, että myös poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa ja sotilastiedustelusta annetussa laissa tarkoitettua tiedustelumenetelmää koskeva asia, jossa tiedonhankinnan kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, käsiteltäisiin ja ratkaisu siinä annettaisiin yleisön läsnä olematta. Ratkaisun sisältävä ja muu oikeudenkäyntiasiakirja tulisivat julkisiksi, kun tiedustelumenetelmän käytöstä on viimeistään ilmoitettava sen kohteelle.

Momentissa säädettäisiin edelleen, että jos henkilölle ilmoitetaan tiedustelumenetelmän käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, oikeudenkäyntiasiakirjat tulisivat julkiseksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Tuomioistuimen harkintavalta aikaistaa oikeudenkäynnin perustietojen julkiseksi tulon ajankohtaa koskisi salaisen tiedonhankinnan ohella myös tiedustelumenetelmän käyttöä koskevia asioita.

Edellä 5 §:ää koskevien perustelujen yhteydessä mainitusta syystä tullilain 20 f §:n sijasta viitattaisiin rikostorjunnasta Tullissa annetun lain 3 lukuun.

2 Voimaantulo

Esitykseen sisältyvän poliisilain muuttamista koskevan lakiehdotuksen 5 a luvussa ehdotetaan säädettäväksi telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta (5 §), televalvonnasta (6 §), teknisestä kuuntelusta (10 §), lähetyksen jäljentämisestä (28 §) ja tietoliikennetiedustelusta, josta säädettäisiin kokonaan uudessa laissa tietoliikennetiedustelusta siviilitiedustelussa, liittyvät oikeusministeriön esitykseen perustuslakisääntelyn tarkistamisesta. Pe-

rustuslain 10 §:n 3 momentin tarkistamista koskeva oikeusministeriön ehdotus on käsiteltävä perustuslain 73 §:ssä säädetyssä järjestyksessä.

Jos perustuslain muutosehdotus käsiteltäisiin perustuslain 73 §:n 1 momentin mukaisessa säätämisjärjestyksessä, poliisilain 5 a luvun ja tietoliikennetiedustelusta siviilitiedustelussa annetun lain edellä mainitut säännökset voisivat tulla voimaan 1.1.2020.

Sen sijaan, jos perustuslain muutosehdotukset käsiteltäisiin perustuslain 73 §:n 2 momentin mukaisessa säätämisjärjestyksessä, poliisilain 5 a luku ja lakiehdotus tietoliikennetiedustelusta siviilitiedustelussa voisivat tulla voimaan vuonna 2018.

Lait ehdotetaan muilta kuin edellä mainituilta osin tulemaan voimaan mahdollisimman pian sen jälkeen kun ne on hyväksytty ja vahvistettu.

3 Suhde perustuslakiin ja säätämisjärjestys

3.1 Johdanto

Esitykseen sisältyy sääntelyä, joka on merkityksellistä perustuslaissa säädettyjen perusoikeuksien kannalta. Siviilitiedustelussa käytettävillä toimivaltuuksilla puututtaisiin monin paikoin yksilön perusoikeuksiin. Perustuslain kannalta merkityksellisimpiä ovat säännösehdotukset, joilla annetaan viranomaisille uusia yksilöön kohdistuvia toimivaltuuksia tai joilla muuten rajoitettaisiin yksilön oikeuksia ja toimintavapautta.

Vaikka tiedustelumenetelmien käytöllä puututtaisiin joihinkin perusoikeuksiin, kuten yksityiselämän suojaan, pyritään siviilitiedustelulain soveltamisella kuitenkin suojaamaan muita perusoikeuksia, kuten oikeutta elämään ja henkilökohtaiseen turvallisuuteen sekä valtiojärjestyksen perusteita, kuten valtion itsemääräämisoikeutta. Ihmisten kollektiivinen turvallisuus samoin kuin yhteiskunnan elintärkeät toiminnot ja järjestäytynyt yhteiskuntaelämä ovat niin tärkeitä suojeluintressejä, että tiedustelusääntelylle on olemassa painava yhteiskunnallinen tarve ja perusoikeusjärjestelmän kannalta hyväksyttävä peruste.

Siviilitiedustelussa saataisiin hankkia tietoa ainoastaan laissa tyhjentävästi luetelluista kohteista. Niistä ehdotetaan säädettäväksi niin yksilöidysti kuin tiedustelutoiminnan erityispiirteistä johtuen on mahdollista. Myös tiedustelumenetelmistä ehdotetaan säädettäväksi mahdollisimman täsmällisesti ja tarkkarajaisesti.

Koska tiedustelu voidaan osoittaa vain kansallisesta turvallisuudesta huolehtivalle viranomaiselle, siviilitiedustelu ehdotetaan osoitettavaksi yksinomaan suojelupoliisin tehtäväksi.

Lakiehdotuksia tarkastellaan lisäksi perusoikeuksien yleisten rajoitusedellytysten, sananvapauden, omaisuuden suojan ja oikeusturvan sekä perustuslain 124 §:n (Hallintotehtävän antaminen muulle kuin viranomaiselle) kannalta.

3.2 Toimivaltuussääntely perusoikeussäännösten kannalta

3.2.1 Yksityiselämän suoja

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta. 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 hä-

nen 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. Viestin sisällön lisäksi perustuslain säännökset suojaavat myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle.

Kotirauha

Perustuslain 10 §:n kannalta merkityksellisiä tiedustelumenetelmiä olisivat suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, peitetoiminta, valeosto ja paikkatiedustelu. Mitään edellä mainituista tiedustelumenetelmistä ei saisi kohdistaa vakituiseen asumiseen käytettävään tilaan, joskin peitetoiminta ja valeosto asunnossa olisi sallittua asuntoa käyttävän aktiivisella myötävaikutuksella. Ehdotettavilla tiedustelumenetelmillä ei näin ollen puututtaisi perustuslaissa tarkoitetun kotirauhan suojan ydinalueelle. Lähtökohtana olisi, ettei tässä mainittuja tiedustelumenetelmiä saisi kohdistaa asuntoon myöskään ulkomailla. Asunnon käyttötarkoituksen selvittäminen saattaa kuitenkin osoittautua mahdottomaksi tai kohtuuttoman vaikeaksi varsinkin heikommin kehittyneissä maissa. Mainittuja tiedustelumenetelmiä ei näin ollen voida pitää ongelmallisina perustuslain 10 §:n 1 momentissa turvatun kotirauhan kannalta.

Viestin salaisuus

Telekuuntelua ja tietojen hankkimista telekuuntelun sijasta, televalvontaa, teknistä kuuntelua, lähetyksen jäljentämistä ja tietoliikennetiedustelua olisi pidettävä merkittävänä puuttumisena perustuslain 10 §:n 2 momentissa turvattuun luottamuksellisen viestin salaisuuteen pois lukien tilanteet, joissa on kyse vieraan valtion sotilas- tai muun viranomaisorganisaation viestinnästä. Vaikka televalvontaa on aiemmin pidetty telekuuntelua vähäisempänä kajoamisena luottamuksellisen viestinnän suojaan, sähköisen viestinnän tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, ettei kategorinen erottelu suojan reuna- ja ydinalueeseen ole enää perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 6). Tietoliikennetiedustelun valtiosääntöoikeudellisessa tarkastelussa taas on huomioitava, että jo pääsy tietojen keräämiseen muodostaa puuttumisen yksityiselämän suojaan (Klass v. Saksa, Liberty ja muut v. Yhdistynyt Kuningaskunta).

Selvää joka tapauksessa on, että perustuslain 10 §:n 3 momentin nojalla ei ole mahdollista säätää sellaisista rajoituksista viestin salaisuuteen, joiden tarkoituksena ei olisi yksilöidyn rikoksen torjuminen, vaan laajemmalti kansallisen turvallisuuden kannalta välttämättömän tiedon hankkiminen vakavista uhkista. Näin ollen telekuuntelun ja sen sijasta tehtävän tietojen hankkimisen, televalvonnan, teknisen kuuntelun, lähetyksen jäljentämisen ja tietoliikennetiedustelun menetelmin tehtävästä tiedonhankinnasta kansallisen turvallisuuden suojaamiseksi olisi mahdollista säätää tavallisen lain säätämisjärjestyksessä vain perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskevan uuden rajoitusperusteen nojalla ja edellyttäen, että sääntely täyttää perusoikeuksien yleiset rajoitusedellytykset. Perustuslain 10 §:n 4 momenttiin ehdotetun tiedon hankkimista koskeva uusi rajoitusperuste ei mahdollista yleisestä, kohdentamattomasta ja kaiken kattavasta tietoliikenteen seurannasta säätämistä.

Tukiasematietojen hankkimista, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknistä katselua, teknistä seurantaa, peitetoimintaa, valeostoa ja paikkatiedustelua koskevassa sääntelyssä on otettu huomioon jäljempänä luvussa 3.2.3 mainitut perusoikeuksien yleiset rajoi-

tusedellytykset. Tämän vuoksi ja ottaen huomioon kyseisten menetelmien melko vähäisenä pidettävä puuttuminen luottamuksellisen viestin salaisuuteen tai tunnistamistietoihin, niitä on pidettävä ongelmattomina perustuslain 10.2 §:n kannalta.

3.2.2 Liikkumisvapaus

Perustuslain 9 §:ssä säädetään liikkumisvapaudesta. Säännöksen mukaan Suomen kansalaisella ja maassa laillisesti oleskelevalla ulkomaalaisella on vapaus liikkua maassa ja valita asuinpaikkansa. Liikkumisvapauden rajoitusten tulee perustua lakiin. Rajoitusten sallittavuutta arvioitaessa on kiinnitettävä huomiota myös Euroopan ihmisoikeussopimuksen 4 lisäpöytäkirjan 2 artiklaan, jonka 3 kappaleen mukaan liikkumisvapaudelle voidaan asettaa sellaisia rajoituksia, jotka ovat lainmukaisia ja välttämättömiä demokraattisessa yhteiskunnassa (HE 309/1993 vp). Perustuslain 9 §:n kannalta merkityksellisiä tiedustelumenetelmiä olisivat tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, tekninen katselu ja tekninen seuranta. Kyseiset menetelmät merkitsisivät melko vähäistä puuttumista liikkumisvapauteen suhteessa siihen rajoitusperusteen välttämättömyyteen, jota kansallinen turvallisuus kansanvaltaisessa yhteiskunnassa edustaa. Näin ollen tässä mainittuja tiedustelumenetelmiä koskevan sääntelyn ei arvioida olevan ongelmallinen liikkumisvapauden kannalta.

3.2.3 Perusoikeuksien yleiset rajoitusedellytykset

Välttämättömyys

Luottamuksellisen viestin salaisuuden suojan rajoittamisen olisi perustuslain 10 §:ään ehdotetun uuden 4 momentin mukaan oltava välttämätöntä. Tämä edellytys seuraa myös perusoikeuksien yleisistä rajoitusedellytyksistä. Arvioitaessa lakiehdotusten säännösten välttämättömyyttä on otettava huomioon, että luottamuksellisen viestin salaisuuden suojaan puuttuvalla tiedustelumenetelmällä saataisiin hankkia tietoa vain sellaisesta siviilitiedustelun kohteena olevasta toiminnasta (Poliisilaki 5 a luku 3 §), joka vakavasti uhkaa kansallista turvallisuutta. Siviilitiedustelun tiedustelumenetelmillä saataisiin hankkia tietoa terrorismista, ulkomaisesta tiedustelutoiminnasta, joukkotuhoaseiden ja kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä, kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminnasta, suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavasta toiminnasta, vieraan valtion toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille, kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä, kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaavasta toiminnasta, Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaavasta toiminnasta sekä yhteiskuntajärjestystä uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta.

Siviilitiedustelun kohteita koskevassa poliisilain 5 a luvun 3 §:ssä siis yksilöitäisiin ja konkretisoitaisiin perustuslain 10 §:ään uutena ehdotettavaan 4 momenttiin sisältyvää sääntelyä, jonka mukaan kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan kansanvaltaista valtio- ja yhteiskuntajärjestystä, yhteiskunnan perustoimintoja, suuren ihmismäärän henkeä tai terveyttä taikka kansainvälistä rauhaa ja turvallisuutta uhkaavaa toimintaa. Koska ensiksi mainitun säännöksen jokainen kohta olisi johdettavissa yhdestä tai useammasta kansallisen turvallisuuskäsitteen kattamasta suojeluintressistä, pykälän arvioidaan täyttävän sääntelyltä tältä osin korostuneet vaatimukset välttämättömyydestä ja ennakoitavuudesta.

Täsmällisyys ja tarkkarajaisuus

Tiedustelumenetelmien käytön yleiset edellytykset koottaisiin poliisilakiin ehdotettavan 5 a luvun 4 §:ään. Kaikkia tiedustelumenetelmiä koskeva yleinen edellytys olisi, että niiden käytöllä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka uhkaa kansallista turvallisuutta. Kyse olisi niin sanotusta perustellusta tuloksellisuusodotuksesta. Koska telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, suunnitelmallinen tarkkailu, tekninen kuuntelu, tekninen katselu, henkilön tekninen seuranta, tekninen laitetarkkailu, tietolähteen ohjattu käyttö ja paikkatiedustelu voivat sisältää merkittävää puuttumista yksityisen suojattuihin oikeushyviin, edellytyksenä olisi näiden menetelmien osalta myös, että niiden käytöllä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Peitetoiminnan ja valeoston käyttäminen edellyttäisi lisäksi, että se olisi välttämätöntä tiedon saamiseksi kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.

Tiedustelumenetelmien käyttöä koskevista erityisistä edellytyksistä säädettäisiin menetelmäkohtaisesti. Tiedustelumenetelmiä koskevasta sääntelystä käy ilmi muun muassa menetelmän käyttöä koskevan vaatimuksen tai päätöksen tietosisältö samoin kuin se, kuka tiedustelusta päättää sekä tiedustelua koskevan luvan, päätöksen tai määräyksen kesto.

Hyväksyttävyys ja suhteellisuus

Tiedustelumenetelmien käytössä tulee kunnioittaa perus- ja ihmisoikeuksia, suhteellisuusperiaatetta, vähimmän haitan periaatetta ja tarkoitussidonnaisuuden periaatetta. Perus- ja ihmisoikeuksien kunnioittamisen vaatimus merkitsee muun ohella sitä, että suojelupoliisin olisi tiedustelutoimivaltuuksia käyttäessään valittava perusteltavissa olevista tiedustelumenetelmistä se, joka parhaiten edistää näiden oikeuksien toteutumista. Suhteellisuusperiaate puolestaan edellyttäisi arvioimaan, onko tiedustelumenetelmän käyttö puolustettavaa suhteessa tiedustelutoimeksiannon tärkeyteen, kiireellisyyteen, tavoiteltavaan päämäärään ja muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin. EIT ja EU-tuomioistuin ovat ratkaisukäytännössään korostaneet suhteellisuusperiaatteen noudattamisen tärkeyttä erityisesti tietoliikennetiedustelun yhteydessä (Weber ja Saravia v. Saksa, Digital Rights Ireland). Tietoliikennetiedustelulta edellytettäisiin siksi viimesijaisuutta eli sitä, että tietojen hankkiminen muulla menetelmällä olisi mahdotonta tai kohtuuttoman vaikeaa. Vähimmän haitan periaatteesta johtuu, että suojelupoliisin toimenpiteillä ei kenenkään oikeuksiin saisi puuttua enempää eikä kenellekään saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tiedustelutehtävän suorittamiseksi. Selvää on, että suojelupoliisi saisi tarkoitussidonnaisuuden periaatteen mukaisesti käyttää tiedustelutoimivaltuuksiaan vain säädettyyn tarkoitukseen.

Oikeusturvajärjestelyt

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen riittävyys ja valvonnan tehokkuus. On tärkeää, että tiedusteluviranomaisella ei ole rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa. Yksi tapa rajoittaa viranomaisen harkintavaltaa on osoittaa vakavinta puuttumista perusoikeussuojaan tarkoittava tiedustelumenetelmien käytöstä päättäminen tuomioistuimelle. Ehdotuksen mukaan tuomioistuinlupaa edellyttäviä tiedustelumenetelmiä olisivat telekuuntelu ja tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, paikkatiedustelu ja tietoliikennetiedustelu. Lupa voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan pois lukien telekuuntelu ja sen sijasta toimitettava tietojen hankkiminen, jos kohteena on henkilö. Näissä tilanteissa lupa voitaisiin antaa enintään kolmeksi kuukaudeksi kerrallaan.

Säännösehdotuksilla kuuntelu- ja katselukiellosta, jäljentämis- ja tiedustelukiellosta, tiedustelutietojen hävittämisestä ja tiedustelumenetelmän käytöstä ilmoittamisesta turvattaisiin niin ikään oikeusturvan toteutumista. Oikeus saada tieto tiedustelun kohteeksi joutumisesta on tärkeää, jotta henkilö ylipäätään ymmärtäisi hakea oikeussuojaa. Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisestä tarkkailusta sekä tietoliikennetiedustelusta olisi viipymättä ilmoitettava kohteelle, kun tiedonhankinnan tarkoitus on saavutettu. Muiden menetelmien käytöstä olisi ilmoitettava, jos asiassa aloitetaan esitutkinta. Ehdotettu sääntely antaisi mahdollisuuden jokaiselle, joka epäilee joutuneensa yksityiselämän suojan loukkauksen kohteeksi, saada asiansa käsitellyksi asianmukaisesti tuomioistuimessa tai muussa viranomaisessa siten kuin perustuslain 21 §:ssä edellytetään.

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

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

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

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

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

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

3.3 Muu sääntely perustuslain kannalta

3.3.1 Sananvapaus ja oikeusturva

Poliisilain 5 a luvun 38 §:ssä ehdotetaan säädettäväksi tiedustelumenetelmää koskevasta ilmaisukiellosta. Suojelupoliisin päällikkö saisi säännöksen myötä tärkeästä kansalliseen turvallisuuteen liittyvästä syystä kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä. Nyt kyseessä olevan ilmaisukiellon ei voida katsoa rajoittavan perustuslain 12 §:n 1 momentissa turvattua sananvapautta ottaen huomioon perusoikeuden yleiset rajoitusedellytykset, erityisesti täsmällisyys- ja tarkkarajaisuusvaatimus sekä hyväksyttävyysvaatimus. Ilmaisukiellon määräämiselle asetettavat edellytykset yksilöityine ja kirjallisine ilmoituksineen määriteltäisiin yksityiskohtaisesti laissa. Ilmaisukieltoa on pidettävä myös välttämättömänä, koska tiedustelumenetelmän käytön tuleminen sivullisen välityksellä kohdehenkilön tietoon voisi estää keinon käytön tai vaarantaa sen tarkoituksen toteutumisen.

Ilmaisukieltoa koskevaan päätökseen ei saisi hakea muutosta valittamalla. Päätöksessä olisi mainittava valituskiellosta ja sen oikeudellisesta perusteesta. Ilmaisukiellon saanut saisi aina ilmoittaa ilmaisukiellosta tiedusteluvaltuutetulle. Koska suojelupoliisilla ei olisi käytännössä koskaan tarvetta, tai edes oikeutta, julkisesti tiedottaa ilmaisukiellon piiriin kuuluvista tiedustelumenetelmän käyttöä koskevista seikoista, sen määräämiseen ei liittyisi vastaavanlaista epäsuhtaa kuin mitä esitutkinnassa saattaa ilmetä tutkinnanjohtajan tiedottaessa seikoista, joista epäillylle tai tämän avustajalle on määrätty ilmaisukielto. Valituskielto ei loukkaisi perustuslain 21 §:n 2 momentissa turvattua muutoksenhakuoikeutta ottaen huomioon kiellon määräämiseltä edellytettävä painava syy ja kiellon kohdistuminen tiedustelumenetelmän käyttöä koskeviin seikkoihin.

Poliisilain 5 a luvun 39 §:ssä säänneltäisiin tiedustelumenetelmän käytöstä päättämisestä eräissä tapauksissa. Säännöksen mukaan muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättäisi suojelupoliisin päällikkö. Selvää on, että suomalainen virkamies ei voisi ulkomaillakaan toimia universaalien perus- ja ihmisoikeuksien vastaisesti. Tämän vuoksi ja ottaen huomioon, että tiedon saaminen tiedustelumenetelmän käytön kohteeksi joutumisesta on tärkeä oikeusturvatae, tiedustelumenetelmän käytöstä tulisi lähtökohtaisesti ilmoittaa myös ulkomailla toimittaessa. Aina tämä ei kuitenkaan ole mahdollista ja toisissa tilanteissa ilmoituksen tekeminen saattaisi paitsi haitata Suomen kansainvälisiä suhteita tai edellytyksiä toimia kansainvälisessä yhteistyössä, myös vaarantaa suojelupoliisin virkamiehen henkeä tai terveyttä. Mahdotonta ilmoittaminen voisi olla esimerkiksi hallinnoltaan sortuneissa tai hauraissa maissa, missä ei ole viranomaisten ylläpitämiä rekistereitä tai muitakaan keinoja selvittää tiedonhankinnan kohteen henkilöllisyyttä tai asuinpaikkaa. Näistä syistä johtuen ja palauttaen mieleen, että tiedustelumenetelmän käytöstä voidaan 46 §:n 2 momentin nojalla jättää ilmoitus kokonaan tekemättä myös Suomessa, aluksi mainittua pykälää ei voida sen harkinnanvaraisen ilmoitusjärjestelyn osalta pitää ongelmallisena perustuslain 21 §:ssä säädetyn oikeusturvan kannalta.

3.3.2 Omaisuuden suoja

Poliisilain 5 a luvun 50 §:ään ehdotetaan säännöstä tietojen saannista yksityiseltä yhteisöltä. Säännös antaisi suojelupoliisille oikeuden saada yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä tietoja, jos niiden voidaan olettaa olevan tarpeen kansalliseen turvallisuuteen kohdistuvan uhkan selvittämisessä. Säännös on merkityksellinen tietopyynnön kohteen kannalta, jotta tämä ei tietoa suojelupoliisille luovuttaessaan syyllistyisi salassapitorikokseen tai muuhun rangaistavaksi säädettyyn tekoon, vaan voisi päinvastoin luottaa toimivansa lain sallimalla

tavalla. Tietojen saantia yksityiseltä yhteisöltä koskeva säännös on ongelmaton paitsi perustuslain 10 §:n 1 momentissa turvatun yksityiselämän suojan kannalta myös 15 §:n 1 momentissa turvatun omaisuuden suojan kannalta ottaen huomioon ehdotetun pykälän taustalla vaikuttava välttämätön yhteiskunnallinen tarve, laissa säädetyn ilmaisuvelvollisuuden ennakoitavuus sitä koskevien tahojen kannalta ja pyyntöön liittyvän tuloksellisuusodotuksen sitominen täsmällisiin kriteereihin.

Poliisilain 5 a luvun 51 §:ään ehdotetaan otettavaksi säännös teleyrityksen avustamisvelvollisuudesta. Kyseinen avustamisvelvollisuus kattaisi muun muassa telekuuntelun ja televalvonnan edellyttämät kytkennät televerkkoon sekä tietojen, välineiden ja henkilöstön käyttöön antamisen telekuuntelun toimeenpanoa varten (HE 224/2010 vp s. 140). Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 21 §:ssä puolestaan ehdotetaan asetettavaksi tiedonsiirtäjän tietojenantovelvollisuus. Kyse olisi tiedonsiirtäjän velvollisuudesta antaa suojelupoliisille tietoliikennetiedustelun kohdentamiseksi tarpeelliset tiedot. 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 suojelupoliisille 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.

3.3.3 Hallintotehtävän antaminen muulle kuin viranomaiselle

Poliisilain 5 a luvun 55 §:ssä ehdotetaan säädettäväksi kansainvälisestä yhteistyöstä. Pykälän mukaan suojelupoliisi voisi tehdä yhteistyötä sekä suorittaa yhteisiä operaatioita ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa. Kansainvälisen avun antamista ja pyytämistä koskevasta päätöksenteosta säädetään erikseen siitä annetussa laissa 418/2017. Säännöksessä edellytettäisiin, että vieraan valtion virkamies olisi eräitä tiedustelumenetelmiä Suomessa käyttäessään velvollinen noudattamaan suojelupoliisin poliisimiehen antamia määräyksiä ja ohjeita. Tiedustelumenetelmien käyttö pysyisi näin ollen aina suomalaisen virkamiehen ohjauksessa ja valvonnassa. Selvää on lisäksi, että vieraan valtion virkamies olisi Suomessa toimiessaan rikos- ja vahingonkorvausoikeudellisen vastuun piirissä, jollei esimerkiksi hänen diplomaattiasemastaan muuta johtuisi. Näistä menettelytakeista ja vastuujärjestelyistä johtuen ehdotetun pykälän ei arvioida olevan ongelmallisessa suhteessa perustuslain 124 §:ssä säädettyyn vaatimukseen siitä, että merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan antaa vain viranomaiselle.

3.4 Säätämisjärjestyksen arviointi

Esitykseen sisältyvät lakiehdotukset voidaan hallituksen käsityksen mukaan käsitellä tavallisen lain säätämisjärjestyksessä lukuun ottamatta sellaisia toimivaltuuksia koskevia säännösehdotuksia, jotka merkitsevät puuttumista perustuslain 10 §:n 2 momentissa turvattuun luottamuksellisen viestin salaisuuteen.

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

Niistä olisi kuitenkin mahdollista säätää tavallisen lain säätämisjärjestyksessä perustuslain 10 §:n 4 momenttiin ehdotetun kansallista turvallisuutta koskevan uuden rajoitusperusteen nojalla.

Edellä luetellut toimivaltuudet kytkeytyvät ehdotettuun perustuslain muutokseen. Tämän vuoksi ja myös esitykseen liittyvien muiden valtiosääntöoikeudellisten näkökohtien vuoksi hallitus pitää tarkoituksenmukaisena, että eduskunta pyytää esityksestä perustuslakivaliokunnan lausunnon.

Kaikki tiedustelutoimintaan liittyvät hallituksen esitykset ovat riippuvaisia toisistaan, ja ne tulisi hallituksen käsityksen mukaan saattaa perustuslakivaliokunnan käsiteltäväksi yhdessä.

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

LUONNOS

Lakiehdotukset

1.

Laki

poliisilain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan poliisilain (872/2011) 1 luvun 1 §:n 1 momentti, 5 luvun 5 §:n 1 momentti, 7 §:n 1 momentti ja 3 momentin 6 kohta, 8 §:n 1momentti, 10 §:n 1—4 momentti ja 6 momentin 7 kohta, 12 §:n 1 momentti ja 3 momentin 5 kohta, 14 §:n 1 momentti ja 3 momentin 5 kohta, 16 §:n 1 momentti, 18 §:n 2 momentti ja 4 momentin 6 kohta, 20 §:n 1 ja 2 momentti sekä 4 momentin 6 kohta, 22 §:n 1 ja 2 momentti sekä 4 momentin 6 kohta, 24 §:n 1 momentti ja 3 momentin 6 kohta, 25 §:n 3 momentti, 32 §:n 1 momentti, 36 §:n 1 momentti ja 3 momentin 7 kohta, 38 §:n 1 momentti, 39 §:n 1 momentti, 40 §:n 1 momentti, 42 §:n 1 momentti, 44 §:n 1 momentti, 47 §:n 2 momentti, 48 §:n 1 momentti, 52 ja 57 §, 58 §:n 1 momentti, 61 §:n 2 momentti, 63 §:n 2 momentti, 9 luvun 8 §, 9 §:n 2 momentti, 10 §:n 2 momentin johdantokappale,
sellaisina kuin niistä ovat 10 §:n 3 momentti ja 6 momentin 7 kohta, 12 §:n 3 momentin 5 kohta, 18 §:n 4 momentin 6 kohta, 20 §:n 4 momentin 6 kohta, 22 §:n 4 momentin 6 kohta, 47 §:n 2 momentti ja 58 §:n 1 momentti laissa 1168/2013, sekä
lisätään lakiin uusi 5 a luku seuraavasti:

1 luku

Yleiset säännökset

1 §

Poliisin tehtävät

Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, kansallisen turvallisuuden suojaaminen, 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.
— —

5 luku

Salaiset tiedonhankintakeinot

5 §

Telekuuntelu ja sen edellytykset

Telekuuntelulla tarkoitetaan sähköisen viestinnän palveluista annetun lain (917/2014) 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 8 §:ssä tarkoitettujen tun-

nistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain siltä henkilöltä lähtöisin olevaan tai sellaiselle henkilölle tarkoitettuun viestiin, jonka voidaan perustellusti olettaa syyllistyvän 2 momentissa mainittuun rikokseen.

— —

7 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta pakkokeinolain 2 luvun 9 §:n 1 momentin 1 kohdassa tarkoitetun poliisimiehen (*pidättämiseen oikeutettu poliisimies*) taikka suojelupoliisin päällikön, apulaispäällikön, osastopäällikön, ylitarkastajan tai tarkastajan *(suojelupoliisin päällystöön kuuluva poliisimies)* vaatimuksesta.

— —

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 1 momentissa tarkoitettu poliisimies;

7) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

8 §

Televalvonta ja sen edellytykset

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 palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun tilaajaan tai mainitun pykälän 30 kohdassa tarkoitettuun käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

— —

10 §

Televalvonnasta päättäminen

Tuomioistuin päättää 8 §:n 2 ja 5 momentissa sekä 9 §:n 1, 4 ja 5 kohdassa tarkoitetusta televalvonnasta sekä televalvonnasta 3 §:ssä tarkoitetuissa tapauksissa pidättämiseen oikeutetun poliisimiehen taikka suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Jos 1 momentissa tarkoitettua muuta kuin 3 §:n nojalla suoritettavaa televalvontaa koskeva asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies 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.

Keskusrikospoliisin tai suojelupoliisin taikka poliisilaitoksen päällikkö päättää 8 §:n 4 momentissa tarkoitetusta televalvonnasta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies saa päättää televalvonnasta siihen asti, kunnes keskusrikospoliisin tai suojelupoliisin päällikkö taikka poliisilaitoksen päällikkö on ratkaissut televalvontaa koskevan asian. Asia on saatettava mainitun poliisimiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies päättää 8 §:n 3 momentissa ja 9 §:n 2 ja 3 kohdassa tarkoitetusta televalvonnasta.

— —

Televalvontaa 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 televalvonnan edellytykset perustuvat;

4) suostumus, jos se on televalvonnan käytön edellytys;

5) luvan voimassaoloaika kellonajan tarkkuudella;

6) toimenpiteen kohteena oleva teleosoite tai telepäätelaite;

7) televalvonnan suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;

8) mahdolliset televalvonnan rajoitukset ja ehdot.

12 §

Tukiasematietojen hankkimisesta päättäminen

Tuomioistuin päättää tukiasematietojen hankkimisesta pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva 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.

— —

Tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika taikka toimenpiteen perusteena oleva vaara;

2) tosiseikat, joihin tukiasematietojen hankkimisen edellytykset perustuvat;

3) ajanjakso, jota lupa koskee;

4) tukiasema, jota lupa koskee;

5) tukiasematietojen hankkimisen suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;

6) mahdolliset tukiasematietojen hankkimisen rajoitukset ja ehdot.

14 §

Suunnitelmallisesta tarkkailusta päättäminen

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies päättää suunnitelmallisesta tarkkailusta.

— —

Päätös suunnitelmallisesta tarkkailusta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpiteen perusteena oleva rikos ja sen tekoaika;
2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;
3) tosiseikat, joihin henkilöön kohdistuva epäily ja suunnitelmallinen tarkkailu perustuvat;
4) luvan voimassaoloaika;
5) suunnitelmallisen tarkkailun suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;
6) mahdolliset suunnitelmallisen tarkkailun rajoitukset ja ehdot.

16 §

Peitellystä tiedonhankinnasta päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies päättää peitellystä tiedonhankinnasta.

— —

18 §

Teknisestä kuuntelusta päättäminen

— —

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies päättää 17 §:n 5 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta.

— —

Teknistä kuuntelua 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 teknisen kuuntelun edellytykset perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) tila tai muu paikka, johon kuuntelu kohdistuu;
6) teknisen kuuntelun suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;
7) mahdolliset teknisen kuuntelun rajoitukset ja ehdot.

20 §

Teknisestä katselusta päättäminen

Tuomioistuin päättää teknisestä katselusta pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta, kun katselu kohdistuu rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan tilaan tai muuhun paikkaan taikka rikoksen johdosta vapautensa menettäneeseen henkilöön.

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies päättää 19 §:n 5 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä katselusta.

— —

Teknistä katselua 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 teknisen katselun edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) tila tai muu paikka, johon katselu kohdistuu;

6) teknisen katselun suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;

7) mahdolliset teknisen katselun rajoitukset ja ehdot.

22 §

Teknisestä seurannasta päättäminen

Tuomioistuin päättää henkilön teknisestä seurannasta pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva 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.

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies päättää 21 §:n 4 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta.

— —

Teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika tai toimenpiteen perusteena oleva vaara;

2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;

3) tosiseikat, joihin henkilöön kohdistuva epäily ja teknisen seurannan edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) toimenpiteen kohteena oleva esine, aine tai omaisuus;

6) teknisen seurannan suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;

7) mahdolliset teknisen seurannan rajoitukset ja ehdot.

24 §

Teknisestä laitetarkkailusta päättäminen

Tuomioistuin päättää teknisestä laitetarkkailusta pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva 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.

— —

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen tekoaika;

2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;

3) tosiseikat, joihin henkilöön kohdistuva epäily ja teknisen laitetarkkailun edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto;

6) teknisen laitetarkkailun suorittamista johtava ja valvova 7 §:n 1 momentissa tarkoitettu poliisimies;

7) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

25 §

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen

— —

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies.

32 §

Peitetoiminnasta päättäminen

Keskusrikospoliisin tai suojelupoliisin päällikkö päättää peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies.

— —

36 §

Valeostosta päättäminen

Keskusrikospoliisin tai suojelupoliisin päällikkö päättää valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies.

— —

Päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava:

LUONNOS

1) toimenpiteen perusteena oleva rikos;
2) valeoston kohteena oleva henkilö;
3) tosiseikat, joihin epäily ja valeoston edellytykset perustuvat;
4) valeoston kohteena oleva esine, aine, omaisuus tai palvelu;
5) valeoston tarkoitus;
6) päätöksen voimassaoloaika;
7) valeoston suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies;
8) mahdolliset valeoston rajoitukset ja ehdot.

38 §

Valeoston toteuttamista koskeva päätös

Päätös valeoston toteuttamisesta on tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies.
— —

39 §

Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa ja valeostossa

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava poliisimies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.
— —

40 §

Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun viranomaisen ulkopuoliselta henkilöltä (*tietolähde*).
— —

42 §

Tietolähteen ohjatusta käytöstä päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies päättää tietolähteen ohjatusta käytöstä.
— —

44 §

Valvotusta läpilaskusta päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies päättää poliisin suorittamasta valvotusta läpilaskusta. Muiden viranomaisten valvottua läpilaskua koskevasta päätöksenteosta säädetään erikseen.

— —

47 §

Suojaamisesta päättäminen

— —

Salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu tai suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta tiedonhankinnan suojaamisesta.

— —

48 §

Salaista tiedonhankintaa koskeva ilmaisukielto

Pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies saa tärkeästä rikoksen estämiseen tai paljastamiseen liittyvästä syystä kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja salaisen tiedonhankintakeinon käytöstä. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan salaisen tiedonhankintakeinon käytön toteuttamisessa.

— —

52 §

Tallenteiden tutkiminen

Salaisen tiedonhankintakeinon käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies. Pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

57 §

Kiireellisessä tilanteessa saadun tiedon hävittäminen

Jos pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies on 10 §:n 2 momentissa, 12 §:n 1 momentissa, 22 §:n 1 momentissa tai 24 §:n 1 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, henkilön teknisen seurannan tai teknisen laitetarkkailun aloittamisesta, mutta tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedonhankinnan käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin ylimääräistä tietoa saadaan käyttää 54 §:n mukaan.

58 §

Salaisen tiedonhankintakeinon käytöstä ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, teknisestä tarkkailusta ja valvotusta läpilaskusta on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu. Salaisen tiedonhankintakeinon käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

— —

61 §

Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin

— —

Poliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin teleyrityksen hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies. Kotietsinnästä säädetään erikseen.

63 §

Salaisen tiedonhankinnan valvonta

— —

Sisäministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta.

— —

5 a luku

Siviilitiedustelun tiedustelumenetelmät

1 §

Siviilitiedustelu

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

2 §

Tiedustelumenetelmät

Tiedustelumenetelmiä ovat 5 luvussa tarkoitetut telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja ohjattu tietolähdetoiminta.

Tiedustelumenetelmiä ovat myös tässä luvussa tarkoitetut paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten ja tietojen saanti yksityiseltä yhteisöltä.

Tässä luvussa säädetään siitä, millä edellytyksillä 1 momentissa tarkoitettuja tiedustelumenetelmiä sekä paikkatiedustelua, jäljentämistä, lähetyksen pysäyttämistä jäljentämistä varten ja tietojen saantia yksityiseltä yhteisöltä käytetään siviilitiedustelussa.

Tietoliikennetiedustelusta tiedustelumenetelmänä siviilitiedustelussa säädetään tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa (/).

3 §

Siviilitiedustelun kohteet

Tiedustelumenetelmällä saadaan hankkia tietoa:

1) terrorismista;

2) ulkomaisesta tiedustelutoiminnasta;

3) joukkotuhoaseiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;

4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1992) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;

5) kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminnasta;

6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavasta toiminnasta;

7) vieraan valtion toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille;

8) kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä;

9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaavasta toiminnasta;

10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaavasta toiminnasta; sekä

11) yhteiskuntajärjestystä uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta.

4 §

Tiedustelumenetelmien käytön edellytykset

Tiedustelumenetelmän käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Sen lisäksi, mitä tiedustelumenetelmien käytön erityisistä edellytyksistä jäljempänä säädetään, telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitetusta toiminnasta. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että menetelmän käyttö on välttämätöntä. Peitetoiminnan käyttäminen edellyttää myös, että tiedonhankintaa on toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena.

Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan tai siihen rinnastuvan tahoon, tiedustelumenetelmän käytön edellytyksistä säädetään 1 momentissa.

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

Tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

5 §

Tiedonhankinnan jatkaminen eräiden rikosten estämiseksi ja paljastamiseksi

Jos tiedustelumenetelmän käytön aikana ilmenee, että henkilön voidaan perustellusti olettaa syyllistyvän 5 luvun 3 §:ssä mainittuun rikokseen taikka valtiopetokseen, törkeään valtiopetokseen tai laittomaan sotilaalliseen toimintaan tai voidaan olettaa, että sellainen rikos on tehty eikä tiedustelumenetelmän käytöllä enää voida olettaa saatavan tietoja luvan tai päätöksen perusteena olevasta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, suojelupoliisi saa jatkaa tiedustelumenetelmän käyttöä 5 luvussa tarkoitettuna salaisena tiedonhankintana rikoksen estämiseksi ja paljastamiseksi tämän luvun nojalla annetun luvan voimassaolon ajan, enintään kuitenkin kuukauden ajan. Jos rikoksen estämiseksi tai paljastamiseksi on tarpeen käyttää 5 luvussa tarkoitettua salaista tiedonhankintakeinoa, asia on saatettava mainitun ajan kuluessa sen viranomaisen ratkaistavaksi, joka on toimivaltainen päättämään kysymyksessä olevan tiedonhankintakeinon käyttämisestä.

6 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Lupa telekuunteluun tai tietojen hankkimiseen telekuuntelun sijasta voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Silloin, kun toimenpiteen kohteena on henkilö, lupa voidaan antaa enintään kolmeksi kuukaudeksi kerrallaan.

Telekuuntelua ja telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite;

3) tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuvat;

4) telekuuntelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;

5) telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

7 §

Televalvonnasta päättäminen

LUONNOS

Tuomioistuin päättää televalvonnasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos televalvontaa koskeva asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Suojelupoliisi saa tietojen hankkimiseksi siviilitiedustelun kohteena olevasta toiminnasta kohdistaa televalvontaa henkilön suostumuksella tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen.

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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) toimenpide, sen tavoite sekä 3 §:ssä tarkoitettu toiminta;
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 suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset televalvonnan rajoitukset ja ehdot.

8 §

Tukiasematietojen hankkimisesta päättäminen

Tuomioistuin päättää tukiasematietojen hankkimisesta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä suojelupoliisin päällystöön kuuluva 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.

Lupa annetaan tietyksi ajanjaksoksi.

Tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;
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 suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset tukiasematietojen hankkimisen rajoitukset ja ehdot.

9 §

Suunnitelmallisesta tarkkailusta päättäminen

Suojelupoliisin päällystöön kuuluva poliisimies päättää suunnitelmallisesta tarkkailusta.
Suunnitelmallista tarkkailua koskeva päätös voidaan tehdä kerrallaan enintään kuudeksi kuukaudeksi.
Päätös suunnitelmallisesta tarkkailusta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) 3 §:ssä tarkoitettu toiminta;
2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä;
3) tosiseikat, joihin suunnitelmallisen tarkkailun edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaoloaika;
5) suunnitelmallisen tarkkailun suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset suunnitelmallisen tarkkailun rajoitukset ja ehdot.

10 §

Peitellystä tiedonhankinnasta päättäminen

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää peitellystä tiedonhankinnasta.
Päätös peitellystä tiedonhankinnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpide ja sen tavoite riittävästi yksilöityinä;
2) 3 §:ssä tarkoitettu toiminta;
3) toimenpiteen kohteena oleva henkilö tai henkilöryhmä;
4) tosiseikat, joihin peitellyn tiedonhankinnan edellytykset ja kohdistaminen perustuvat;
5) peitellyn tiedonhankinnan suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;
6) toimenpiteen suunniteltu toteuttamisajankohta;
7) 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.

11 §

Teknisestä kuuntelusta päättäminen

Tuomioistuin päättää vapautensa menettäneen henkilön teknisestä kuuntelusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.
Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta.
Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.
Teknistä kuuntelua koskevassa vaatimuksessa ja päätöksessä on mainittava:
1) 3 §:ssä tarkoitettu toiminta;
2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä taikka tila tai muu paikka;
3) tosiseikat, joihin teknisen kuuntelun edellytykset ja kohdistaminen perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) teknisen kuuntelun suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset teknisen kuuntelun rajoitukset ja ehdot.

12 §

Teknisestä katselusta päättäminen

Tuomioistuin päättää vapautensa menettäneen henkilön teknisestä katselusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää teknisestä katselusta 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.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä taikka tila tai muu paikka;

3) tosiseikat, joihin teknisen katselun edellytykset ja kohdistaminen perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) teknisen katselun suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset teknisen katselun rajoitukset ja ehdot.

13 §

Teknisestä seurannasta päättäminen

Tuomioistuin päättää henkilön teknisestä seurannasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva 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.

Suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta.

Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva 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 suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset teknisen seurannan rajoitukset ja ehdot.

14 §

Teknisestä laitetarkkailusta päättäminen

Tuomioistuin päättää teknisestä laitetarkkailusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, suojelupoliisin päällystöön kuuluva 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.

Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;
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 suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

15 §

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen

Suojelupoliisi saa hankkia teknisellä laitteella teleosoitteen tai telepäätelaitteen yksilöintitiedot.

Viestintävirasto tarkastaa, ettei tekninen laite ominaisuuksiensa vuoksi aiheuta haitallista häiriötä yleisen viestintäverkon laitteille tai palveluille.

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää suojelupoliisin päällystöön kuuluva poliisimies.

16 §

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Suojelupoliisin palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan ja tekniseen laitetarkkailuun, käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos mainitun tiedustelumenetelmän käytön toteuttaminen sitä edellyttää. Suojelupoliisin palveluksessa olevalla 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.

Telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan ja tekniseen laitetarkkailuun käytettävän laitteen, menetelmän tai ohjelmiston saa asentaa vakituiseen asumiseen käytettävään tilaan vain, jos tuomioistuin on antanut siihen luvan suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Edellä 1 momentissa tarkoitetun toimenpiteen kohteena ei saa olla sellainen esine, aine, omaisuus, tila tai muu paikka, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11–14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta. tai johon ei pakkokeinolain 7 luvun 3 §:n nojalla saa kohdistaa takavarikkoa tai asiakirjan jäljentämistä, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

17 §

Peitetoimintaa koskeva esitys ja suunnitelma

Peitetoimintaa koskevassa esityksessä on mainittava:
1) toimenpiteen esittäjä;
2) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöityinä;
3) 3 §:ssä tarkoitettu toiminta;
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.

18 §

Peitetoiminnasta päättäminen

Suojelupoliisin päällikkö päättää 16 §:ssä tarkoitetusta peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää suojelupoliisin päällikkö taikka tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös peitetoiminnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpiteen esittäjä;
2) peitetoiminnan toteuttamisesta vastaava poliisimies;
3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä;
4) 3 §:ssä tarkoitettu toiminta;
5) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöityinä;
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.

19 §

Rikoksentekokielto

Peitetoimintaa suorittava suojelupoliisin poliisimies ei saa tehdä rikosta eikä aloitetta rikoksen tekemiseen.

Jos peitetoimintaa suorittava suojelupoliisin poliisimies tekee liikennerikkomuksen, järjestysrikkomuksen tai muun niihin rinnastettavan rikoksen, josta on säädetty rangaistukseksi rikesakko, hän on rangaistusvastuusta vapaa, jos teko on ollut välttämätön peitetoiminnan tavoitteen saavuttamiseksi tai tiedonhankinnan paljastumisen estämiseksi.

20 §

LUONNOS

Valeostosta päättäminen

Suojelupoliisin päällikkö päättää valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Valeostoa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;
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.

21 §

Valeoston toteuttamista koskeva suunnitelma

Valeoston toteuttamisesta on laadittava kirjallinen suunnitelma, jos se on tarpeen toiminnan laajuuden tai muun vastaavan syyn vuoksi.

Valeoston toteuttamista koskevaa suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

22 §

Valeoston toteuttamista koskeva päätös

Päätös valeoston toteuttamisesta on tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Päätöksessä on mainittava:

1) valeostosta päättänyt poliisimies, päätöksen antopäivä ja sisältö;
2) tunnistetiedot valeoston suorittavista poliisimiehistä;
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.

23 §

Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa, valeostossa ja tietolähdetoiminnassa

Suojelupoliisin päällystöön kuuluva poliisimies saa päättää, että tässä luvussa tarkoitettua peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava sekä tietolähdetoimintaa valmisteleva tai toteuttava poliisimies 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 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.

24 §

Tietolähteen ohjatusta käytöstä päättäminen

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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) tiedonhankinnan toteuttamisesta vastaava poliisimies;
3) tunnistetiedot tietolähteestä;
4) 3 §:ssä tarkoitettu toiminta;
5) tiedonhankinnan tavoite ja toteuttamissuunnitelma;
6) päätöksen voimassaoloaika;
7) mahdolliset tietolähteen ohjatun käytön rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Tietolähteen ohjatun käytön lopettamisesta on tehtävä kirjallinen päätös.

Tietolähdettä koskevien tietojen tallettamisesta henkilörekisteriin ja palkkion maksamisesta säädetään 5 luvun 41 §:ssä.

25 §

Tietolähteen turvaaminen

Suojelupoliisi 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.

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.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää, että tietolähde tämän suostumuksella varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on yksittäistapauksessa välttämätöntä hänen turvallisuutensa varmistamiseksi. Kuuntelu ja katselu saadaan tallentaa. Tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita tietolähteen turvaamiseen.

26 §

Paikkatiedustelu

Paikkatiedustelulla tarkoitetaan muussa kuin vakituiseen asumiseen käytettävässä tilassa tai sellaisessa tilassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

27 §

Paikkatiedustelusta päättäminen

Tuomioistuin päättää paikkatiedustelusta, kun se kohdistuu kotirauhan suojaamaan paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana, tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Jos 1 momentissa tarkoitettu asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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) 3 §:ssä tarkoitettu toiminta;
2) paikkatiedustelun kohteena oleva paikka;
3) ne tosiseikat, 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.

Jos paikkatiedustelun aikana ilmenee, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti lopetettava ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

28 §

Jäljentäminen

Suojelupoliisilla on oikeus jäljentää asiakirja tai esine.

29 §

Jäljentämiskiellot

LUONNOS

Asiakirjaa tai muuta 26 §:ssä tarkoitettua kohdetta ei saa jäljentää, jos se sisältää tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 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, 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.

30 §

Telekuunteluun, televalvontaan ja tukiasematietoihin liittyvät jäljentämiskiellot

Sähköisen viestinnän palveluista annetun lain 3 §:n 27 kohdassa tarkoitetun teleyrityksen (*teleyritys*) tai mainitun lain 3 §:n 36 kohdassa tarkoitetun yhteisötilaajan 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.

31 §

Lähetyksen jäljentäminen

Suojelupoliisilla on oikeus jäljentää kirje tai muu lähetys ennen sen saapumista vastaanottajalle.

32 §

Lähetyksen pysäyttäminen jäljentämistä varten

Jos on syytä olettaa, että kirje tai muu lähetys, joka voidaan jäljentää, on tulossa postin toimipisteeseen, rautatieliikennepaikkaan tai sen osaan tai lähetysten kuljetusta ammatikseen liikennöinnin yhteydessä tai muuten harjoittavan toimipaikkaan taikka on jo siellä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa määrätä lähetyksen pidettäväksi mainitussa toimipaikassa, kunnes jäljentäminen on ehditty suorittaa.

Määräys annetaan enintään kuukauden määräajaksi, joka alkaa siitä, kun toimipaikan esimies on saanut tiedon määräyksestä. Lähetystä ei saa ilman 1 momentissa tarkoitetun virkamiehen lupaa luovuttaa muulle kuin hänelle tai hänen määräämälleen henkilölle.

Toimipaikan esimiehen on heti ilmoitettava määräyksen antajalle lähetyksen saapumisesta. Tämän on ilman aiheetonta viivytystä päätettävä jäljentämisestä.

33 §

Jäljentämisestä päättäminen

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää jäljentämisestä.

Jos asia ei siedä viivytystä, myös muu kuin 1 momentissa tarkoitettu suojelupoliisin poliisimies saa yksittäistapauksessa päättää jäljentämisestä, kunnes 1 momentissa tarkoitettu poliisimies on ratkaissut asian. Asia on saatettava 1 momentissa tarkoitetun poliisimiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedonhankintakeinon käytön aloittamisesta.

34 §

Jäljennöksen hävittäminen

Jäljennös on hävitettävä viipymättä, jos käy ilmi, että jäljentäminen on kohdistunut jäljentämiskiellon alaiseen materiaaliin tai tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi.

35 §

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 tiedustelumenetelmäkohtaisesti. 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 suullisesta 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.

36 §

Siviilitiedustelun suojaaminen

Suojelupoliisi 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 siviilitiedustelun suojaamiseksi.

Edellä 1 momentissa tarkoitettu rekisterimerkintä on oikaistava sen jälkeen, kun momentissa tarkoitettuja edellytyksiä ei enää ole.

37 §

Suojaamisesta päättäminen

Suojelupoliisin päällikkö päättää 36 §:n 1 momentissa tarkoitetun rekisterimerkinnän tekemisestä sekä asiakirjan valmistamisesta.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 36 §:n 1 momentissa tarkoitetusta suojaamisesta.

Rekisterimerkintöjen tekemisestä sekä asiakirjojen valmistamisesta päättäneen viranomaisen on pidettävä luetteloa merkinnöistä ja asiakirjoista, valvottava niiden käyttöä sekä huolehdittava merkintöjen oikaisemisesta.

38 §

Ilmaisukielto

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä, jos se on perusteltua tiedustelumenetelmän käytön suojaamiseksi. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytön toteuttamisessa.

Ilmaisukielto annetaan enintään vuodeksi kerrallaan. Kielto on annettava saajalleen kirjallisena todisteellisesti tiedoksi. Siinä on yksilöitävä kiellon kohteena olevat seikat, mainittava kiellon voimassaoloaika ja ilmoitettava sen rikkomiseen liittyvästä rangaistusuhasta.

Ilmaisukieltoa koskevaan päätökseen ei saa hakea muutosta valittamalla. Kiellon saanut saa kuitenkin ilman määräaikaa kannella Helsingin hovioikeudelle. Kantelu on käsiteltävä kiireellisenä.

Rangaistus ilmaisukiellon rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

Ilmaisukiellon saanut saa 4 momentin estämättä ilmoittaa ilmaisukiellosta tiedusteluvaltuutetulle.

39 §

Tiedustelumenetelmän käytöstä päättäminen eräissä tapauksissa

Muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättää suojelupoliisin päällikkö.

Tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatetaan mitä esityksestä, suunnitelmasta, vaatimuksesta tai päätöksestä tässä luvussa säädetään.

Tämän luvun 4 §:n 4 momentin, 41, 44, 46 ja 47 §:n säännöksiä voidaan soveltaa 1 momentissa tarkoitettuun siviilitiedusteluun ja tiedustelumenetelmän käyttöön.

40 §

Määräaikojen laskeminen

Tässä luvussa tarkoitettujen määräaikojen laskemiseen ei sovelleta säädettyjen määräaikain laskemisesta annettua lakia (150/1930).

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.

41 §

Kuuntelu- ja katselukiellot

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua ja teknistä katselua ei saa kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16, 20 tai 22 §:n 2 momentin nojalla.

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.

Tässä pykälässä tarkoitetut kuuntelu- ja katselukiellot eivät kuitenkaan koske tapauksia, joissa 1 momentissa tarkoitettu henkilö osallistuu siviilitiedustelun kohteena olevaan toimintaan, joka vakavasti uhkaa kansallista turvallisuutta ja myös hänen osaltaan on tehty päätös telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, teknisestä kuuntelusta tai teknisestä katselusta.

42 §

Tallenteiden ja asiakirjojen tarkastaminen

Suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen on ilman aiheetonta viivytystä tarkastettava tiedustelumenetelmän käytössä kertyneet tallenteet ja asiakirjat.

43 §

Tallenteiden tutkiminen

Tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja suojelupoliisin päällystöön kuuluva poliisimies. Suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

44 §

Tiedon luovuttaminen rikostorjuntaan

LUONNOS

Suojelupoliisin on ilman aiheetonta viivytystä ilmoitettava keskusrikospoliisille, jos tiedustelumenetelmän käytön aikana ilmenee, että voidaan olettaa tehdyksi sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Ilmoitusta saadaan suojelupoliisin päällikön päätöksellä siirtää enintään vuodeksi kerrallaan, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Suojelupoliisi saa ilmoittaa tehdystä rikoksesta keskusrikospoliisille, jos rikoksesta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta.

Suojelupoliisin on viipymättä ilmoitettava toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee, että hankkeilla on sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä. Tiedustelumenetelmän käytöllä saatua tietoa saa luovuttaa toimivaltaiselle viranomaiselle sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Kun harkitaan 1 momentissa tarkoitettua ilmoituksen siirtämistä tai 1 ja 2 momentissa tarkoitettua ilmoituksen tekemistä tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta tai sellaisen rikoksen estämisestä, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta, arvioinnissa on otettava huomioon rikoksen selvittämisen tai rikoksen estämisen merkitys yleisen ja yksityisen edun kannalta.

Tiedustelumenetelmän käytöllä saatua tietoa saa aina luovuttaa syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Jos esitutkintaviranomainen käynnistää esitutkinnan tai ryhtyy esitutkintatoimenpiteen käyttämiseen taikka toimivaltainen viranomainen käynnistää rikoksen estämiseen tähtäävän toimenpiteen tässä pykälässä tarkoitetun ilmoituksen perusteella, on esitutkintaviranomaisen tai toimivaltaisen viranomaisen ennen esitutkinnan käynnistämistä tai esitutkintatoimenpiteen käyttämistä taikka rikoksen estämiseen tähtäävän toimenpiteen käynnistämistä ilmoitettava siitä suojelupoliisille.

45 §

Tiedustelutietojen hävittäminen

Tiedustelumenetelmällä saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi.

Tieto voidaan kuitenkin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin, jos tämä on tarpeen 44 §:ssä tarkoitetuissa tapauksissa.

Edellä 7 §:ssä tarkoitetut tukiasematiedot on hävitettävä, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi.

46 §

Kiiretilanteessa saadun tiedon hävittäminen

Jos suojelupoliisin päällystöön kuuluva poliisimies on 7 §:n 1 momentissa, 8 §:n 1 momentissa, 11 §:n 1 momentissa, 12 §:n 1 momentissa, 13 §:n 1 momentissa, 14 §:n 1 momentissa tai 27 §:n 2 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, teknisen kuuntelun, teknisen katselun, henkilön teknisen seurannan, teknisen laitetarkkailun tai paikkatiedustelun 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. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että

LUONNOS

hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

Jos suojelupoliisin poliisimies on 33§:n 2 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt jäljentämisestä, mutta tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

47 §

Tiedustelumenetelmän käytöstä ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä tai viestiin kohdistuvasta lähetyksen jäljentämisestä on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu. Tiedustelumenetelmän käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

Tuomioistuin voi suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Jos tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Jos suojelupoliisi jatkaa tiedonhankintaa 5 §:n perusteella, noudatetaan mitä salaisen tiedonhankintakeinon käytöstä ilmoittamisesta 5 luvun 58 §:ssä säädetään.

Suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain 10 luvun 60 §:n 2–7 momentissa säädetään.

Tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, kun tiedonhankinnan kohteena on ollut 4 §:n 3 momentissa mainittu valtiollinen toimija.

Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan mitä 35 §:ssä säädetään.

48 §

Pöytäkirja

Tiedustelumenetelmän käytön lopettamisen jälkeen on laadittava ilman aiheetonta viivytystä pöytäkirja.

49 §

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 luvussa tarkoitetun tiedustelumenetelmän käytöstä, ennen kuin 47 §:ssä tarkoitettu ilmoitus on tehty.

Rekisteröidyn tarkastusoikeudesta säädetään henkilötietojen käsittelystä poliisitoimessa annetussa laissa.

50 §

Tietojen saanti yksityiseltä yhteisöltä

Suojelupoliisilla on suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä sellaisia tietoja, joiden yksittäistapauksessa voidaan olettaa olevan tarpeen sellaisen siviilitiedustelun kohteena olevan toiminnan selvittämisessä, joka vakavasti uhkaa kansallista turvallisuutta, ja jolla voidaan olettaa olevan merkitystä:

1) siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi, tavoittamiseksi tai yhteystietojen selvittämiseksi taikka tällaisen henkilön liikkumisen selvittämiseksi;

2) tiedustelumenetelmän käytön kohdentamiseksi tiettyyn siviilitiedustelun kohteena olevaan henkilöön; tai

3) siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön 3 §:ssä tarkoitettuun toimintaan oletettavasti kytkeytyvän taloudellisen toiminnan selvittämiseksi.

51 §

Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin

Teleyrityksen avustamisvelvollisuuteen sovelletaan mitä 5 luvun 61 §:ssä säädetään teleyrityksen avustamisvelvollisuudesta ja pääsystä eräisiin tiloihin.

52 §

Korvaus teleyritykselle

Teleyrityksen oikeudesta korvaukseen sovelletaan mitä 5 luvun 62 §:ssä säädetään korvauksesta teleyritykselle.

53 §

Teleyrityksen säilyttämien tietojen käyttäminen

Sen lisäksi mitä sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentissa säädetään säilytettävien tietojen käyttämisestä, säilytettäviä tietoja saadaan käyttää myös, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

54 §

Yhteistyö sotilastiedusteluviranomaisen kanssa

Suojelupoliisin on toimittava yhteistyössä sotilastiedusteluviranomaisen kanssa tiedustelun tarkoituksenmukaiseksi hoitamiseksi sekä annettava sotilastiedusteluviranomaiselle tässä tarkoituksessa tarpeellisia tietoja sen estämättä mitä salassapitovelvollisuudesta säädetään.

55 §

Yhteistyö muiden viranomaisten ja yhteisöjen kanssa

Suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi.

Suojelupoliisi voi tehtävänsä toteuttamiseksi toimia yhteistyössä yhteisöjen kanssa sekä luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi.

Tietojen luovuttamisesta rikostorjuntaan säädetään 44 §:ssä.

56 §

Salaisen tiedonhankinnan yhteensovittaminen

Tässä luvussa säädettyjen tiedustelumenetelmien käyttöä voidaan yhteen sovittaa suojelupoliisin, sotilastiedusteluviranomaisen, keskusrikospoliisin ja muun viranomaisen virkamiesten työturvallisuuden varmistamiseksi sekä salaisessa tiedonhankinnassa käytettävien taktisten ja teknisten menetelmien ja suunnitelmien paljastumisen estämiseksi.

57 §

Kansainvälinen yhteistyö

Suojelupoliisi voi tehdä yhteistyötä sekä toteuttaa tiedonhankintaa yhdessä ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa kansallisen turvallisuuden suojaamiseksi.

Jos yhteinen tiedonhankinta toteutetaan yhteistyössä sen valtion kanssa, jonka alueella tiedustelumenetelmiä on tarkoitus käyttää, suojelupoliisin poliisimiehen on noudatettava niitä rajoituksia ja ehtoja tiedustelumenetelmien käytölle, jotka kyseinen valtio asettaa.

Suojelupoliisin päällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja tiedustelumenetelmien käytöstä. Vieraan valtion toimivaltaisella virkamiehellä on suojelupoliisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä.

Suojelupoliisi voi salassapitosäännösten estämättä luovuttaa tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua.

Henkilötietojen luovuttamiseen sovelletaan henkilötietojen käsittelystä poliisitoimessa annettua lakia (761/2003).

58 §

Tiedustelutoiminnan yhteensovittaminen

Siviili- ja sotilastiedustelutoimintaa sovitetaan yhteen tasavallan presidentin, valtioneuvoston kanslian, ulkoasiainministeriön, puolustusministeriön ja sisäministeriön sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken.

Jos siviilitiedustelutoiminnalla arvioidaan olevan ulko- ja turvallisuuspoliittisia vaikutuksia, asia on valmistelevasti käsiteltävä 1 momentissa tarkoitettujen viranomaisten kesken.

59 §

Siviilitiedustelun valvonta sisäasiainhallinnossa

Tässä luvussa tarkoitettua tiedonhankintaa valvoo suojelupoliisin päällikkö sekä sisäministeriö.

60 §

Siviilitiedustelun ulkoinen valvonta

Sisäministeriön on annettava eduskunnan oikeusasiamiehelle ja tiedusteluvaltuutetulle vuosittain kertomus tässä luvussa tarkoitettujen tiedustelumenetelmien ja siviilitiedustelun suojaamisen käytöstä ja valvonnasta.

Tiedusteluvaltuutetun harjoittamasta valvonnasta säädetään tiedustelutoiminnan valvonnasta annetussa laissa (/).

61 §

Tiedusteluvaltuutetulle tehtävät ilmoitukset

Suojelupoliisin on annettava tieto tiedusteluvaltuutetulle tämän luvun nojalla annetuista tuomioistuimen päätöksistä ja luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen.

Suojelupoliisin on mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee:

1) muuta kuin 1 momentissa tarkoitettua tiedustelumenetelmää;
2) siviilitiedustelun suojaamista;
3) ilmaisukieltoa;
4) 44 §:n 1 momentissa tarkoitetun ilmoituksen siirtämistä.

Tiedustelumenetelmää koskevan päätöksen ilmoittamisessa on kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

62 §

Tarkemmat säännökset

LUONNOS

Valtioneuvoston asetuksella voidaan säätää:
1) tiedustelumenetelmien käytön ja niiden suojaamisen järjestämisestä;
2) toimenpiteiden kirjaamisesta valvontaa varten;
3) siviilitiedustelun valvontaa varten annettavista selvityksistä;
4) rikostorjuntaan luovutettavan tiedon siirtämistä koskevasta menettelystä ja siinä yhteydessä annettavista tarpeellisista tiedoista;
5) suojelupoliisin ja sotilastiedusteluviranomaisen välisen yhteistyön järjestämisestä;
6) suojelupoliisin ja muiden viranomaisten välisen yhteistyön järjestämisestä;
7) salaisen tiedonhankinnan yhteensovittamisen järjestämisestä;
8) tiedustelutoiminnan yhteensovittamisen järjestämisestä.
Sisäministeriön asetuksella voidaan säätää:
1) siviilitiedustelun valvonnan järjestämisestä sisäasiainhallinnossa;
2) suojelupoliisin ja muun sisäasiainhallinnon välisen yhteistyön järjestämisestä;
3) suojelupoliisin kansainvälisen yhteistyön järjestämisestä.

9 luku

Erinäiset säännökset

8 §

Liikkumis- ja oleskelurajoitukset

Erittäin tärkeän toiminnan tai omaisuuden turvaamiseksi taikka ihmisten suojaamiseksi voidaan sisäministeriön asetuksella rajoittaa liikkumista tai oleskelua turvattavassa tai suojattavassa kohteessa tai sen ympäristössä kohteesta aiheutuvan tai siihen kohdistuvan vaaran vuoksi taikka kieltää turvallisuutta vaarantavien esineiden tai aineiden tuonti sinne. Kiellon tai rajoituksen rikkomisesta voidaan tuomita sakkoon, jos teosta ei ole muualla laissa säädetty ankarampaa rangaistusta.

9 §

Kansainvälinen yhteistoiminta

— —

Sisäministeriö voi asioissa, jotka eivät kuulu lainsäädännön alaan tai muuten vaadi eduskunnan suostumusta, tehdä poliisin toimialaan kuuluvia, tavanomaisina pidettäviä yhteistoimintasopimuksia naapurivaltioiden, Itämeren rantavaltioiden ja Euroopan talousalueeseen kuuluvien valtioiden kanssa.

10 §

Tarkemmat säännökset

— —

Sisäministeriön asetuksella voidaan säätää tarkemmin:
1) poliisimiehen aseman ilmaisemisesta ja poliisimiehen yksilöimisestä huolehtimisesta;
2) haltuun otetun omaisuuden säilyttämisestä;
3) poliisitutkinnan suorittamisesta;
4) kulkuneuvon pysäyttämisessä käytettävistä merkeistä ja menetelmistä;
5) automaattisesta tieliikenteen valvonnasta;

6) voimakeinojen käytön määritelmistä, voimankäyttökoulutuksesta, voimankäytön harjoittelusta ja seurannasta, oikeudesta kantaa voimankäyttövälineitä, voimankäyttövälineiden säilyttämisestä sekä voimakeinojen käytön valvonnasta;
7) eläimen kiinniottamisesta, säilyttämisestä ja lopettamisesta;
8) virka-avun antamisesta muulle kuin tullilaitokselle tai rajavartiolaitokselle;
9) poliisitoimenpiteiden kirjaamisesta;
10) turvatarkastustoimenpiteiden teknisestä toteuttamisesta ja turvatarkastusten käytännön järjestämisestä sekä turvatarkastuksista järjestettävästä koulutuksesta;
11) virkapuvun mallista ja sen yhteydessä käytettävistä merkeistä sekä siitä, milloin virkatehtävän laatu tai luonne edellyttää virkapuvun käyttöä.

Tämä laki tulee voimaan päivänä kuuta 20 .

LUONNOS

2.

Laki

tietoliikennetiedustelusta siviilitiedustelussa

Eduskunnan päätöksen mukaisesti säädetään:

1 §

Soveltamisala ja suhde muuhun lainsäädäntöön

Tässä laissa säädetään tietoliikennetiedustelun käyttämisestä siviilitiedustelussa.

Tietoliikennetiedustelun käyttämisestä sotilastiedustelussa ja tietoliikennetiedustelun teknisestä toteuttamisesta säädetään sotilastiedustelulaissa (/). Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta sekä televalvonnasta siviilitiedustelussa säädetään poliisilain (872/2011) 5 a luvussa.

Siltä osin kuin tietoliikennetiedustelulla saatujen tietojen käsittelystä ei säädetä tässä laissa, tietojen käsittelystä säädetään laissa henkilötietojen käsittelystä poliisitoimessa (761/2003).

2 §

Määritelmät

Tässä laissa tarkoitetaan:

1) tietoliikennetiedustelulla Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä ja

2) viestintäverkolla toisiinsa liitetyistä johtimista sekä laitteista muodostuvaa järjestelmää, joka on tarkoitettu viestien siirtoon tai jakeluun johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla.

3) tiedonsiirtäjällä tahoa, joka omistaa tai hallitsee viestintäverkon sitä osaa, joka ylittää Suomen rajan.

3 §

Tietoliikennetiedustelun kohteet

Tietoliikennetiedustelulla saadaan hankkia tietoa:

1) terrorismista;

2) ulkomaisesta tiedustelutoiminnasta;

3) joukkotuhoaseiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;

4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1992) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;

5) kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminnasta;

6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavasta toiminnasta;

7) vieraan valtion toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille;

8) kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä;

LUONNOS

9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaavasta toiminnasta;
10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaavasta toiminnasta; sekä
11) yhteiskuntajärjestystä uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta.

4 §

Tietoliikennetiedustelun käytön edellytykset

Tietoliikennetiedustelun käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Jos tietoliikennetiedustelun hakuehtojen käyttö ei koske ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, on edellytyksenä lisäksi, että tietoliikennetiedustelun voidaan olettaa olevan välttämätöntä tiedon saamiseksi tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

5 §

Tietoliikennetiedustelun kohdistaminen

Tietoliikennetiedustelun kohdistaminen toteutetaan tietoliikenteen automatisoidun erottelun avulla. Automatisoitu erottelu perustuu 7 tai 9 §:n mukaisessa menettelyssä hyväksyttyjen hakuehtojen käyttöön.

Viestin sisältöä kuvaavaa hakuehtoa saadaan käyttää ainoastaan, jos
1) hakuehtoa käytetään pelkästään vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenteeseen, tai
2) hakuehto kuvaa haitallisen tietokoneohjelman tai -käskyn sisältöä.

Hakuehtona ei saa käyttää Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

6 §

Automatisoidun erottelun avulla kerätyn tiedon jatkokäsittely

Tietoliikenteestä edellä 5 §:ssä tarkoitetulla tavalla automatisoidusti eroteltua tietoliikennettä saadaan käsitellä automaattisesti ja manuaalisesti. Käsittelyssä saadaan selvittää viestin sisältö ja muut luottamukselliset tiedot.

7 §

Tietoliikennetiedustelua koskeva tuomioistuimen lupa

Tuomioistuin päättää tietoliikennetiedustelusta suojelupoliisin päällikön kirjallisesta vaatimuksesta.

Tietoliikennetiedustelua koskevassa vaatimuksessa ja päätöksessä on mainittava:
1) tietoliikennetiedustelun kohteena oleva 3 §:ssä tarkoitettu toiminta;
2) 1 kohdassa tarkoitettua toimintaa koskevat tosiseikat;
3) tosiseikat, joihin tietoliikennetiedustelun käytön edellytykset perustuvat;
4) tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille;

LUONNOS

5) rajan ylittävän viestintäverkon osa, jossa liikkuvaan tietoliikenteeseen hakuehtoja käytetään, sekä perustelut viestintäverkon osan valinnalle;
6) tietoliikennetiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;
7) tietoliikennetiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies;
8) mahdolliset tietoliikennetiedustelun rajoitukset ja ehdot.

Lupa tietoliikennetiedusteluun voidaan myöntää enintään kuudeksi kuukaudeksi kerrallaan.

Tietoliikennetiedustelu on lopetettava ennen luvassa mainitun määräajan päättymistä, jos tietoliikennetiedustelun tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

8 §

Menettely tuomioistuimessa

Tietoliikennetiedustelua koskevan lupa-asian käsittelemisessä ja ratkaisemisessa tuomioistuimessa noudatetaan, mitä poliisilain 5 a luvun 35 §:ssä säädetään tiedustelumenetelmää koskevan lupa-asian käsittelemisestä

9 §

Kiiretilanteen päätösmenettely

Jos tietoliikennetiedustelua koskeva asia ei siedä viivytystä, saa suojelupoliisin päällikkö päättää tietoliikennetiedustelusta 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 alkamisesta.

Jos tuomioistuin katsoo, että 4 §:n mukaisia edellytyksiä tietoliikennetiedustelulle ei ole ollut, on tietoliikennetiedustelun käyttö lopetettava välittömästi sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot heti hävitettävä. Jos tuomioistuin katsoo, että 1 momentissa tarkoitettu päätös on ollut joltain muulta osin virheellinen, on tietoliikennetiedustelun käyttö välittömästi lopetettava siltä osin kuin tuomioistuimen päätös sitä edellyttää sekä tietoliikennetiedustelulla saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot samoilta osin viipymättä hävitettävä. Tieto saadaan kuitenkin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin poliisilain 5 a luvun 46 §:n 1 momentissa säädetyin edellytyksin.

10 §

Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa

Tietoliikennetiedustelun teknisenä toteuttajana toimii puolustusvoimien tiedustelulaitos.

Suojelupoliisi voi antaa puolustusvoimien tiedustelulaitokselle toimeksiannon sotilastiedustelulain 66 §:ssä tarkoitettuun teknisten tietojen käsittelyyn. Puolustusvoimien tiedustelulaitos hakee suojelupoliisin puolesta sotilastiedustelulain 67 §:n mukaisen luvan teknisten tietojen käsittelyyn. Puolustusvoimien tiedustelulaitos toimittaa sotilastiedustelulain 66 § 2 momentissa tarkoitetun tilastollisen analyysin tuloksen suojelupoliisille sen jälkeen kun se on saanut luvan teknisten tietojen käsittelyyn ja toteuttanut luvan mukaiset toimenpiteet.

Suojelupoliisi toimittaa tämän lain 7 tai 9 §:ssä tarkoitetun päätöksen puolustusvoimien tiedustelulaitokselle, joka suorittaa 5 §:n mukaiset toimenpiteet suojelupoliisin puolesta. Puolus-

tusvoimien tiedustelulaitos toimittaa toimeksiannon toteuttamisella erottelemansa tietoliikenteen suojelupoliisille.

Suojelupoliisin muuhun yhteistyöhön sotilastiedusteluviranomaisen kanssa sovelletaan poliisilain 5 a luvun 54 §:ää.

11 §

Määräaikojen laskeminen

Tässä laissa tarkoitettujen määräaikojen laskemiseen ei sovelleta säädettyjen määräaikain laskemisesta annettua lakia (150/1930).

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.

12 §

Tiedustelukielto

Tietoliikennetiedustelua ei saa kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa, eikä tietoon, josta lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla.

13 §

Tallenteiden ja asiakirjojen tarkastaminen

Suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen on ilman aiheetonta viivytystä tarkastettava tietoliikennetiedustelun käytössä kertyneet tallenteet ja asiakirjat.

14 §

Tallenteiden tutkiminen

Tietoliikennetiedustelun käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja suojelupoliisin päällystöön kuuluva poliisimies. Suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

15 §

Tietojen hävittäminen

Tietoliikennetiedustelulla saatu tieto on hävitettävä viipymättä, jos käy ilmi, että

1) viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui,

2) lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta 12 §:ssä tarkoitetulla tavalla.

3) tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi.

Edellä 1 momentin 3 kohdassa tarkoitettu tieto voidaan kuitenkin luovuttaa rikostorjuntaan poliisilain 5 a luvun 44 §:ssä säädetyin edellytyksin sekä säilyttää ja tallettaa henkilötietojen

LUONNOS

käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin poliisilain 5 a luvun 45 §:n 1 momentissa säädetyin edellytyksin.

Tietojen hävittämisestä vastaa tietoliikennetiedustelun tekninen toteuttaja tai, jos se on ehtinyt toimittaa tiedot toimeksiantajalle, toimeksiantaja.

16 §

Haitallista tietokoneohjelmaa tai -käskyä koskevien tietojen luovuttaminen viranomaiselle, yritykselle tai yhteisölle

Suojelupoliisi saa salassapitosäännösten estämättä luovuttaa tietoliikennetiedustelun avulla hankitun tiedon haitallisesta tietokoneohjelmasta tai käskystä viranomaiselle, yritykselle tai yhteisölle, jos tiedon luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi tai tiedon saajan etujen turvaamiseksi.

Yrityksen tai yhteisön palveluksessa olevan vaitiolovelvollisuuteen sovelletaan, mitä viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 23 §:n 2 momentissa säädetään.

17 §

Tiedon luovuttaminen rikostorjuntaan

Tietoliikennetiedustelulla saadun tiedon rikostorjuntaan luovuttamiseen sovelletaan poliisilain 5 a luvun 44 §:ää.

18 §

Asianosaisjulkisuuden rajoittaminen eräissä tapauksissa

Viranomaisten toiminnan julkisuudesta annetun lain (621/1999) 11 §:ssä säädetystä huolimatta henkilöllä ei ole oikeutta saada tietoa tietoliikennetiedustelun käytöstä ennen kuin 20 §:ssä tarkoitettu ilmoitus on tehty.

Rekisteröidyn tarkastusoikeudesta säädetään henkilötietojen käsittelystä poliisitoimessa annetussa laissa.

19 §

Pöytäkirja

Tietoliikennetiedustelun käytön lopettamisen jälkeen on laadittava ilman aiheetonta viivytystä pöytäkirja.

20 §

Tietoliikennetiedustelun käytöstä ilmoittaminen

Jos 6 §:ssä tarkoitetussa käsittelyssä on manuaalisesti selvitetty Suomessa olevan henkilön luottamuksellisen viestin tai tallentaman tiedon sisältö, ilmoitetaan hänelle tietoliikennetiedustelusta noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan ole, jos tietoliikennetiedustelulla saatu tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

21 §

Tietoliikennetiedustelun edellyttämän kytkennän toteuttaminen

Tietoliikennetiedustelun edellyttämän kytkennän toteuttamisessa siviilitiedustelua varten noudatetaan, mitä sotilastiedustelulain 72 §:ssä säädetään.

22 §

Tiedonsiirtäjän tietojenantovelvollisuus

Tiedonsiirtäjän on ilman aiheetonta viivytystä annettava suojelupoliisille tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen päällystöön kuuluvan suojelupoliisin poliisimiehen yksilöidystä pyynnöstä hallussaan olevat Suomen rajan ylittävän viestintäverkon rakenteeseen ja siinä kulkevan tietoliikenteen reitittymiseen liittyvät tekniset tiedot, jotka ovat tarpeen viestintäverkon osan yksilöimiseksi tietoliikennetiedustelun käyttöä koskevaa lupavaatimusta ja -päätöstä varten.

23 §

Korvaus tiedonsiirtäjälle

Tiedonsiirtäjällä on oikeus saada valtion varoista korvaus 22 §:ssä tarkoitetusta tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksen maksamisesta päättää suojelupoliisi.

Päätökseen 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.

24 §

Tietoliikennetiedustelun valvonta sisäasiainhallinnossa

Tässä laissa tarkoitettua tiedonhankintaa valvoo suojelupoliisin päällikkö sekä sisäministeriö.

25 §

Tietoliikennetiedustelun ulkoinen valvonta

Sisäministeriön on annettava eduskunnan oikeusasiamiehelle ja tiedusteluvaltuutetulle vuosittain kertomus tietoliikennetiedustelun käyttämisestä.

Tiedusteluvaltuutetun harjoittamasta valvonnasta säädetään tiedustelutoiminnan valvonnasta annetussa laissa (/).

26 §

Tiedusteluvaltuutetulle tehtävät ilmoitukset

Suojelupoliisin on annettava tieto tiedusteluvaltuutetulle tämän lain nojalla annetuista tuomioistuimen luvista ja päätöksistä mahdollisimman pian tehdyn päätöksen jälkeen.

27 §

Tarkemmat säännökset

Valtioneuvoston asetuksella voidaan antaa tarkempia säännöksiä tietoliikennetiedustelun käytön järjestämisestä ja valvonnasta sekä toimenpiteiden kirjaamisesta ja valvontaa varten annettavista selvityksistä.

28 §

Voimaantulo

Tämä laki tulee voimaan päivänä kuuta 20 .

Ennen tämän lain voimaantuloa voidaan ryhtyä sen täytäntöönpanon edellyttämiin toimenpiteisiin.

LUONNOS

3.

Laki

poliisin hallinnosta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan poliisin hallinnosta annetun lain (110/1992) 10 §:n 1 ja 2 momentti,
sellaisena kuin ne ovat laissa 860/2015, sekä
lisätään 15 a §:ään sellaisena kuin se on osaksi laissa 873/2011, uusi 3 momentti seuraavasti:

10 §

Suojelupoliisi

Suojelupoliisin tehtävänä on sisäministeriön ohjauksen mukaisesti hankkia tietoa kansallisen turvallisuuden suojaamiseksi sekä havaita, estää ja paljastaa sellaisia toimintoja, hankkeita ja rikoksia, jotka voivat uhata valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta yhteiskunnan turvallisuutta uhkaavan toiminnan havaitsemiseksi ja estämiseksi.

Sisäministeriö määrää Poliisihallitusta kuultuaan tarvittaessa tarkemmin suojelupoliisin ja muiden poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä.

— —

15 a §

Poliisivaltuudet

— —

Sen lisäksi mitä 1 momentissa säädetään, suojelupoliisin virkamiehellä on oikeus käyttää poliisilain 5 a luvussa tarkoitettuja tiedustelumenetelmiä kansallisen turvallisuuden suojaamiseksi sen mukaan kuin mainitussa luvussa säädetään.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

LUONNOS

4.

Laki

henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan henkilötietojen käsittelystä poliisitoimessa annetun lain (761/2003) 5 §:n 2 momentti, 13 §:n 1 momentin 2, 4, 6, 15 ja 16 kohta, 45 §:n 1 momentin 5 kohta,
sellaisina kuin niistä ovat 13 §:n 1 momentin 2 kohta laissa 1073/2015 ja 13 §:n 1 momentin 15 kohta laissa 29/2015, seuraavasti

5 §

Suojelupoliisin toiminnallinen tietojärjestelmä

— —

Suojelupoliisin toiminnallinen tietojärjestelmä voi sisältää tietoja, joita on tarpeen käsitellä kansallisen turvallisuuden suojaamiseksi, oikeus- ja yhteiskuntajärjestystä tai valtion turvallisuutta vaarantavien hankkeiden tai rikosten estämiseksi, paljastamiseksi tai selvittämiseksi.

— —

13 §

Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä

Poliisilla on sen lisäksi, mitä muualla laissa säädetään, oikeus saada tehtäviensä suorittamista ja henkilörekisteriensä ylläpitämistä varten salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona tarpeellisia tietoja rekistereistä siten kuin asianomaisen rekisterinpitäjän kanssa sovitaan, seuraavasti:

— —

2) kansallisen turvallisuuden suojaamiseksi, rikosten estämiseksi, paljastamiseksi ja selvittämiseksi ja syyteharkintaan saattamiseksi tai henkilön luotettavuutta edellyttävän poliisin lupaa tai hyväksyntää varten henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain (1069/2015) 14 §:n 1 ja 2 momentissa säädetystä Rikosseuraamuslaitoksen tietojärjestelmästä tuomitusta, vangista ja Rikosseuraamuslaitoksen yksikköön otetusta henkilöstä;

— —

4) majoitus- ja ravitsemistoiminnasta annetun lain (308/2006) 6 §:n 1 momentissa tarkoitettuja matkustajatietoja majoitustoiminnan harjoittajilta kansallisen turvallisuuden suojaamiseksi, yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikosten estämiseksi, paljastamiseksi tai selvittämiseksi ja poliisille laissa säädetyn muun tehtävän suorittamiseksi;

— —

6) Patentti- ja rekisterihallituksen kaupparekisteristä tiedot elinkeinonharjoittajia koskevista ilmoituksista ja tiedonannoista kansallisen turvallisuuden suojaamiseksi, rikosten estämistä, paljastamista ja selvittämistä varten;

— —

15) panostajalain (219/2000) 3 §:ssä tarkoitetusta panostajarekisteristä valvonta- ja hälytystehtäviä sekä kansallisen turvallisuuden suojaamiseksi, rikosten estämistä, selvittämistä ja paljastamista varten;

— —

LUONNOS

16) kansallisen turvallisuuden suojaamiseksi, rikosten estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi sekä etsintäkuulutettujen tavoittamiseksi yhteisöiltä ja yhtymiltä matkustajaa ja kulkuneuvon henkilökuntaa koskevista rekistereistä.

— —

45 §

Tarkastusoikeuden rajoittaminen

Tarkastusoikeutta ei ole lainkaan:

— —

5) tietoihin, jotka on saatu poliisilain 4 luvun 3 §:n, 5 ja 5 a luvun, pakkokeinolain 10 luvun tai siviilitiedustelusta tietoliikennetiedustelusta annetun lain mukaisia toimivaltuuksia käyttäen;

— —

Tämä laki tulee voimaan päivänä kuuta 20 .

LUONNOS

5.

Laki

esitutkintalain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan esitutkintalain (805/2011) 2 luvun 1 §:n 1 momentti seuraavasti:

2 luku

Esitutkintaan osalliset

1 §

Viranomaiset esitutkinnassa

Esitutkinnan toimittaa poliisi. Suojelupoliisi ei ole kuitenkaan esitutkintaviranomainen.

Tämä laki tulee voimaan _____ päivänä kuuta 20 _____.

LUONNOS

6.

Laki

rikoslain muuttamisesta

Eduskunnan päätöksen mukaisesti
lisätään rikoslain (89/1889) 12 lukuun sellaisena kuin se on laissa 578/1995 uusi 12 § seuraavasti:

12 luku

Maanpetosrikoksista

12 §

Rajoitussäännös

Tässä luvussa tarkoitettuna rikoksena ei pidetä poliisilain (872/2011) 5 a luvun, tietoliikennetiedustelusta siviilitiedustelussa annetun lain (/) tai sotilastiedustelusta annetun lain (/) mukaista tiedustelumenetelmän käyttämistä.

Tämä laki tulee voimaan päivänä kuuta 20 .

LUONNOS

7.

Laki

pakkokeinolain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan pakkokeinolain (806/2011) 2 luvun 9 §:n 1 momentin 1 kohta, 10 luvun 3 §:n 1 momentti ja 6 §:n 1 momentti sekä 39 §:n 1 momentti seuraavasti:

2 luku

Kiinniottaminen, pidättäminen ja vangitseminen

9 §

Pidättämiseen oikeutettu virkamies

Pidättämisestä päättää pidättämiseen oikeutettu virkamies. Pidättämiseen oikeutettuja virkamiehiä ovat:
1) poliisiylijohtaja, Poliisihallituksen poliisijohtaja, poliisiylitarkastaja ja poliisitarkastaja, poliisipäällikkö, apulaispoliisipäällikkö, keskusrikospoliisin päällikkö ja apulaispäällikkö, rikosylitarkastaja, rikostarkastaja, rikosylikomisario, ylikomisario, rikoskomisario ja komisario;
2) Tullin rikostorjunnan päällikkö, Tullin rikostorjunnan toimintayksikön päällikkö sekä Tullin rikostorjunnan tulliylitarkastaja, jonka Tullin rikostorjunnan päällikkö on määrännyt tutkinnanjohtajaksi;
3) rajavartiolaitoksen päällikkö ja apulaispäällikkö, rajavartiolaitoksen esikunnan raja- ja meriosaston osastopäällikkö, rajavartiolaitoksen esikunnan oikeudellisen osaston osastopäällikkö, apulaisosastopäällikkö, rikostorjuntayksikön yksikönpäällikkö, rajavartioylitarkastaja, ylitarkastaja, rikosylitarkastaja ja rikostarkastaja, rajavartioston ja merivartioston komentaja ja apulaiskomentaja, rajavartioston ja merivartioston rajatoimiston ja meritoimiston päällikkö, Suomenlahden merivartioston Helsingin rajatarkastusosaston päällikkö ja varapäällikkö sekä vähintään luutnantin arvoinen rajavartiomies, joka on saanut tutkinnanjohtajalle rajavartiolaitoksessa säädetyn koulutuksen ja jonka rajavartiolaitoksen tai sen hallintoyksikön päällikkö on määrännyt tutkinnanjohtajaksi;
4) syyttäjä.
Pidättämiseen oikeutetuista puolustusvoimien virkamiehistä säädetään laissa erikseen.

10 luku

Salaiset pakkokeinot

3 §

Telekuuntelu ja sen edellytykset

Telekuuntelulla tarkoitetaan sähköisen viestinnän palveluista annetun lain (917/2014) 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 8 §:ssä tarkoitettujen tun-

nistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain rikoksesta epäillyltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin.

— —

6 §

Televalvonta ja sen edellytykset

Televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty 3 §: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 palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun tilaajaan tai mainitun pykälän 30 kohdassa tarkoitettuun käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

— —

39 §

Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun viranomaisen ulkopuoliselta henkilöltä (*tietolähde*).

— —

Tämä laki tulee voimaan päivänä kuuta 20 .

LUONNOS

8.

Laki

oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain (370/2007) 5 §:n 2 momentti, 12 §:n 2 momentin 3 kohta, 16 §:n 4 momentti,
sellaisina kuin ne ovat 5 §:n 2 momentti ja 16 §:n 4 momentti laissa 1159/2013 sekä 12 §:n 2 momentin 3 kohta laissa 633/2015 seuraavasti:

5 §

Oikeudenkäyntiä koskevien perustietojen julkiseksi tulemisen ajankohta

— —

Pakkokeinolain (806/2011) 10 luvussa, poliisilain (872/2011) 5 luvussa tai rikostorjunnasta Tullissa annetun lain (623/2015) 3 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa (/) tai sotilastiedustelusta annetussa laissa (/) tarkoitettua tiedustelumenetelmää koskevassa asiassa, jossa tiedonhankintakeinon tai tiedustelumenetelmän kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, perustiedot tulevat julkisiksi vasta, kun tiedonhankintakeinon tai tiedustelumenetelmän käytöstä on viimeistään ilmoitettava rikoksesta epäillylle taikka tiedonhankintakeinon tai tiedustelumenetelmän kohteena olevalle. Jos hänelle ilmoitetaan tiedonhankintakeinon tai tiedustelumenetelmän käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, perustiedot tulevat julkisiksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Tuomioistuin voi päättää, että perustiedot tulevat julkisiksi aikaisemmin.

12 §

Asianosaisen oikeus tiedonsaantiin

— —

Asianosaisella ei ole 1 momentissa tarkoitettua oikeutta:
1) viranomaisten toiminnan julkisuudesta annetun lain 11 §:n 2 momentin 7 tai 7 a kohdassa tarkoitettuihin tietoihin;
2) tuomioistuimessa laadittuihin oikeudenkäyntiasiakirjoihin ennen 8 §:ssä tarkoitettua ajankohtaa;
3) pakkokeinolain 10 luvussa, poliisilain 5 luvussa tai rikostorjunnasta Tullissa annetun lain 3 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa tai sotilastiedustelusta annetussa laissa tarkoitettua tiedustelumenetelmää koskevassa asiassa, jossa tiedonhankintakeinon tai tiedustelumenetelmän kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla; eikä
4) oikeudenkäyntiasiakirjoihin siltä osin kuin niihin sisältyy tietoja tuomioistuimen neuvottelusta.

16 §

Pakkokeinoasioiden julkisuus

— —

Pakkokeinolain 10 luvussa, poliisilain 5 luvussa tai rikostorjunnasta Tullissa annetun lain 3 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa tai sotilastiedustelusta annetussa laissa tarkoitettua tiedustelumenetelmää koskeva asia, jossa tiedonhankintakeinon tai tiedustelumenetelmän kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, käsitellään ja ratkaisu siinä julistetaan yleisön läsnä olematta. Ratkaisun sisältävä ja muu oikeudenkäyntiasiakirja tulevat julkisiksi, kun tiedonhankintakeinon tai tiedustelumenetelmän käytöstä on viimeistään ilmoitettava rikoksesta epäillylle taikka tiedonhankintakeinon tai tiedustelumenetelmän kohteena olevalle. Jos hänelle ilmoitetaan tiedonhankintakeinon tai tiedustelumenetelmän käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, oikeudenkäyntiasiakirjat tulevat julkisiksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Tuomioistuin voi erityisestä syystä päättää, että oikeudenkäyntiasiakirja tulee julkiseksi aikaisemmin.

Tämä laki tulee voimaan päivänä kuuta 20 .

Helsingissä xx päivänä kuuta 20

Pääministeri

Juha Sipilä

Sisäministeri Paula Risikko

LUONNOS

Rinnakkaisteksti

1.

Laki

poliisilain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan poliisilain (872/2011) 1 luvun 1 §:n 1 momentti, 5 luvun 5 §:n 1 momentti, 7 §:n 1 momentti ja 3 momentin 6 kohta, 8 §:n 1 momentti, 10 §:n 1—4 momentti ja 6 momentin 7 kohta, 12 §:n 1 momentti ja 3 momentin 5 kohta, 14 §:n 1 momentti ja 3 momentin 5 kohta, 16 §:n 1 momentti, 18 §:n 2 momentti ja 4 momentin 6 kohta, 20 §:n 1 ja 2 momentti sekä 4 momentin 6 kohta, 22 §:n 1 ja 2 momentti sekä 4 momentin 6 kohta, 24 §:n 1 momentti ja 3 momentin 6 kohta, 25 §:n 3 momentti, 32 §:n 1 momentti, 36 §:n 1 momentti ja 3 momentin 7 kohta, 38 §:n 1 momentti, 39 §:n 1 momentti, 40 §:n 1 momentti, 42 §:n 1 momentti, 44 §:n 1 momentti, 47 §:n 2 momentti, 48 §:n 1 momentti, 52 ja 57 §, 58 §:n 1 momentti, 61 §:n 2 momentti, 63 §:n 2 momentti, 9 luvun 8 §, 9 §:n 2 momentti, 10 §:n 2 momentin johdantokappale,

sellaisina kuin niistä ovat 10 §:n 3 momentti ja 6 momentin 7 kohta, 12 §:n 3 momentin 5 kohta, 18 §:n 4 momentin 6 kohta, 20 §:n 4 momentin 6 kohta, 22 §:n 4 momentin 6 kohta, 47 §:n 2 momentti ja 58 §:n 1 momentti laissa 1168/2013, sekä

lisätään lakiin uusi 5 a luku seuraavasti:

Voimassa oleva laki	*Ehdotus*
1 luku	1 luku
Yleiset säännökset	**Yleiset säännökset**
1 §	1 §
Poliisin tehtävät	*Poliisin tehtävät*
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 tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, *kansallisen turvallisuuden suojaaminen*, 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.
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —

LUONNOS

Voimassa oleva laki

5 luku

Salaiset tiedonhankintakeinot

5 §

Telekuuntelu ja sen edellytykset

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.

— — — — — — — — — — — — — — — — — —

7 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta pakkokeinolain 2 luvun 9 §:n 1 momentin 1 kohdassa tarkoitetun poliisimiehen *(pidättämiseen oikeutettu poliisimies)* vaatimuksesta.

— — — — — — — — — — — — — — — — — —

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

Ehdotus

5 luku

Salaiset tiedonhankintakeinot

5 §

Telekuuntelu ja sen edellytykset

Telekuuntelulla tarkoitetaan *sähköisen viestinnän palveluista annetun lain (917/2014) 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 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.

— — — — — — — — — — — — — — — — — —

7 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta pakkokeinolain 2 luvun 9 §:n 1 momentin 1 kohdassa tarkoitetun poliisimiehen (*pidättämiseen oikeutettu poliisimies*) *taikka suojelupoliisin päällikön, apulaispäällikön, osastopäällikön, ylitarkastajan tai tarkastajan (suojelupoliisin päällystöön kuuluva poliisimies)* vaatimuksesta.

— — — — — — — — — — — — — — — — — —

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

LUONNOS

Voimassa oleva laki

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.

8 §

Televalvonta ja sen edellytykset

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.

— — — — — — — — — — — — — — — — —

10 §

Televalvonnasta päättäminen

Tuomioistuin päättää 8 §:n 2 ja 5 momentissa sekä 9 §:n 1, 4 ja 5 kohdassa tarkoitetusta televalvonnasta sekä televalvonnasta 3 §:ssä tarkoitetuissa tapauksissa pidättämiseen oikeutetun poliisimiehen vaatimuksesta.

Ehdotus

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 *1 momentissa tarkoitettu* poliisimies;

7) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

8 §

Televalvonta ja sen edellytykset

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 *palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun* tilaajaan tai *mainitun pykälän 30 kohdassa tarkoitettuun* käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

— — — — — — — — — — — — — — — — —

10 §

Televalvonnasta päättäminen

Tuomioistuin päättää 8 §:n 2 ja 5 momentissa sekä 9 §:n 1, 4 ja 5 kohdassa tarkoitetusta televalvonnasta sekä televalvonnasta 3 §:ssä tarkoitetuissa tapauksissa pidättämiseen oikeutetun poliisimiehen *taikka suojelupoliisin päällystöön kuuluvan poliisimiehen* vaa-

Voimassa oleva laki

Jos 1 momentissa tarkoitettua muuta kuin 3 §:n nojalla suoritettavaa televalvontaa koskeva asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies 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.

Keskusrikospoliisin tai suojelupoliisin taikka poliisilaitoksen päällikkö päättää 8 §:n 4 momentissa tarkoitetusta televalvonnasta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies saa päättää televalvonnasta siihen asti, kunnes keskusrikospoliisin tai suojelupoliisin päällikkö taikka poliisilaitoksen päällikkö on ratkaissut televalvontaa koskevan asian. Asia on saatettava mainitun poliisimiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Pidättämiseen oikeutettu poliisimies päättää 8 §:n 3 momentissa ja 9 §:n 2 ja 3 kohdassa tarkoitetusta televalvonnasta.

— — — — — — — — — — — — — — — — — —

Televalvontaa 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 televalvonnan edellytykset perustuvat;

4) suostumus, jos se on televalvonnan käytön edellytys;

5) luvan voimassaoloaika kellonajan tarkkuudella;

6) toimenpiteen kohteena oleva teleosoite tai telepäätelaite;

7) televalvonnan suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;

Ehdotus

timuksesta.

Jos 1 momentissa tarkoitettua muuta kuin 3 §:n nojalla suoritettavaa televalvontaa koskeva asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* 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.

Keskusrikospoliisin tai suojelupoliisin taikka poliisilaitoksen päällikkö päättää 8 §:n 4 momentissa tarkoitetusta televalvonnasta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* saa päättää televalvonnasta siihen asti, kunnes keskusrikospoliisin tai suojelupoliisin päällikkö taikka poliisilaitoksen päällikkö on ratkaissut televalvontaa koskevan asian. Asia on saatettava mainitun poliisimiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua keinon käytön aloittamisesta.

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* päättää 8 §:n 3 momentissa ja 9 §:n 2 ja 3 kohdassa tarkoitetusta televalvonnasta.

— — — — — — — — — — — — — — — — — —

Televalvontaa 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 televalvonnan edellytykset perustuvat;

4) suostumus, jos se on televalvonnan käytön edellytys;

5) luvan voimassaoloaika kellonajan tarkkuudella;

6) toimenpiteen kohteena oleva teleosoite tai telepäätelaite;

7) televalvonnan suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisi-

Voimassa oleva laki

8) mahdolliset televalvonnan rajoitukset ja ehdot.

12 §

Tukiasematietojen hankkimisesta päättäminen

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.

— — — — — — — — — — — — — — — — — —

Tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika taikka toimenpiteen perusteena oleva vaara;
2) tosiseikat, joihin tukiasematietojen hankkimisen edellytykset perustuvat;
3) ajanjakso, jota lupa koskee;
4) tukiasema, jota lupa koskee;
5) tukiasematietojen hankkimisen suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;
6) mahdolliset tukiasematietojen hankkimisen rajoitukset ja ehdot.

14 §

Suunnitelmallisesta tarkkailusta päättäminen

Pidättämiseen oikeutettu poliisimies päättää suunnitelmallisesta tarkkailusta.

— — — — — — — — — — — — — — — — — —

Päätös suunnitelmallisesta tarkkailusta on tehtävä kirjallisesti. Päätöksessä on mainittava:

Ehdotus

simies;
8) mahdolliset televalvonnan rajoitukset ja ehdot.

12 §

Tukiasematietojen hankkimisesta päättäminen

Tuomioistuin päättää tukiasematietojen hankkimisesta pidättämiseen oikeutetun poliisimiehen *tai suojelupoliisin päällystöön kuuluvan poliisimiehen* vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva 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.

— — — — — — — — — — — — — — — — — —

Tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika taikka toimenpiteen perusteena oleva vaara;
2) tosiseikat, joihin tukiasematietojen hankkimisen edellytykset perustuvat;
3) ajanjakso, jota lupa koskee;
4) tukiasema, jota lupa koskee;
5) tukiasematietojen hankkimisen suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisimies;
6) mahdolliset tukiasematietojen hankkimisen rajoitukset ja ehdot.

14 §

Suunnitelmallisesta tarkkailusta päättäminen

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* päättää suunnitelmallisesta tarkkailusta.

— — — — — — — — — — — — — — — — — —

Päätös suunnitelmallisesta tarkkailusta on tehtävä kirjallisesti. Päätöksessä on mainittava:

LUONNOS

Voimassa oleva laki

1) toimenpiteen perusteena oleva rikos ja sen tekoaika;
2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;
3) tosiseikat, joihin henkilöön kohdistuva epäily ja suunnitelmallinen tarkkailu perustuvat;
4) luvan voimassaoloaika;
5) suunnitelmallisen tarkkailun suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;
6) mahdolliset suunnitelmallisen tarkkailun rajoitukset ja ehdot.

16 §

Peitellystä tiedonhankinnasta päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies päättää peitellystä tiedonhankinnasta.

— — — — — — — — — — — — — — — — — —

18 §

Teknisestä kuuntelusta päättäminen

— — — — — — — — — — — — — — — — — —

Pidättämiseen oikeutettu poliisimies päättää 17 §:n 5 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta.

— — — — — — — — — — — — — — — — — —

Teknistä kuuntelua 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 teknisen kuuntelun edellytykset perustuvat;
4) luvan voimassaoloaika kellonajan tark-

Ehdotus

1) toimenpiteen perusteena oleva rikos ja sen tekoaika;
2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;
3) tosiseikat, joihin henkilöön kohdistuva epäily ja suunnitelmallinen tarkkailu perustuvat;
4) luvan voimassaoloaika;
5) suunnitelmallisen tarkkailun suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisimies;
6) mahdolliset suunnitelmallisen tarkkailun rajoitukset ja ehdot.

16 §

Peitellystä tiedonhankinnasta päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupolitisin päällystöön kuuluva* poliisimies päättää peitellystä tiedonhankinnasta.

— — — — — — — — — — — — — — — — — —

18 §

Teknisestä kuuntelusta päättäminen

— — — — — — — — — — — — — — — — — —

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* päättää 17 §:n 5 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta.

— — — — — — — — — — — — — — — — — —

Teknistä kuuntelua 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 teknisen kuuntelun edellytykset perustuvat;
4) luvan voimassaoloaika kellonajan tark-

Voimassa oleva laki

kuudella;
5) tila tai muu paikka, johon kuuntelu kohdistuu;
6) teknisen kuuntelun suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;
7) mahdolliset teknisen kuuntelun rajoitukset ja ehdot.

20 §

Teknisestä katselusta päättäminen

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.

Pidättämiseen oikeutettu poliisimies päättää 19 §:n 5 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä katselusta.

— — — — — — — — — — — — — —

Teknistä katselua 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 teknisen katselun edellytykset perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) tila tai muu paikka, johon katselu kohdistuu;
6) teknisen katselun suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;
7) mahdolliset teknisen katselun rajoitukset ja ehdot.

Ehdotus

kuudella;
5) tila tai muu paikka, johon kuuntelu kohdistuu;
6) teknisen kuuntelun suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisimies;
7) mahdolliset teknisen kuuntelun rajoitukset ja ehdot.

20 §

Teknisestä katselusta päättäminen

Tuomioistuin päättää teknisestä katselusta pidättämiseen oikeutetun poliisimiehen *tai suojelupoliisin päällystöön kuuluvan poliisimiehen* vaatimuksesta, kun katselu kohdistuu rikoslain 24 luvun 11 §:ssä tarkoitettuun kotirauhan suojaamaan tilaan tai muuhun paikkaan taikka rikoksen johdosta vapautensa menettäneeseen henkilöön.

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* päättää 19 §:n 5 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä katselusta.

— — — — — — — — — — — — — —

Teknistä katselua 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 teknisen katselun edellytykset perustuvat;
4) luvan voimassaoloaika kellonajan tarkkuudella;
5) tila tai muu paikka, johon katselu kohdistuu;
6) teknisen katselun suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisimies;
7) mahdolliset teknisen katselun rajoitukset ja ehdot.

LUONNOS

Voimassa oleva laki

22 §

Teknisestä seurannasta päättäminen

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.

Pidättämiseen oikeutettu poliisimies päättää 21 §:n 4 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta.

— — — — — — — — — — — — — —

Teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika tai toimenpiteen perusteena oleva vaara;

2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;

3) tosiseikat, joihin henkilöön kohdistuva epäily ja teknisen seurannan edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) toimenpiteen kohteena oleva esine, aine tai omaisuus;

6) teknisen seurannan suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;

7) mahdolliset teknisen seurannan rajoitukset ja ehdot.

24 §

Teknisestä laitetarkkailusta päättäminen

Tuomioistuin päättää teknisestä laitetarkkailusta pidättämiseen oikeutetun poliisimie-

Ehdotus

22 §

Teknisestä seurannasta päättäminen

Tuomioistuin päättää henkilön teknisestä seurannasta pidättämiseen oikeutetun poliisimiehen *tai suojelupoliisin päällystöön kuuluvan poliisimiehen* vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva 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.

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* päättää 21 §:n 4 momentissa tarkoitetusta ja muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta.

— — — — — — — — — — — — — —

Teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen oletettu tekoaika tai toimenpiteen perusteena oleva vaara;

2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;

3) tosiseikat, joihin henkilöön kohdistuva epäily ja teknisen seurannan edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) toimenpiteen kohteena oleva esine, aine tai omaisuus;

6) teknisen seurannan suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisimies;

7) mahdolliset teknisen seurannan rajoitukset ja ehdot.

24 §

Teknisestä laitetarkkailusta päättäminen

Tuomioistuin päättää teknisestä laitetarkkailusta pidättämiseen oikeutetun poliisimie-

LUONNOS

Voimassa oleva laki

hen 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.

— — — — — — — — — — — — — — —

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen tekoaika;

2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;

3) tosiseikat, joihin henkilöön kohdistuva epäily ja teknisen laitetarkkailun edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto;

6) teknisen laitetarkkailun suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;

7) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

25 §

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen

— — — — — — — — — — — — — — —

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää pidättämiseen oikeutettu poliisimies.

32 §

Peitetoiminnasta päättäminen

Keskusrikospoliisin tai suojelupoliisin päällikkö päättää peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoi-

Ehdotus

hen *tai suojelupoliisin päällystöön kuuluvan poliisimiehen* vaatimuksesta. Jos asia ei siedä viivytystä, pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva 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.

— — — — — — — — — — — — — — —

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) toimenpiteen perusteena oleva rikos ja sen tekoaika;

2) henkilö, jonka voidaan perustellusti olettaa syyllistyvän 1 kohdassa tarkoitettuun rikokseen;

3) tosiseikat, joihin henkilöön kohdistuva epäily ja teknisen laitetarkkailun edellytykset perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto;

6) teknisen laitetarkkailun suorittamista johtava ja valvova *7 §:n 1 momentissa tarkoitettu* poliisimies;

7) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

25 §

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen

— — — — — — — — — — — — — — —

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies.*

32 §

Peitetoiminnasta päättäminen

Keskusrikospoliisin tai suojelupoliisin päällikkö päättää peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoi-

LUONNOS

Voimassa oleva laki

minnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies.

— — — — — — — — — — — — — — —

36 §

Valeostosta päättäminen

Keskusrikospoliisin tai suojelupoliisin päällikkö päättää valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies.

— — — — — — — — — — — — — — —

Päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpiteen perusteena oleva rikos;
2) valeoston kohteena oleva henkilö;
3) tosiseikat, joihin epäily ja valeoston edellytykset perustuvat;
4) valeoston kohteena oleva esine, aine, omaisuus tai palvelu;
5) valeoston tarkoitus;
6) päätöksen voimassaoloaika;
7) valeoston suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies;
8) mahdolliset valeoston rajoitukset ja ehdot.

38 §

Valeoston toteuttamista koskeva päätös

Päätös valeoston toteuttamisesta on tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies.

— — — — — — — — — — — — — — —

Ehdotus

minnasta päättää keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupoliisin päällystöön kuuluva* poliisimies.

— — — — — — — — — — — — — — —

36 §

Valeostosta päättäminen

Keskusrikospoliisin tai suojelupoliisin päällikkö päättää valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupoliisin päällystöön kuuluva* poliisimies.

— — — — — — — — — — — — — — —

Päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpiteen perusteena oleva rikos;
2) valeoston kohteena oleva henkilö;
3) tosiseikat, joihin epäily ja valeoston edellytykset perustuvat;
4) valeoston kohteena oleva esine, aine, omaisuus tai palvelu;
5) valeoston tarkoitus;
6) päätöksen voimassaoloaika;
7) valeoston suorittamista johtava ja valvova pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies*;
8) mahdolliset valeoston rajoitukset ja ehdot.

38 §

Valeoston toteuttamista koskeva päätös

Päätös valeoston toteuttamisesta on tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupoliisin päällystöön kuuluva* poliisimies.

— — — — — — — — — — — — — — —

LUONNOS

Voimassa oleva laki

39 §

Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa ja valeostossa

Pidättämiseen oikeutettu poliisimies saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava poliisimies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.

— — — — — — — — — — — — — — —

40 §

Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun *esitutkinta*viranomaisen ulkopuoliselta henkilöltä *(tietolähde)*.

— — — — — — — — — — — — — — —

42 §

Tietolähteen ohjatusta käytöstä päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies päättää tietolähteen ohjatusta käytöstä.

— — — — — — — — — — — — — — —

44 §

Valvotusta läpilaskusta päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies päättää poliisin suorittamasta valvotusta

Ehdotus

39 §

Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa ja valeostossa

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* saa päättää, että peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava poliisimies varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on perusteltua hänen turvallisuutensa varmistamiseksi.

— — — — — — — — — — — — — — —

40 §

Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, 1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi merkityksellisten tietojen vastaanottamista poliisin ja muun viranomaisen ulkopuoliselta henkilöltä (*tietolähde*).

— — — — — — — — — — — — — — —

42 §

Tietolähteen ohjatusta käytöstä päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupoliisin päällystöön kuuluva* poliisimies päättää tietolähteen ohjatusta käytöstä.

— — — — — — — — — — — — — — —

44 §

Valvotusta läpilaskusta päättäminen

Keskusrikospoliisin, suojelupoliisin tai poliisilaitoksen päällikkö taikka tehtävään määrätty salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupoliisin päällystöön kuuluva* poliisimies

LUONNOS

Voimassa oleva laki

läpilaskusta. Muiden viranomaisten valvottua läpilaskua koskevasta päätöksenteosta säädetään erikseen.

— — — — — — — — — — — — — — —

47 §

Suojaamisesta päättäminen

— — — — — — — — — — — — — — —

Salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu poliisimies päättää muusta kuin 1 momentissa tarkoitetusta tiedonhankinnan suojaamisesta.

— — — — — — — — — — — — — — —

48 §

Salaista tiedonhankintaa koskeva ilmaisukielto

Pidättämiseen oikeutettu poliisimies saa tärkeästä rikoksen estämiseen tai paljastamiseen liittyvästä syystä kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja salaisen tiedonhankintakeinon käytöstä. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan salaisen tiedonhankintakeinon käytön toteuttamisessa.

— — — — — — — — — — — — — — —

52 §

Tallenteiden tutkiminen

Salaisen tiedonhankintakeinon käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pidättämiseen oikeutettu poliisimies. Pidättämiseen oikeutetun poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

Ehdotus

päättää poliisin suorittamasta valvotusta läpilaskusta. Muiden viranomaisten valvottua läpilaskua koskevasta päätöksenteosta säädetään erikseen.

— — — — — — — — — — — — — — —

47 §

Suojaamisesta päättäminen

— — — — — — — — — — — — — — —

Salaiseen tiedonhankintaan erityisesti koulutettu pidättämiseen oikeutettu *tai suojelupoliisin päällystöön kuuluva* poliisimies päättää muusta kuin 1 momentissa tarkoitetusta tiedonhankinnan suojaamisesta.

— — — — — — — — — — — — — — —

48 §

Salaista tiedonhankintaa koskeva ilmaisukielto

Pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* saa tärkeästä rikoksen estämiseen tai paljastamiseen liittyvästä syystä kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja salaisen tiedonhankintakeinon käytöstä. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan salaisen tiedonhankintakeinon käytön toteuttamisessa.

— — — — — — — — — — — — — — —

52 §

Tallenteiden tutkiminen

Salaisen tiedonhankintakeinon käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies*. Pidättämiseen oikeutetun poliisimiehen *tai suojelupoliisin päällystöön kuuluvan poliisimiehen* määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

LUONNOS

Voimassa oleva laki

57 §

Kiireellisessä tilanteessa saadun tiedon hävittäminen

Jos pidättämiseen oikeutettu poliisimies on 10 §:n 2 momentissa, 12 §:n 1 momentissa, 22 §:n 1 momentissa tai 24 §:n 1 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, henkilön teknisen seurannan tai teknisen laitetarkkailun aloittamisesta, mutta tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedonhankinnan käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin ylimääräistä tietoa saadaan käyttää 54 §:n mukaan.

58 §

Salaisen tiedonhankintakeinon käytöstä ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, *suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta,* teknisestä tarkkailusta ja valvotusta läpilaskusta on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu. Salaisen tiedonhankintakeinon käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

— — — — — — — — — — — — — — —

61 §

Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin

— — — — — — — — — — — — — — —

Poliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua varten tarpeellisen yhteyden kytkemi-

Ehdotus

57 §

Kiireellisessä tilanteessa saadun tiedon hävittäminen

Jos pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies* on 10 §:n 2 momentissa, 12 §:n 1 momentissa, 22 §:n 1 momentissa tai 24 §:n 1 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, henkilön teknisen seurannan tai teknisen laitetarkkailun aloittamisesta, mutta tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedonhankinnan käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin ylimääräistä tietoa saadaan käyttää 54 §:n mukaan.

58 §

Salaisen tiedonhankintakeinon käytöstä ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta, teknisestä tarkkailusta ja valvotusta läpilaskusta on viipymättä ilmoitettava tiedonhankinnan kohteelle kirjallisesti sen jälkeen, kun tiedonhankinnan tarkoitus on saavutettu. Salaisen tiedonhankintakeinon käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

— — — — — — — — — — — — — — —

61 §

Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin

— — — — — — — — — — — — — — —

Poliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua varten tarpeellisen yhteyden kytkemi-

LUONNOS

Voimassa oleva laki

seksi päästä myös muihin kuin teleyrityksen hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää pidättämiseen oikeutettu poliisimies. Kotietsinnästä säädetään erikseen.

63 §

Salaisen tiedonhankinnan valvonta

— — — — — — — — — — — — — — — —

Sisä*asiain*ministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta.

— — — — — — — — — — — — — — — —

(uusi)

(uusi)

Ehdotus

seksi päästä myös muihin kuin teleyrityksen hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää pidättämiseen oikeutettu poliisimies *tai suojelupoliisin päällystöön kuuluva poliisimies*. Kotietsinnästä säädetään erikseen.

63 §

Salaisen tiedonhankinnan valvonta

— — — — — — — — — — — — — — — —

Sisäministeriön on annettava eduskunnan oikeusasiamiehelle vuosittain kertomus salaisten tiedonhankintakeinojen ja niiden suojaamisen käytöstä ja valvonnasta.

— — — — — — — — — — — — — — — —

5 a luku

Siviilitiedustelun tiedustelumenetelmät

1 §

Siviilitiedustelu

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

2 §

Tiedustelumenetelmät

Tiedustelumenetelmiä ovat 5 luvussa tarkoitetut telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja ohjattu tietolähdetoiminta.

Tiedustelumenetelmiä ovat myös tässä lu-

LUONNOS

Voimassa oleva laki

Ehdotus

vussa tarkoitetut paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten ja tietojen saanti yksityiseltä yhteisöltä.

Tässä luvussa säädetään siitä, millä edellytyksillä 1 momentissa tarkoitettuja tiedustelumenetelmiä sekä paikkatiedustelua, jäljentämistä, lähetyksen pysäyttämistä jäljentämistä varten ja tietojen saantia yksityiseltä yhteisöltä käytetään siviilitiedustelussa.

Tietoliikennetiedustelusta tiedustelumenetelmänä siviilitiedustelussa säädetään tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa (/).

(uusi)

3 §

Siviilitiedustelun kohteet

Tiedustelumenetelmällä saadaan hankkia tietoa:

1) terrorismista;

2) ulkomaisesta tiedustelutoiminnasta;

3) joukkotuhoaseiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;

4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1992) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelusta, valmistamisesta, levittämisestä ja käytöstä;

5) kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminnasta;

6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaavasta toiminnasta;

7) vieraan valtion toiminnasta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille;

8) kansainvälistä rauhaa ja turvallisuutta uhkaavasta kriisistä;

9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaavasta toiminnasta;

10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaavasta toiminnasta; sekä

11) yhteiskuntajärjestystä uhkaavasta kansainvälisestä järjestäytyneestä rikollisuudesta.

LUONNOS

Voimassa oleva laki

(uusi)

Ehdotus

4 §

Tiedustelumenetelmien käytön edellytykset

Tiedustelumenetelmän käytön yleisenä edellytyksenä on, että sillä voidaan perustellusti olettaa saatavan tietoja sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Sen lisäksi, mitä tiedustelumenetelmien käytön erityisistä edellytyksistä jäljempänä säädetään, telekuuntelua, tietojen hankkimista telekuuntelun sijasta, suunnitelmallista tarkkailua, teknistä kuuntelua, teknistä katselua, henkilön teknistä seurantaa, teknistä laitetarkkailua, peitetoimintaa, valeostoa, tietolähteen ohjattua käyttöä ja paikkatiedustelua saadaan käyttää vain, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi 1 momentissa tarkoitetusta toiminnasta. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että menetelmän käyttö on välttämätöntä. Peitetoiminnan käyttäminen edellyttää myös, että tiedonhankintaa on toiminnan suunnitelmallisuuden, järjestäytyneisyyden tai ammattimaisuuden taikka ennakoitavissa olevan jatkuvuuden tai toistuvuuden vuoksi pidettävä tarpeellisena.

Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan tai siihen rinnastuvan tahoon, tiedustelumenetelmän käytön edellytyksistä säädetään 1 momentissa.

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

Tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

LUONNOS

Voimassa oleva laki

(uusi)

Ehdotus

5 §

Tiedonhankinnan jatkaminen eräiden rikosten estämiseksi ja paljastamiseksi

Jos tiedustelumenetelmän käytön aikana ilmenee, että henkilön voidaan perustellusti olettaa syyllistyvän 5 luvun 3 §:ssä mainittuun rikokseen taikka valtiopetokseen, törkeään valtiopetokseen tai laittomaan sotilaalliseen toimintaan tai voidaan olettaa, että sellainen rikos on tehty eikä tiedustelumenetelmän käytöllä enää voida olettaa saatavan tietoja luvan tai päätöksen perusteena olevasta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta, suojelupoliisi saa jatkaa tiedustelumenetelmän käyttöä 5 luvussa tarkoitettuna salaisena tiedonhankintana rikoksen estämiseksi ja paljastamiseksi tämän luvun nojalla annetun luvan voimassaolon ajan, enintään kuitenkin kuukauden ajan. Jos rikoksen estämiseksi tai paljastamiseksi on tarpeen käyttää 5 luvussa tarkoitettua salaista tiedonhankintakeinoa, asia on saatettava mainitun ajan kuluessa sen viranomaisen ratkaistavaksi, joka on toimivaltainen päättämään kysymyksessä olevan tiedonhankintakeinon käyttämisestä.

(uusi)

6 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Lupa telekuunteluun tai tietojen hankkimiseen telekuuntelun sijasta voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan. Silloin, kun toimenpiteen kohteena on henkilö, lupa voidaan antaa enintään kolmeksi kuukaudeksi kerrallaan.

Telekuuntelua ja telekuuntelun sijasta toimitettavaa tietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite;

LUONNOS

Voimassa oleva laki

Ehdotus

3) tosiseikat, joihin telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen edellytykset ja kohdistaminen perustuvat;

4) telekuuntelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;

5) telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset telekuuntelun tai telekuuntelun sijasta toimitettavan tietojen hankkimisen rajoitukset ja ehdot.

(uusi)

7 §

Televalvonnasta päättäminen

Tuomioistuin päättää televalvonnasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos televalvontaa koskeva asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Suojelupoliisi saa tietojen hankkimiseksi siviilitiedustelun kohteena olevasta toiminnasta kohdistaa televalvontaa henkilön suostumuksella tämän hallinnassa olevaan teleosoitteeseen tai telepäätelaitteeseen.

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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) toimenpide, sen tavoite sekä 3 §:ssä tar-

LUONNOS

Voimassa oleva laki

Ehdotus

koitettu toiminta;
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 suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset televalvonnan rajoitukset ja ehdot.

(uusi)

8 §

Tukiasematietojen hankkimisesta päättäminen

Tuomioistuin päättää tukiasematietojen hankkimisesta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä suojelupoliisin päällystöön kuuluva 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.
Lupa annetaan tietyksi ajanjaksoksi.
Tukiasematietojen hankkimista koskevassa vaatimuksessa ja päätöksessä on mainittava:
1) 3 §:ssä tarkoitettu toiminta;
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 suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset tukiasematietojen hankkimisen rajoitukset ja ehdot.

(uusi)

9 §

Suunnitelmallisesta tarkkailusta päättäminen

Suojelupoliisin päällystöön kuuluva polii-

LUONNOS

Voimassa oleva laki

Ehdotus

simies päättää suunnitelmallisesta tarkkailusta.

Suunnitelmallista tarkkailua koskeva päätös voidaan tehdä kerrallaan enintään kuudeksi kuukaudeksi.

Päätös suunnitelmallisesta tarkkailusta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä;

3) tosiseikat, joihin suunnitelmallisen tarkkailun edellytykset ja kohdistaminen perustuvat;

4) luvan voimassaoloaika;

5) suunnitelmallisen tarkkailun suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset suunnitelmallisen tarkkailun rajoitukset ja ehdot.

(uusi)

10 §

Peitellystä tiedonhankinnasta päättäminen

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää peitellystä tiedonhankinnasta.

Päätös peitellystä tiedonhankinnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) toimenpide ja sen tavoite riittävästi yksilöityinä;

2) 3 §:ssä tarkoitettu toiminta;

3) toimenpiteen kohteena oleva henkilö tai henkilöryhmä;

4) tosiseikat, joihin peitellyn tiedonhankinnan edellytykset ja kohdistaminen perustuvat;

5) peitellyn tiedonhankinnan suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) toimenpiteen suunniteltu toteuttamisajankohta;

7) mahdolliset peitellyn tiedonhankinnan rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

LUONNOS

Voimassa oleva laki

Ehdotus

Jos toimenpide ei siedä viivytystä, 1 momentissa tarkoitettua päätöstä ei tarvitse laatia kirjallisesti ennen peiteltyä tiedonhankintaa. Päätös on kuitenkin laadittava kirjallisesti viipymättä toimenpiteen jälkeen.

(uusi)

11 §

Teknisestä kuuntelusta päättäminen

Tuomioistuin päättää vapautensa menettäneen henkilön teknisestä kuuntelusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä kuuntelusta.

Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä kuuntelua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä taikka tila tai muu paikka;

3) tosiseikat, joihin teknisen kuuntelun edellytykset ja kohdistaminen perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) teknisen kuuntelun suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset teknisen kuuntelun rajoitukset ja ehdot.

(uusi)

12 §

Teknisestä katselusta päättäminen

Tuomioistuin päättää vapautensa menettä-

LUONNOS

Voimassa oleva laki

Ehdotus

neen henkilön teknisestä katselusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää teknisestä katselusta 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.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva henkilö tai henkilöryhmä taikka tila tai muu paikka;

3) tosiseikat, joihin teknisen katselun edellytykset ja kohdistaminen perustuvat;

4) luvan voimassaoloaika kellonajan tarkkuudella;

5) teknisen katselun suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset teknisen katselun rajoitukset ja ehdot.

(uusi)

13 §

Teknisestä seurannasta päättäminen

Tuomioistuin päättää henkilön teknisestä seurannasta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva 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.

LUONNOS

Voimassa oleva laki

Ehdotus

Suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta teknisestä seurannasta.

Lupa voidaan antaa ja päätös tehdä enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä seurantaa koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva 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 suojelupoliisin päällystöön kuuluva poliisimies;

6) mahdolliset teknisen seurannan rajoitukset ja ehdot.

(uusi)

14 §

Teknisestä laitetarkkailusta päättäminen

Tuomioistuin päättää teknisestä laitetarkkailusta suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos asia ei siedä viivytystä, suojelupoliisin päällystöön kuuluva 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.

Lupa voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

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 suojelupoliisin päällystöön kuuluva poliisimies;

LUONNOS

Voimassa oleva laki

Ehdotus

6) mahdolliset teknisen laitetarkkailun rajoitukset ja ehdot.

(uusi)

15 §

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen

Suojelupoliisi saa hankkia teknisellä laitteella teleosoitteen tai telepäätelaitteen yksilöintitiedot.

Viestintävirasto tarkastaa, ettei tekninen laite ominaisuuksiensa vuoksi aiheuta haitallista häiriötä yleisen viestintäverkon laitteille tai palveluille.

Teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisesta päättää suojelupoliisin päällystöön kuuluva poliisimies.

(uusi)

16 §

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen

Suojelupoliisin palveluksessa olevalla virkamiehellä on oikeus sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan ja tekniseen laitetarkkailuun, käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan taikka tietojärjestelmään, jos mainitun tiedustelumenetelmän käytön toteuttaminen sitä edellyttää. Suojelupoliisin palveluksessa olevalla 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.

Telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan ja tekniseen laitetarkkailuun käytettävän laitteen, menetelmän tai ohjelmiston saa asentaa vakituiseen asumiseen käytettä-

LUONNOS

Voimassa oleva laki

Ehdotus

vään tilaan vain, jos tuomioistuin on antanut siihen luvan suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Edellä 1 momentissa tarkoitetun toimenpiteen kohteena ei saa olla sellainen esine, aine, omaisuus, tila tai muu paikka, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11–14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta. tai johon ei pakkokeinolain 7 luvun 3 §:n nojalla saa kohdistaa takavarikkoa tai asiakirjan jäljentämistä, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

(uusi)

17 §

Peitetoimintaa koskeva esitys ja suunnitelma

Peitetoimintaa koskevassa esityksessä on mainittava:

1) toimenpiteen esittäjä;

2) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöityinä;

3) 3 §:ssä tarkoitettu toiminta;

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.

(uusi)

18 §

Peitetoiminnasta päättäminen

Suojelupoliisin päällikkö päättää 16 §:ssä tarkoitetusta peitetoiminnasta. Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättää suojelupoliisin päällikkö taikka tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Peitetoimintaa koskeva päätös voidaan an-

LUONNOS

Voimassa oleva laki

Ehdotus

taa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös peitetoiminnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) toimenpiteen esittäjä;

2) peitetoiminnan toteuttamisesta vastaava poliisimies;

3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä;

4) 3 §:ssä tarkoitettu toiminta;

5) tiedonhankinnan kohteena oleva henkilö tai henkilöryhmä riittävästi yksilöityinä;

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.

(uusi)

19 §

Rikoksentekokielto

Peitetoimintaa suorittava suojelupoliisin poliisimies ei saa tehdä rikosta eikä aloitetta rikoksen tekemiseen.

Jos peitetoimintaa suorittava suojelupoliisin poliisimies tekee liikennerikkomuksen, järjestysrikkomuksen tai muun niihin rinnastettavan rikoksen, josta on säädetty rangaistukseksi rikesakko, hän on rangaistusvastuusta vapaa, jos teko on ollut välttämätön peitetoiminnan tavoitteen saavuttamiseksi tai tiedonhankinnan paljastumisen estämiseksi.

(uusi)

20 §

Valeostosta päättäminen

Suojelupoliisin päällikkö päättää valeostosta. Yksinomaan yleisön saataville toimitetusta myyntitarjouksesta tehtävästä valeostosta saa päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisi-

LUONNOS

Voimassa oleva laki | *Ehdotus*

mies.

Valeostoa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös valeostosta on tehtävä kirjallisesti. Päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

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.

(uusi)

21 §

Valeoston toteuttamista koskeva suunnitelma

Valeoston toteuttamisesta on laadittava kirjallinen suunnitelma, jos se on tarpeen toiminnan laajuuden tai muun vastaavan syyn vuoksi.

Valeoston toteuttamista koskevaa suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava.

(uusi)

22 §

Valeoston toteuttamista koskeva päätös

Päätös valeoston toteuttamisesta on tehtävä kirjallisesti. Päätöksen tekee valeoston toteuttamisesta vastaava tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Päätöksessä on mainittava:

1) valeostosta päättänyt poliisimies, päätöksen antopäivä ja sisältö;

2) tunnistetiedot valeoston suorittavista poliisimiehistä;

3) selvitys siitä, miten on varmistuttu, että valeosto ei saa sen kohteena olevaa tai muuta henkilöä tekemään rikosta, jota hän ei muuten tekisi;

LUONNOS

Voimassa oleva laki

Ehdotus

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.

(uusi)

23 §

Poliisimiehen turvaaminen peitellyssä tiedonhankinnassa, peitetoiminnassa, valeostossa ja tietolähdetoiminnassa

Suojelupoliisin päällystöön kuuluva poliisimies saa päättää, että tässä luvussa tarkoitettua peiteltyä tiedonhankintaa, peitetoimintaa tai valeostoa toteuttava sekä tietolähdetoimintaa valmisteleva tai toteuttava poliisimies 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 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.

(uusi)

24 §

Tietolähteen ohjatusta käytöstä päättäminen

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää tietolähteen ohjatusta käytöstä.

Tietolähteen ohjattua käyttöä koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös tietolähteen ohjatusta käytöstä on tehtävä kirjallisesti. Päätöksessä on mainit-

LUONNOS

Voimassa oleva laki

Ehdotus

tava:
1) toimenpiteen esittäjä;
2) tiedonhankinnan toteuttamisesta vastaava poliisimies;
3) tunnistetiedot tietolähteestä;
4) 3 §:ssä tarkoitettu toiminta;
5) tiedonhankinnan tavoite ja toteuttamissuunnitelma;
6) päätöksen voimassaoloaika;
7) mahdolliset tietolähteen ohjatun käytön rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. Tietolähteen ohjatun käytön lopettamisesta on tehtävä kirjallinen päätös.

Tietolähdettä koskevien tietojen tallettamisesta henkilörekisteriin ja palkkion maksamisesta säädetään 5 luvun 41 §:ssä.

(uusi)

25 §

Tietolähteen turvaaminen

Suojelupoliisi 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.

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.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää, että tietolähde tämän suostumuksella varustetaan kuuntelun ja katselun mahdollistavalla teknisellä laitteella, jos varustaminen on yksittäis-

LUONNOS

Voimassa oleva laki

Ehdotus

tapauksessa välttämätöntä hänen turvallisuutensa varmistamiseksi. Kuuntelu ja katselu saadaan tallentaa. Tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita tietolähteen turvaamiseen.

(uusi)

26 §

Paikkatiedustelu

Paikkatiedustelulla tarkoitetaan muussa kuin vakituiseen asumiseen käytettävässä tilassa tai sellaisessa tilassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

(uusi)

27 §

Paikkatiedustelusta päättäminen

Tuomioistuin päättää paikkatiedustelusta, kun se kohdistuu kotirauhan suojaamaan paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai yleinen pääsy siihen on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana, tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Jos 1 momentissa tarkoitettu asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies 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.

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.

LUONNOS

Voimassa oleva laki

Ehdotus

Lupa voidaan antaa ja päätös tehdä enintään kuukaudeksi kerrallaan.

Paikkatiedustelu koskevassa vaatimuksessa tai päätöksessä on riittävällä tarkkuudella yksilöitävä:

1) 3 §:ssä tarkoitettu toiminta;

2) paikkatiedustelun kohteena oleva paikka;

3) ne tosiseikat, 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.

Jos paikkatiedustelun aikana ilmenee, että tiedustelu on kohdistunut tietoon, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20, 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, on tiedustelu siltä osin heti lopetettava ja tietoa koskevat muistiinpanot ja jäljennökset heti hävitettävä.

(uusi)

28 §

Jäljentäminen

Suojelupoliisilla on oikeus jäljentää asiakirja tai esine.

(uusi)

29 §

Jäljentämiskiellot

Asiakirjaa tai muuta 26 §:ssä tarkoitettua kohdetta ei saa jäljentää, jos se sisältää tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 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

LUONNOS

Voimassa oleva laki

Ehdotus

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, 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.

(uusi)

30 §

Telekuunteluun, televalvontaan ja tukiasematietoihin liittyvät jäljentämiskiellot

Sähköisen viestinnän palveluista annetun lain 3 §:n 27 kohdassa tarkoitetun teleyrityksen (teleyritys) tai mainitun lain 3 §:n 36 kohdassa tarkoitetun yhteisötilaajan 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.

(uusi)

31 §

Lähetyksen jäljentäminen

Suojelupoliisilla on oikeus jäljentää kirje tai muu lähetys ennen sen saapumista vastaanottajalle.

(uusi)

32 §

Lähetyksen pysäyttäminen jäljentämistä varten

Jos on syytä olettaa, että kirje tai muu lähetys, joka voidaan jäljentää, on tulossa postin toimipisteeseen, rautatieliikennepaikkaan tai sen osaan tai lähetysten kuljetusta ammatikseen liikennöinnin yhteydessä tai muuten harjoittavan toimipaikkaan taikka on jo siel-

LUONNOS

Voimassa oleva laki

Ehdotus

lä, tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa määrätä lähetyksen pidettäväksi mainitussa toimipaikassa, kunnes jäljentäminen on ehditty suorittaa.

Määräys annetaan enintään kuukauden määräajaksi, joka alkaa siitä, kun toimipaikan esimies on saanut tiedon määräyksestä. Lähetystä ei saa ilman 1 momentissa tarkoitetun virkamiehen lupaa luovuttaa muulle kuin hänelle tai hänen määräämälleen henkilölle.

Toimipaikan esimiehen on heti ilmoitettava määräyksen antajalle lähetyksen saapumisesta. Tämän on ilman aiheetonta viivytystä päätettävä jäljentämisestä.

(uusi)

33 §

Jäljentämisestä päättäminen

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää jäljentämisestä.

Jos asia ei siedä viivytystä, myös muu kuin 1 momentissa tarkoitettu suojelupoliisin poliisimies saa yksittäistapauksessa päättää jäljentämisestä, kunnes 1 momentissa tarkoitettu poliisimies on ratkaissut asian. Asia on saatettava 1 momentissa tarkoitetun poliisimiehen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedonhankintakeinon käytön aloittamisesta.

(uusi)

34 §

Jäljennöksen hävittäminen

Jäljennös on hävitettävä viipymättä, jos käy ilmi, että jäljentäminen on kohdistunut jäljentämiskiellon alaiseen materiaaliin tai tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi.

LUONNOS

Voimassa oleva laki

(uusi)

Ehdotus

35 §

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 tiedustelumenetelmäkohtaisesti. 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 suullisesta 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 tietoturvallisuusjärjes-

LUONNOS

Voimassa oleva laki

Ehdotus

telyin.

(uusi)

36 §

Siviilitiedustelun suojaaminen

Suojelupoliisi 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 siviilitiedustelun suojaamiseksi.

Edellä 1 momentissa tarkoitettu rekisterimerkintä on oikaistava sen jälkeen, kun momentissa tarkoitettuja edellytyksiä ei enää ole.

(uusi)

37 §

Suojaamisesta päättäminen

Suojelupoliisin päällikkö päättää 36 §:n 1 momentissa tarkoitetun rekisterimerkinnän tekemisestä sekä asiakirjan valmistamisesta.

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 36 §:n 1 momentissa tarkoitetusta suojaamisesta.

Rekisterimerkintöjen tekemisestä sekä asiakirjojen valmistamisesta päättäneen viranomaisen on pidettävä luetteloa merkinnöistä ja asiakirjoista, valvottava niiden käyttöä sekä huolehdittava merkintöjen oikaisemisesta.

(uusi)

38 §

Ilmaisukielto

Tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa kieltää sivullista ilmaisemasta tämän tietoon tulleita seikkoja tiedustelumenetelmän käytöstä, jos se on perusteltua tiedustelumenetelmän käytön suojaamiseksi. Edellytyksenä on lisäksi, että sivullinen on tehtävänsä tai asemansa johdosta avustanut tai häntä on pyydetty avustamaan tiedustelumenetelmän käytön toteuttamisessa.

LUONNOS

Voimassa oleva laki

Ehdotus

Ilmaisukielto annetaan enintään vuodeksi kerrallaan. Kielto on annettava saajalleen kirjallisena todisteellisesti tiedoksi. Siinä on yksilöitävä kiellon kohteena olevat seikat, mainittava kiellon voimassaoloaika ja ilmoitettava sen rikkomiseen liittyvästä rangaistusuhasta.

Ilmaisukieltoa koskevaan päätökseen ei saa hakea muutosta valittamalla. Kiellon saanut saa kuitenkin ilman määräaikaa kannella Helsingin hovioikeudelle. Kantelu on käsiteltävä kiireellisenä.

Rangaistus ilmaisukiellon rikkomisesta tuomitaan rikoslain 38 luvun 1 tai 2 §:n mukaan, jollei teosta muualla laissa säädetä ankarampaa rangaistusta.

Ilmaisukiellon saanut saa 4 momentin estämättä ilmoittaa ilmaisukiellosta tiedusteluvaltuutetulle.

(uusi)

39 §

Tiedustelumenetelmän käytöstä päättäminen eräissä tapauksissa

Muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättää suojelupoliisin päällikkö.

Tiedustelumenetelmän käyttöä koskevan päätöksen, esityksen ja suunnitelman sisällön osalta noudatetaan mitä esityksestä, suunnitelmasta, vaatimuksesta tai päätöksestä tässä luvussa säädetään.

Tämän luvun 4 §:n 4 momentin, 41, 44, 46 ja 47 §:n säännöksiä voidaan soveltaa 1 momentissa tarkoitettuun siviilitiedusteluun ja tiedustelumenetelmän käyttöön.

(uusi)

40 §

Määräaikojen laskeminen

Tässä luvussa tarkoitettujen määräaikojen laskemiseen ei sovelleta säädettyjen määräaikain laskemisesta annettua lakia (150/1930).

Aika, joka on määrätty kuukausina, päättyy sinä määräkuukauden päivänä, joka järjestysnumeroltaan vastaa sanottua päivää. Jos vastaavaa päivää ei ole siinä kuussa, jona

LUONNOS

Voimassa oleva laki

Ehdotus

määräaika päättyy, määräaika päättyy kuukauden viimeisenä päivänä.

(uusi)

41 §

Kuuntelu- ja katselukiellot

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua ja teknistä katselua ei saa kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16, 20 tai 22 §:n 2 momentin nojalla.

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.

Tässä pykälässä tarkoitetut kuuntelu- ja katselukiellot eivät kuitenkaan koske tapauksia, joissa 1 momentissa tarkoitettu henkilö osallistuu siviilitiedustelun kohteena olevaan toimintaan, joka vakavasti uhkaa kansallista turvallisuutta ja myös hänen osaltaan on tehty päätös telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, teknisestä kuuntelusta tai teknisestä katselusta.

(uusi)

42 §

Tallenteiden ja asiakirjojen tarkastaminen

Suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen on ilman aiheetonta viivytystä tarkastettava tiedustelumenetelmän käytössä kertyneet tallenteet ja asiakirjat.

(uusi)

43 §

Tallenteiden tutkiminen

Tiedustelumenetelmien käytössä kertyneitä tallenteita saa tutkia vain tuomioistuin ja suojelupoliisin päällystöön kuuluva poliisi-

LUONNOS

Voimassa oleva laki

Ehdotus

mies. Suojelupoliisin päällystöön kuuluvan poliisimiehen määräyksestä tai tuomioistuimen osoituksen mukaan tallennetta saa tutkia myös muu poliisimies, asiantuntija tai muu henkilö, jota käytetään apuna tiedonhankintaa toteutettaessa.

(uusi)

44 §

Tiedon luovuttaminen rikostorjuntaan

Suojelupoliisin on ilman aiheetonta viivytystä ilmoitettava keskusrikospoliisille, jos tiedustelumenetelmän käytön aikana ilmenee, että voidaan olettaa tehdyksi sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Ilmoitusta saadaan suojelupoliisin päällikön päätöksellä siirtää enintään vuodeksi kerrallaan, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi tai hengen tai terveyden suojaamiseksi. Suojelupoliisi saa ilmoittaa tehdystä rikoksesta keskusrikospoliisille, jos rikoksesta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta.

Suojelupoliisin on viipymättä ilmoitettava toimivaltaiselle viranomaiselle, jos tiedustelumenetelmän käytön aikana ilmenee, että hankkeilla on sellainen rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä. Tiedustelumenetelmän käytöllä saatua tietoa saa luovuttaa toimivaltaiselle viranomaiselle sellaisen rikoksen estämiseksi, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta.

Kun harkitaan 1 momentissa tarkoitettua ilmoituksen siirtämistä tai 1 ja 2 momentissa tarkoitettua ilmoituksen tekemistä tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kolme vuotta vankeutta tai sellaisen rikoksen estämisestä, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta, arvioinnissa on otettava huomioon rikoksen selvittämisen tai rikoksen estämisen merkitys yleisen ja yksityisen edun kannalta.

Tiedustelumenetelmän käytöllä saatua tietoa saa aina luovuttaa syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran

LUONNOS

Voimassa oleva laki

Ehdotus

taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Jos esitutkintaviranomainen käynnistää esitutkinnan tai ryhtyy esitutkintatoimenpiteen käyttämiseen taikka toimivaltainen viranomainen käynnistää rikoksen estämiseen tähtäävän toimenpiteen tässä pykälässä tarkoitetun ilmoituksen perusteella, on esitutkintaviranomaisen tai toimivaltaisen viranomaisen ennen esitutkinnan käynnistämistä tai esitutkintatoimenpiteen käyttämistä taikka rikoksen estämiseen tähtäävän toimenpiteen käynnistämistä ilmoitettava siitä suojelupoliisille.

(uusi)

45 §

Tiedustelutietojen hävittäminen

Tiedustelumenetelmällä saatu tieto on hävitettävä viipymättä sen jälkeen, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi.

Tieto voidaan kuitenkin säilyttää ja tallettaa henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin, jos tämä on tarpeen 44 §:ssä tarkoitetuissa tapauksissa.

Edellä 7 §:ssä tarkoitetut tukiasematiedot on hävitettävä, kun on käynyt ilmi, ettei tietoa tarvita kansallisen turvallisuuden suojaamiseksi.

(uusi)

46 §

Kiiretilanteessa saadun tiedon hävittäminen

Jos suojelupoliisin päällystöön kuuluva poliisimies on 7 §:n 1 momentissa, 8 §:n 1 momentissa, 11 §:n 1 momentissa, 12 §:n 1 momentissa, 13 §:n 1 momentissa, 14 §:n 1 momentissa tai 27 §:n 2 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt televalvonnan, tukiasematietojen hankkimisen, teknisen kuuntelun, teknisen katselun, henkilön teknisen seurannan, teknisen laitetarkkailun tai paikkatiedustelun aloittamisesta, mutta tuomioistuin katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö on lopetettava sekä sillä saatu ai-

LUONNOS

Voimassa oleva laki

Ehdotus

neisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

Jos suojelupoliisin poliisimies on 33§:n 2 momentissa tarkoitetussa kiireellisessä tilanteessa päättänyt jäljentämisestä, mutta tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies katsoo, että edellytyksiä toimenpiteelle ei ole ollut, tiedustelumenetelmän käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää samoin edellytyksin kuin tietoa saadaan käyttää 44 §:n 1 momentissa tai 2 momentissa tarkoitetuissa tapauksissa, jos voidaan olettaa tehdyksi rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta tai jos ilmenee, että hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

(uusi)

47 §

Tiedustelumenetelmän käytöstä ilmoittaminen

Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä sekä viestiin kohdistuvasta jäljentämisestä tai viestiin kohdistuvasta lähetyksen jäljentämisestä on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu. Tiedustelumenetelmän käytöstä on kuitenkin ilmoitettava tiedonhankinnan kohteelle viimeistään vuoden kuluttua sen käytön lopettamisesta.

LUONNOS

Voimassa oleva laki

Ehdotus

Tuomioistuin voi suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta päättää, että 1 momentissa tarkoitettua ilmoitusta kohteelle saadaan lykätä enintään kaksi vuotta kerrallaan, jos se on perusteltua käynnissä olevan tiedustelumenetelmän käytön turvaamiseksi, kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi. Ilmoitus saadaan tuomioistuimen päätöksellä jättää kokonaan tekemättä, jos se on välttämätöntä kansallisen turvallisuuden varmistamiseksi taikka hengen tai terveyden suojaamiseksi.

Jos tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Kohteelle ilmoittamisesta on samalla annettava kirjallisesti tieto luvan myöntäneelle tuomioistuimelle.

Jos suojelupoliisi jatkaa tiedonhankintaa 5 §:n perusteella, noudatetaan mitä salaisen tiedonhankintakeinon käytöstä ilmoittamisesta 5 luvun 58 §:ssä säädetään.

Suunnitelmallisesta tarkkailusta, peitellystä tiedonhankinnasta, peitetoiminnasta, valeostosta, tietolähteen ohjatusta käytöstä, paikkatiedustelusta, muuhun kuin viestiin kohdistuvasta jäljentämisestä ja muuhun kuin viestiin kohdistuvasta lähetyksen jäljentämisestä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain 10 luvun 60 §:n 2–7 momentissa säädetään.

Tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, kun tiedonhankinnan kohteena on ollut 4 §:n 3 momentissa mainittu valtiollinen toimija.

Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan mitä 35 §:ssä säädetään.

LUONNOS

Voimassa oleva laki | *Ehdotus*

(uusi)

48 §

Pöytäkirja

Tiedustelumenetelmän käytön lopettamisen jälkeen on laadittava ilman aiheetonta viivytystä pöytäkirja.

(uusi)

49 §

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 luvussa tarkoitetun tiedustelumenetelmän käytöstä, ennen kuin 47 §:ssä tarkoitettu ilmoitus on tehty.

Rekisteröidyn tarkastusoikeudesta säädetään henkilötietojen käsittelystä poliisitoimessa annetussa laissa.

(uusi)

50 §

Tietojen saanti yksityiseltä yhteisöltä

Suojelupoliisilla on suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä oikeus saada yhteisön jäsentä, tilintarkastajaa, toimitusjohtajaa, hallituksen jäsentä tai työntekijää velvoittavan yritys-, pankki- tai vakuutussalaisuuden estämättä sellaisia tietoja, joiden yksittäistapauksessa voidaan olettaa olevan tarpeen sellaisen siviilitiedustelun kohteena olevan toiminnan selvittämisessä, joka vakavasti uhkaa kansallista turvallisuutta, ja jolla voidaan olettaa olevan merkitystä:

1) siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön tunnistamiseksi, tavoittamiseksi tai yhteystietojen selvittämiseksi taikka tällaisen henkilön liikkumisen selvittämiseksi;

2) tiedustelumenetelmän käytön kohdentamiseksi tiettyyn siviilitiedustelun kohteena olevaan henkilöön; tai

3) siviilitiedustelun kohteena olevan henkilön tai oikeushenkilön 3 §:ssä tarkoitettuun toimintaan oletettavasti kytkeytyvän taloudel-

LUONNOS

Voimassa oleva laki

Ehdotus

lisen toiminnan selvittämiseksi.

(uusi)

51 §

Teleyrityksen avustamisvelvollisuus ja pääsy eräisiin tiloihin

Teleyrityksen avustamisvelvollisuuteen sovelletaan mitä 5 luvun 61 §:ssä säädetään teleyrityksen avustamisvelvollisuudesta ja pääsystä eräisiin tiloihin.

(uusi)

52 §

Korvaus teleyritykselle

Teleyrityksen oikeudesta korvaukseen sovelletaan mitä 5 luvun 62 §:ssä säädetään korvauksesta teleyritykselle.

(uusi)

53 §

Teleyrityksen säilyttämien tietojen käyttäminen

Sen lisäksi mitä sähköisen viestinnän palveluista annetun lain 157 §:n 1 momentissa säädetään säilytettävien tietojen käyttämisestä, säilytettäviä tietoja saadaan käyttää myös, jos niillä voidaan perustellusti olettaa olevan erittäin tärkeä merkitys tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

(uusi)

54 §

Yhteistyö sotilastiedusteluviranomaisen kanssa

Suojelupoliisin on toimittava yhteistyössä sotilastiedusteluviranomaisen kanssa tiedustelun tarkoituksenmukaiseksi hoitamiseksi sekä annettava sotilastiedusteluviranomaiselle tässä tarkoituksessa tarpeellisia tietoja sen estämättä mitä salassapitovelvollisuudesta säädetään.

LUONNOS

Voimassa oleva laki

(uusi)

Ehdotus

55 §

Yhteistyö muiden viranomaisten ja yhteisöjen kanssa

Suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi.

Suojelupoliisi voi tehtävänsä toteuttamiseksi toimia yhteistyössä yhteisöjen kanssa sekä luovuttaa muille viranomaisille ja yhteisöille salassapitosäännösten estämättä tietoja, jos tietojen luovuttaminen on välttämätöntä kansallisen turvallisuuden suojaamiseksi.

Tietojen luovuttamisesta rikostorjuntaan säädetään 44 §:ssä.

(uusi)

56 §

Salaisen tiedonhankinnan yhteensovittaminen

Tässä luvussa säädettyjen tiedustelumenetelmien käyttöä voidaan yhteen sovittaa suojelupoliisin, sotilastiedusteluviranomaisen, keskusrikospoliisin ja muun viranomaisen virkamiesten työturvallisuuden varmistamiseksi sekä salaisessa tiedonhankinnassa käytettävien taktisten ja teknisten menetelmien ja suunnitelmien paljastumisen estämiseksi.

(uusi)

57 §

Kansainvälinen yhteistyö

Suojelupoliisi voi tehdä yhteistyötä sekä toteuttaa tiedonhankintaa yhdessä ulkomaisten turvallisuus- ja tiedustelupalveluiden kanssa kansallisen turvallisuuden suojaamiseksi.

Jos yhteinen tiedonhankinta toteutetaan yhteistyössä sen valtion kanssa, jonka alueella tiedustelumenetelmiä on tarkoitus käyttää, suojelupoliisin poliisimiehen on noudatettava niitä rajoituksia ja ehtoja tiedustelumenetelmien käytölle, jotka kyseinen valtio asettaa.

Suojelupoliisin päällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja tiedustelumenetelmien käytöstä. Vieraan valtion toimivaltaisella virkamiehellä on suojelupo-

LUONNOS

Voimassa oleva laki

Ehdotus

liisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä.

Suojelupoliisi voi salassapitosäännösten estämättä luovuttaa tietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua.

Henkilötietojen luovuttamiseen sovelletaan henkilötietojen käsittelystä poliisitoimessa annettua lakia (761/2003).

(uusi)

58 §

Tiedustelutoiminnan yhteensovittaminen

Siviili- ja sotilastiedustelutoimintaa sovitetaan yhteen tasavallan presidentin, valtioneuvoston kanslian, ulkoasiainministeriön, puolustusministeriön ja sisäministeriön sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken.

Jos siviilitiedustelutoiminnalla arvioidaan olevan ulko- ja turvallisuuspoliittisia vaikutuksia, asia on valmistelevasti käsiteltävä 1 momentissa tarkoitettujen viranomaisten kesken.

(uusi)

59 §

Siviilitiedustelun valvonta sisäasiainhallinnossa

Tässä luvussa tarkoitettua tiedonhankintaa valvoo suojelupoliisin päällikkö sekä sisäministeriö.

(uusi)

60 §

Siviilitiedustelun ulkoinen valvonta

Sisäministeriön on annettava eduskunnan oikeusasiamiehelle ja tiedusteluvaltuutetulle vuosittain kertomus tässä luvussa tarkoitettujen tiedustelumenetelmien ja siviilitiedustelun

LUONNOS

Voimassa oleva laki

Ehdotus

suojaamisen käytöstä ja valvonnasta.

Tiedusteluvaltuutetun harjoittamasta valvonnasta säädetään tiedustelutoiminnan valvonnasta annetussa laissa (/).

(uusi)

61 §

Tiedusteluvaltuutetulle tehtävät ilmoitukset

Suojelupoliisin on annettava tieto tiedusteluvaltuutetulle tämän luvun nojalla annetuista tuomioistuimen päätöksistä ja luvista mahdollisimman pian tuomioistuimen päätöksen jälkeen.

Suojelupoliisin on mahdollisimman pian ilmoitettava tiedusteluvaltuutetulle päätöksestä, joka koskee:

1) muuta kuin 1 momentissa tarkoitettua tiedustelumenetelmää;

2) siviilitiedustelun suojaamista;

3) ilmaisukieltoa;

4) 44 §:n 1 momentissa tarkoitetun ilmoituksen siirtämistä.

Tiedustelumenetelmää koskevan päätöksen ilmoittamisessa on kiinnitettävä erityistä huomiota salassapitovelvollisuuden toteutumiseen ja siihen, että asiakirjoihin ja tietojärjestelmiin sisältyvien tietojen suoja turvataan tarvittavin menettelytavoin ja tietoturvallisuusjärjestelyin.

(uusi)

62 §

Tarkemmat säännökset

Valtioneuvoston asetuksella voidaan säätää:

1) tiedustelumenetelmien käytön ja niiden suojaamisen järjestämisestä;

2) toimenpiteiden kirjaamisesta valvontaa varten;

3) siviilitiedustelun valvontaa varten annettavista selvityksistä;

4) rikostorjuntaan luovutettavan tiedon siirtämistä koskevasta menettelystä ja siinä yhteydessä annettavista tarpeellisista tiedoista;

5) suojelupoliisin ja sotilastiedusteluviranomaisen välisen yhteistyön järjestämisestä;

6) suojelupoliisin ja muiden viranomaisten

LUONNOS

Voimassa oleva laki

9 luku

Erinäiset säännökset

8 §

Liikkumis- ja oleskelurajoitukset

Erittäin tärkeän toiminnan tai omaisuuden turvaamiseksi taikka ihmisten suojaamiseksi voidaan sisä*asiain*ministeriön asetuksella rajoittaa liikkumista tai oleskelua turvattavassa tai suojattavassa kohteessa tai sen ympäristössä kohteesta aiheutuvan tai siihen kohdistuvan vaaran vuoksi taikka kieltää turvallisuutta vaarantavien esineiden tai aineiden tuonti sinne. Kiellon tai rajoituksen rikkomisesta voidaan tuomita sakkoon, jos teosta ei ole muualla laissa säädetty ankarampaa rangaistusta.

9 §

Kansainvälinen yhteistoiminta

— — — — — — — — — — — — — — — —

Sisä*asiain*ministeriö voi asioissa, jotka eivät kuulu lainsäädännön alaan tai muuten vaadi eduskunnan suostumusta, tehdä poliisin toimialaan kuuluvia, tavanomaisina pidettäviä yhteistoimintasopimuksia naapurivaltioiden, Itämeren rantavaltioiden ja Euroopan talousalueeseen kuuluvien valtioiden kanssa.

Ehdotus

välisen yhteistyön järjestämisestä;

7) salaisen tiedonhankinnan yhteensovittamisen järjestämisestä;

8) tiedustelutoiminnan yhteensovittamisen järjestämisestä.

Sisäministeriön asetuksella voidaan säätää:

1) siviilitiedustelun valvonnan järjestämisestä sisäasiainhallinnossa;

2) suojelupoliisin ja muun sisäasiainhallinnon välisen yhteistyön järjestämisestä;

3) suojelupoliisin kansainvälisen yhteistyön järjestämisestä.

9 luku

Erinäiset säännökset

8 §

Liikkumis- ja oleskelurajoitukset

Erittäin tärkeän toiminnan tai omaisuuden turvaamiseksi taikka ihmisten suojaamiseksi voidaan sisäministeriön asetuksella rajoittaa liikkumista tai oleskelua turvattavassa tai suojattavassa kohteessa tai sen ympäristössä kohteesta aiheutuvan tai siihen kohdistuvan vaaran vuoksi taikka kieltää turvallisuutta vaarantavien esineiden tai aineiden tuonti sinne. Kiellon tai rajoituksen rikkomisesta voidaan tuomita sakkoon, jos teosta ei ole muualla laissa säädetty ankarampaa rangaistusta.

9 §

Kansainvälinen yhteistoiminta

— — — — — — — — — — — — — — — —

Sisäministeriö voi asioissa, jotka eivät kuulu lainsäädännön alaan tai muuten vaadi eduskunnan suostumusta, tehdä poliisin toimialaan kuuluvia, tavanomaisina pidettäviä yhteistoimintasopimuksia naapurivaltioiden, Itämeren rantavaltioiden ja Euroopan talousalueeseen kuuluvien valtioiden kanssa.

LUONNOS

Voimassa oleva laki

10 §

Tarkemmat säännökset

— — — — — — — — — — — — — — —

Sisä*asiain*ministeriön asetuksella voidaan säätää tarkemmin:

1) poliisimiehen aseman ilmaisemisesta ja poliisimiehen yksilöimisestä huolehtimisesta;

2) haltuun otetun omaisuuden säilyttämisestä;

3) poliisitutkinnan suorittamisesta;

4) kulkuneuvon pysäyttämisessä käytettävistä merkeistä ja menetelmistä;

5) automaattisesta tieliikenteen valvonnasta;

6) voimakeinojen käytön määritelmistä, voimankäyttökoulutuksesta, voimankäytön harjoittelusta ja seurannasta, oikeudesta kantaa voimankäyttövälineitä, voimankäyttövälineiden säilyttämisestä sekä voimakeinojen käytön valvonnasta;

7) eläimen kiinniottamisesta, säilyttämisestä ja lopettamisesta;

8) virka-avun antamisesta muulle kuin tullilaitokselle tai rajavartiolaitokselle;

9) poliisitoimenpiteiden kirjaamisesta;

10) turvatarkastustoimenpiteiden teknisestä toteuttamisesta ja turvatarkastusten käytännön järjestämisestä sekä turvatarkastuksista järjestettävästä koulutuksesta;

11) virkapuvun mallista ja sen yhteydessä käytettävistä merkeistä sekä siitä, milloin virkatehtävän laatu tai luonne edellyttää virkapuvun käyttöä.

Ehdotus

10 §

Tarkemmat säännökset

— — — — — — — — — — — — — — —

Sisäministeriön asetuksella voidaan säätää tarkemmin:

1) poliisimiehen aseman ilmaisemisesta ja poliisimiehen yksilöimisestä huolehtimisesta;

2) haltuun otetun omaisuuden säilyttämisestä;

3) poliisitutkinnan suorittamisesta;

4) kulkuneuvon pysäyttämisessä käytettävistä merkeistä ja menetelmistä;

5) automaattisesta tieliikenteen valvonnasta;

6) voimakeinojen käytön määritelmistä, voimankäyttökoulutuksesta, voimankäytön harjoittelusta ja seurannasta, oikeudesta kantaa voimankäyttövälineitä, voimankäyttövälineiden säilyttämisestä sekä voimakeinojen käytön valvonnasta;

7) eläimen kiinniottamisesta, säilyttämisestä ja lopettamisesta;

8) virka-avun antamisesta muulle kuin tullilaitokselle tai rajavartiolaitokselle;

9) poliisitoimenpiteiden kirjaamisesta;

10) turvatarkastustoimenpiteiden teknisestä toteuttamisesta ja turvatarkastusten käytännön järjestämisestä sekä turvatarkastuksista järjestettävästä koulutuksesta;

11) virkapuvun mallista ja sen yhteydessä käytettävistä merkeistä sekä siitä, milloin virkatehtävän laatu tai luonne edellyttää virkapuvun käyttöä.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———

LUONNOS

3.

Laki

poliisin hallinnosta annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan poliisin hallinnosta annetun lain (110/1992) 10 §:n 1 ja 2 momentti, sellaisena kuin ne ovat laissa 860/2015, sekä
lisätään 15 a §:ään sellaisena kuin se on osaksi laissa 873/2011, uusi 3 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
10 §	10 §
Suojelupoliisi	*Suojelupoliisi*
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. 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*.	Suojelupoliisin tehtävänä on sisäministeriön ohjauksen mukaisesti *hankkia tietoa kansallisen turvallisuuden suojaamiseksi sekä havaita, estää ja paljastaa sellaisia toimintoja, hankkeita ja rikoksia*, jotka voivat *uhata* valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta yhteiskunnan turvallisuutta uhkaavan toiminnan havaitsemiseksi ja estämiseksi. Sisäministeriö määrää Poliisihallitusta kuultuaan tarvittaessa tarkemmin suojelupoliisin ja muiden poliisiyksiköiden välisestä yhteistoiminnasta ja yhteistyöstä.
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
15 a §	15 a §
Poliisivaltuudet	*Poliisivaltuudet*
— — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — —
(uusi)	*Sen lisäksi mitä 1 momentissa säädetään, suojelupoliisin virkamiehellä on oikeus käyttää poliisilain 5 a luvussa tarkoitettuja tiedustelumenetelmiä kansallisen turvallisuuden suojaamiseksi sen mukaan kuin mainitussa luvussa säädetään.*

———

Voimassa oleva laki	*Ehdotus*
	Tämä laki tulee voimaan päivänä kuuta 20 .

LUONNOS

4.

Laki

henkilötietojen käsittelystä poliisitoimessa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan henkilötietojen käsittelystä poliisitoimessa annetun lain (761/2003) 5 §:n 2 momentti, 13 §:n 1 momentin 2, 4, 6, 15 ja 16 kohta, 45 §:n 1 momentin 5 kohta,

sellaisina kuin niistä ovat 13 §:n 1 momentin 2 kohta laissa 1073/2015 ja 13 §:n 1 momentin 15 kohta laissa 29/2015, seuraavasti

Voimassa oleva laki	*Ehdotus*
5 §	5 §
Suojelupoliisin toiminnallinen tietojärjestelmä	*Suojelupoliisin toiminnallinen tietojärjestelmä*
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
Suojelupoliisin toiminnallinen tietojärjestelmä voi sisältää tietoja, joita on tarpeen käsitellä oikeus- ja yhteiskuntajärjestystä tai valtion turvallisuutta vaarantavien hankkeiden tai rikosten estämiseksi tai selvittämiseksi.	Suojelupoliisin toiminnallinen tietojärjestelmä voi sisältää tietoja, joita on tarpeen käsitellä *kansallisen turvallisuuden suojaamiseksi*, oikeus- ja yhteiskuntajärjestystä tai valtion turvallisuutta vaarantavien hankkeiden tai rikosten estämiseksi, *paljastamiseksi* tai selvittämiseksi.
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
13 §	13 §
Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä	*Poliisin oikeus saada tietoja eräistä rekistereistä ja tietojärjestelmistä*
Poliisilla on sen lisäksi, mitä muualla laissa säädetään, oikeus saada tehtäviensä suorittamista ja henkilörekisteriensä ylläpitämistä varten salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona tarpeellisia tietoja rekistereistä siten kuin asianomaisen rekisterinpitäjän kanssa sovitaan, seuraavasti:	Poliisilla on sen lisäksi, mitä muualla laissa säädetään, oikeus saada tehtäviensä suorittamista ja henkilörekisteriensä ylläpitämistä varten salassapitosäännösten estämättä teknisen käyttöyhteyden avulla tai tietojoukkona tarpeellisia tietoja rekistereistä siten kuin asianomaisen rekisterinpitäjän kanssa sovitaan, seuraavasti:
— — — — — — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — — — — — —
2) rikosten estämiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi tai henkilön luotettavuutta edellyttävän poliisin lupaa tai hyväksyntää varten henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain (1069/2015) 14 §:n 1 ja 2 momentissa säädetystä Rikosseuraamuslaitoksen tietojärjestel-	2) *kansallisen turvallisuuden suojaamiseksi*, rikosten estämiseksi, *paljastamiseksi ja* selvittämiseksi ja syyteharkintaan saattamiseksi tai henkilön luotettavuutta edellyttävän poliisin lupaa tai hyväksyntää varten henkilötietojen käsittelystä Rikosseuraamuslaitoksessa annetun lain (1069/2015) 14 §:n 1 ja 2

Voimassa oleva laki	*Ehdotus*
mästä tuomitusta, vangista ja Rikosseuraamuslaitoksen yksikköön otetusta henkilöstä;	momentissa säädetystä Rikosseuraamuslaitoksen tietojärjestelmästä tuomitusta, vangista ja Rikosseuraamuslaitoksen yksikköön otetusta henkilöstä;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
4) majoitus- ja ravitsemistoiminnasta annetun lain (308/2006) 6 §:n 1 momentissa tarkoitettuja matkustajatietoja majoitustoiminnan harjoittajilta yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikosten estämiseksi, paljastamiseksi tai selvittämiseksi ja poliisille laissa säädetyn muun tehtävän suorittamiseksi;	4) majoitus- ja ravitsemistoiminnasta annetun lain (308/2006) 6 §:n 1 momentissa tarkoitettuja matkustajatietoja majoitustoiminnan harjoittajilta *kansallisen turvallisuuden suojaamiseksi*, yleisen järjestyksen ja turvallisuuden ylläpitämiseksi sekä rikosten estämiseksi, paljastamiseksi tai selvittämiseksi ja poliisille laissa säädetyn muun tehtävän suorittamiseksi;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
6) Patentti- ja rekisterihallituksen kaupparekisteristä tiedot elinkeinonharjoittajia koskevista ilmoituksista ja tiedonannoista rikosten estämistä, paljastamista ja selvittämistä varten;	6) Patentti- ja rekisterihallituksen kaupparekisteristä tiedot elinkeinonharjoittajia koskevista ilmoituksista ja tiedonannoista *kansallisen turvallisuuden suojaamiseksi*, rikosten estämistä, paljastamista ja selvittämistä varten;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
15) panostajalain (219/2000) 3 §:ssä tarkoitetusta panostajarekisteristä valvonta- ja hälytystehtäviä sekä rikosten estämistä, selvittämistä ja paljastamista varten;	15) panostajalain (219/2000) 3 §:ssä tarkoitetusta panostajarekisteristä valvonta- ja hälytystehtäviä sekä *kansallisen turvallisuuden suojaamiseksi,* rikosten estämistä, selvittämistä ja paljastamista varten;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
16) rikosten estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi sekä etsintäkuulutettujen tavoittamiseksi yhteisöiltä ja yhtymiltä matkustajaa ja kulkuneuvon henkilökuntaa koskevista rekistereistä.	16) *kansallisen turvallisuuden suojaamiseksi,* rikosten estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi sekä etsintäkuulutettujen tavoittamiseksi yhteisöiltä ja yhtymiltä matkustajaa ja kulkuneuvon henkilökuntaa koskevista rekistereistä.
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
45 §	45 §
Tarkastusoikeuden rajoittaminen	*Tarkastusoikeuden rajoittaminen*
Tarkastusoikeutta ei ole lainkaan:	Tarkastusoikeutta ei ole lainkaan:
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
5) tietoihin, jotka on saatu poliisilain 5 luvun, pakkokeinolain 10 luvun sekä sähköisen viestinnän tietosuojalain 36 §:n mukaisia tiedonhankintamenetelmiä käyttäen;	5) tietoihin, jotka on saatu poliisilain *4* luvun *3 §:n, 5 ja 5 a luvun*, pakkokeinolain 10 luvun *tai siviilitiedustelusta tietoliikennetiedustelusta annetun lain* mukaisia *toimivaltuuksia* käyttäen;
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —

LUONNOS

Voimassa oleva laki	*Ehdotus*
	Tämä laki tulee voimaan päivänä kuuta 20 .

LUONNOS

5.

Laki

esitutkintalain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan esitutkintalain (805/2011) 2 luvun 1 §:n 1 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
2 luku	2 luku
Esitutkintaan osalliset	**Esitutkintaan osalliset**
1 §	1 §
Viranomaiset esitutkinnassa	*Viranomaiset esitutkinnassa*
Esitutkinnan toimittaa poliisi.	Esitutkinnan toimittaa poliisi. *Suojelupoliisi ei ole kuitenkaan esitutkintaviranomainen.*
— — — — — — — — — — — — — —	— — — — — — — — — — — — — —
	———
	Tämä laki tulee voimaan päivänä kuuta 20 .
	———

LUONNOS

7.

Laki

pakkokeinolain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan pakkokeinolain (806/2011) 2 luvun 9 §:n 1 momentin 1 kohta, 10 luvun 3 §:n 1 momentti ja 6 §:n 1 momentti sekä 39 §:n 1 momentti seuraavasti:

Voimassa oleva laki

2 luku

Kiinniottaminen, pidättäminen ja vangitseminen

9 §

Pidättämiseen oikeutettu virkamies

Pidättämisestä päättää pidättämiseen oikeutettu virkamies. Pidättämiseen oikeutettuja virkamiehiä ovat:

1) poliisiylijohtaja, Poliisihallituksen poliisijohtaja, poliisiylitarkastaja ja poliisitarkastaja, poliisipäällikkö, apulaispoliisipäällikkö, keskusrikospoliisin päällikkö ja apulaispäällikkö, *suojelupoliisin päällikkö, esitutkintatehtäviin määrätty apulaispäällikkö, esitutkintatehtäviin määrätty osastopäällikkö, esitutkintatehtäviin määrätty ylitarkastaja ja tarkastaja,* rikosylitarkastaja, rikostarkastaja, rikosylikomisario, ylikomisario, rikoskomisario ja komisario;

2) Tullin rikostorjunnan päällikkö, Tullin rikostorjunnan toimintayksikön päällikkö sekä Tullin rikostorjunnan tulliylitarkastaja, jonka Tullin rikostorjunnan päällikkö on määrännyt tutkinnanjohtajaksi;

3) rajavartiolaitoksen päällikkö ja apulaispäällikkö, rajavartiolaitoksen esikunnan raja- ja meriosaston osastopäällikkö, rajavartiolaitoksen esikunnan oikeudellisen osaston osastopäällikkö, apulaisosastopäällikkö, rikostorjuntayksikön yksikönpäällikkö, rajavartioylitarkastaja, ylitarkastaja, rikosylitarkastaja ja rikostarkastaja, rajavartioston ja merivartioston komentaja ja apulaiskomentaja, rajavartioston ja merivartioston rajatoimiston ja meritoimiston päällikkö, Suomenlahden meri-

Ehdotus

2 luku

Kiinniottaminen, pidättäminen ja vangitseminen

9 §

Pidättämiseen oikeutettu virkamies

Pidättämisestä päättää pidättämiseen oikeutettu virkamies. Pidättämiseen oikeutettuja virkamiehiä ovat:

1) poliisiylijohtaja, Poliisihallituksen poliisijohtaja, poliisiylitarkastaja ja poliisitarkastaja, poliisipäällikkö, apulaispoliisipäällikkö, keskusrikospoliisin päällikkö ja apulaispäällikkö, rikosylitarkastaja, rikostarkastaja, rikosylikomisario, ylikomisario, rikoskomisario ja komisario;

2) Tullin rikostorjunnan päällikkö, Tullin rikostorjunnan toimintayksikön päällikkö sekä Tullin rikostorjunnan tulliylitarkastaja, jonka Tullin rikostorjunnan päällikkö on määrännyt tutkinnanjohtajaksi;

3) rajavartiolaitoksen päällikkö ja apulaispäällikkö, rajavartiolaitoksen esikunnan raja- ja meriosaston osastopäällikkö, rajavartiolaitoksen esikunnan oikeudellisen osaston osastopäällikkö, apulaisosastopäällikkö, rikostorjuntayksikön yksikönpäällikkö, rajavartioylitarkastaja, ylitarkastaja, rikosylitarkastaja ja rikostarkastaja, rajavartioston ja merivartioston komentaja ja apulaiskomentaja, rajavartioston ja merivartioston rajatoimiston ja meritoimiston päällikkö, Suomenlahden meri-

LUONNOS

Voimassa oleva laki

vartioston Helsingin rajatarkastusosaston päällikkö ja varapäällikkö sekä vähintään luutnantin arvoinen rajavartiomies, joka on saanut tutkinnanjohtajalle rajavartiolaitoksessa säädetyn koulutuksen ja jonka rajavartiolaitoksen tai sen hallintoyksikön päällikkö on määrännyt tutkinnanjohtajaksi;

4) syyttäjä.

Pidättämiseen oikeutetuista puolustusvoimien virkamiehistä säädetään laissa erikseen.

10 luku

Salaiset pakkokeinot

3 §

Telekuuntelu ja sen edellytykset

Telekuuntelulla tarkoitetaan viestintämarkkinalaissa 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 6 §:ssä tarkoitettujen tunnistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain rikoksesta epäillyltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin.

6 §

Televalvonta ja sen edellytykset

Televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty 3 §:ssä tarkoitettuun viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista taikka *tele*osoitteen tai *telepääte*laitteen käytön tilapäistä estämistä. *Tunnistamistiedolla* tarkoitetaan sähköisen viestinnän tietosuojalain 2 §:n 8 kohdassa tarkoitettua tilaajaan tai käyttäjään yhdistettävissä olevaa viestiä koskevaa

Ehdotus

vartioston Helsingin rajatarkastusosaston päällikkö ja varapäällikkö sekä vähintään luutnantin arvoinen rajavartiomies, joka on saanut tutkinnanjohtajalle rajavartiolaitoksessa säädetyn koulutuksen ja jonka rajavartiolaitoksen tai sen hallintoyksikön päällikkö on määrännyt tutkinnanjohtajaksi;

4) syyttäjä.

Pidättämiseen oikeutetuista puolustusvoimien virkamiehistä säädetään laissa erikseen.

10 luku

Salaiset pakkokeinot

3 §

Telekuuntelu ja sen edellytykset

Telekuuntelulla tarkoitetaan *sähköisen viestinnän palveluista annetun lain (917/2014) 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 *8* §:ssä tarkoitettujen tunnistamistietojen selvittämiseksi. Telekuuntelua saadaan kohdistaa vain rikoksesta epäillyltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin.

6 §

Televalvonta ja sen edellytykset

Televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty 3 §: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 *palveluista annetun lain 3 §:n 7 kohdassa tarkoitettuun* tilaajaan tai *mainitun pykälän 30 kohdassa tarkoitettuun*

Voimassa oleva laki

tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

— — — — — — — — — — — — — — —

39 §

Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, rikoksen selvittämiselle merkityksellisten tietojen vastaanottamista poliisin ja muun *esitutkinta*viranomaisen ulkopuoliselta henkilöltä *(tietolähde)*.

— — — — — — — — — — — — — — —

Ehdotus

käyttäjään yhdistettävissä olevaa viestiä koskevaa tietoa, jota viestintäverkoissa käsitellään viestien siirtämiseksi, jakelemiseksi tai tarjolla pitämiseksi.

— — — — — — — — — — — — — — —

39 §

Tietolähdetoiminta ja tietolähteen ohjatun käytön edellytykset

Tietolähdetoiminnalla tarkoitetaan muuta kuin satunnaista luottamuksellista, *1 luvun 1 §:ssä tarkoitettujen tehtävien hoitamiseksi* merkityksellisten tietojen vastaanottamista poliisin ja muun viranomaisen ulkopuoliselta henkilöltä (*tietolähde*).

— — — — — — — — — — — — — — —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

LUONNOS

8.

Laki

oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan oikeudenkäynnin julkisuudesta yleisissä tuomioistuimissa annetun lain (370/2007) 5 §:n 2 momentti, 12 §:n 2 momentin 3 kohta, 16 §:n 4 momentti,

sellaisina kuin ne ovat 5 §:n 2 momentti ja 16 §:n 4 momentti laissa 1159/2013 sekä 12 §:n 2 momentin 3 kohta laissa 633/2015 seuraavasti:

Voimassa oleva laki

5 §

Oikeudenkäyntiä koskevien perustietojen julkiseksi tulemisen ajankohta

— — — — — — — — — — — — — — —

Pakkokeinolain (806/2011) 10 luvussa *tai* poliisilain (872/2011) 5 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka tullilain (1466/1994) 20 f §:ssä tarkoitettua tullitoimenpidettä koskevassa asiassa, jossa tiedonhankintakeinon tai toimenpiteen kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, perustiedot tulevat julkisiksi vasta, kun tiedonhankintakeinon tai toimenpiteen käytöstä on viimeistään ilmoitettava rikoksesta epäillylle taikka tiedonhankintakeinon tai toimenpiteen kohteena olevalle. Jos hänelle ilmoitetaan tiedonhankintakeinon tai toimenpiteen käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, perustiedot tulevat julkisiksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Tuomioistuin voi päättää, että perustiedot tulevat julkisiksi aikaisemmin.

12 §

Asianosaisen oikeus tiedonsaantiin

— — — — — — — — — — — — — — —

Asianosaisella ei ole 1 momentissa tarkoi-

Ehdotus

5 §

Oikeudenkäyntiä koskevien perustietojen julkiseksi tulemisen ajankohta

— — — — — — — — — — — — — — —

Pakkokeinolain (806/2011) 10 luvussa, poliisilain (872/2011) 5 luvussa *tai rikostorjunnasta Tullissa annetun lain (623/2015) 3 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa (/) tai sotilastiedustelusta annetussa laissa (/) tarkoitettua tiedustelumenetelmää* koskevassa asiassa, jossa tiedonhankintakeinon tai *tiedustelumenetelmän* kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, perustiedot tulevat julkisiksi vasta, kun tiedonhankintakeinon tai *tiedustelumenetelmän* käytöstä on viimeistään ilmoitettava rikoksesta epäillylle taikka tiedonhankintakeinon tai *tiedustelumenetelmän* kohteena olevalle. Jos hänelle ilmoitetaan tiedonhankintakeinon tai *tiedustelumenetelmän* käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, perustiedot tulevat julkisiksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Tuomioistuin voi päättää, että perustiedot tulevat julkisiksi aikaisemmin.

12 §

Asianosaisen oikeus tiedonsaantiin

— — — — — — — — — — — — — — —

Asianosaisella ei ole 1 momentissa tarkoi-

LUONNOS

Voimassa oleva laki

tettua oikeutta:

1) viranomaisten toiminnan julkisuudesta annetun lain 11 §:n 2 momentin 7 tai 7 a kohdassa tarkoitettuihin tietoihin;

2) tuomioistuimessa laadittuihin oikeudenkäyntiasiakirjoihin ennen 8 §:ssä tarkoitettua ajankohtaa;

3) pakkokeinolain 10 luvussa, poliisilain 5 luvussa tai rikostorjunnasta Tullissa annetun lain *(623/2015)* 3 luvussa tarkoitettua salaista tiedonhankintakeinoa koskevassa asiassa, jossa tiedonhankintakeinon tai toimenpiteen kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla; eikä

4) oikeudenkäyntiasiakirjoihin siltä osin kuin niihin sisältyy tietoja tuomioistuimen neuvottelusta.

16 §

Pakkokeinoasioiden julkisuus

— — — — — — — — — — — — — — — — — — — —

Pakkokeinolain 10 luvussa tai poliisilain 5 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka tullilain 20 f §:ssä tarkoitettua tullitoimenpidettä koskeva asia, jossa tiedonhankintakeinon tai toimenpiteen kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, käsitellään ja ratkaisu siinä julistetaan yleisön läsnä olematta. Ratkaisun sisältävä ja muu oikeudenkäyntiasiakirja tulevat julkisiksi, kun tiedonhankintakeinon tai toimenpiteen käytöstä on viimeistään ilmoitettava rikoksesta epäillylle taikka tiedonhankintakeinon tai toimenpiteen kohteena olevalle. Jos hänelle ilmoitetaan tiedonhankintakeinon tai toimenpiteen käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, oikeudenkäyntiasiakirjat tulevat julkisiksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta. Tuomioistuin voi erityisestä syystä päättää, että oikeudenkäyntiasiakirja tulee julkiseksi aikaisemmin.

Ehdotus

tettua oikeutta:

1) viranomaisten toiminnan julkisuudesta annetun lain 11 §:n 2 momentin 7 tai 7 a kohdassa tarkoitettuihin tietoihin;

2) tuomioistuimessa laadittuihin oikeudenkäyntiasiakirjoihin ennen 8 §:ssä tarkoitettua ajankohtaa;

3) pakkokeinolain 10 luvussa, poliisilain 5 luvussa tai rikostorjunnasta Tullissa annetun lain 3 luvussa tarkoitettua salaista tiedonhankintakeinoa *taikka poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa tai sotilastiedustelusta annetussa laissa tarkoitettua tiedustelumenetelmää* koskevassa asiassa, jossa tiedonhankintakeinon tai t*iedustelumenetelmän* kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla; eikä

4) oikeudenkäyntiasiakirjoihin siltä osin kuin niihin sisältyy tietoja tuomioistuimen neuvottelusta.

16 §

Pakkokeinoasioiden julkisuus

— — — — — — — — — — — — — — — — — — — —

Pakkokeinolain 10 luvussa, poliisilain 5 luvussa *tai rikostorjunnasta Tullissa annetun lain 3 luvussa tarkoitettua salaista tiedonhankintakeinoa taikka poliisilain 5 a luvussa, tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa tai sotilastiedustelusta annetussa laissa tarkoitettua tiedustelumenetelmää koskeva asia, jossa tiedonhankintakeinon tai tiedustelumenetelmän* kohteena olevaa henkilöä ei vaatimusta käsiteltäessä tarvitse kuulla, käsitellään ja ratkaisu siinä julistetaan yleisön läsnä olematta. Ratkaisun sisältävä ja muu oikeudenkäyntiasiakirja tulevat julkisiksi, kun tiedonhankintakeinon tai *tiedustelumenetelmän* käytöstä on viimeistään ilmoitettava rikoksesta epäillylle taikka tiedonhankintakeinon tai *tiedustelumenetelmän* kohteena olevalle. Jos hänelle ilmoitetaan tiedonhankintakeinon tai *tiedustelumenetelmän* käytöstä myöhemmin hänen henkilöllisyytensä selvittyä, oikeudenkäyntiasiakirjat tulevat julkisiksi, kun tuomioistuimelle ilmoitetaan edellä tarkoitetusta ilmoituksesta.

LUONNOS

Voimassa oleva laki

Ehdotus

Tuomioistuin voi erityisestä syystä päättää, että oikeudenkäyntiasiakirja tulee julkiseksi aikaisemmin.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

LUONNOS