luonnos
7.4.2026

Hallituksen esitys eduskunnalle laiksi poliisilain 5 a luvun muuttamiseksi ja eräiksi muiksi laeiksi

ESITYKSEN PÄÄASIALLINEN SISÄLTÖ

Esityksessä ehdotetaan muutettavaksi poliisilakia, lakia tietoliikennetiedustelusta siviilitiedustelussa, rajavartiolakia, henkilötietojen käsittelystä rajavartiolaitoksessa annettua lakia ja rikoslakia. Lisäksi ehdotetaan muutettavaksi viranomaisten toiminnan julkisuudesta annettua lakia.

Esityksessä ehdotetaan säädettäväksi valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla voitaisiin hankkia tietoa kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta. Edelleen ehdotetaan säädettäväksi tietojärjestelmän käytön estämisestä tai sen toiminnan haittaamisesta. Tietoliikennetiedustelussa valtiolliseen toimijaan kohdistuvan tietoliikennetiedustelun määritelmää ja sen edellytyskynnystä ehdotetaan tarkistettavaksi.

Rajavartiolaitokselle ehdotetaan säädettäväksi toimivalta avustaa suojelupoliisia ja suorittaa tiettyjen tiedustelumenetelmien käyttöön liittyviä toimenpiteitä suojelupoliisin pyynnöstä.

Lisäksi esityksessä ehdotetaan tehtäväksi muutoksia käytännön siviilitiedustelutoiminnasta havaittujen tarkennustarpeiden johdosta sekä säädettäväksi yksinomaan tietoverkossa toteutettavasta peitetoiminnasta ja uudesta paikkatiedusteluun liittyvästä näytteenotosta.

Julkisuuslakia ehdotetaan muutettavaksi siten, että valtion turvallisuuden ylläpitämiseksi salassa pidettäväksi säädetyn tiedon salassapitoaika olisi 60 vuotta. Perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvien asiakirjojen osalta salassapitoaikaa pidennettäisiin 25 vuodesta 40 vuoteen.

Esityksellä toteutettaisiin pääministeri Petteri Orpon hallituksen hallitusohjelman jakson 10.1 kirjauksia tiedustelulainsäädännön kehittämisestä.

Ehdotetut lait on tarkoitettu tulemaan voimaan xx.xx.2026.

———————

SISÄLLYS

PERUSTELUT

1 Asian tausta ja valmistelu

1.1 Tausta

Siviilitiedustelulainsäädäntö tuli voimaan 1. kesäkuuta 2019. Sen antaminen mahdollistettiin säätämällä luottamuksellisen viestinnän suojaa koskeva perustuslain 10 §:n 4 momentti sekä laki tiedustelutoiminnan valvonnasta (121/2019). Siviilitiedustelutoimintaa koskevat keskeiset säännökset sisältyvät poliisilain (872/2011) 5 a lukuun ja tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin (582/2019). Siviilitiedustelulainsäädännön kokonaisuus on toiminut tarkoitetulla tavalla. Lainsäädännön myötä uhkiin liittyvän tilannekuvan voidaan katsoa parantuneen. Suojelupoliisin laajentuneiden toimivaltuuksien lisäksi niiden valvontaa on toteutettu tehokkaasti ja tuloksellisesti. Toiminnan käynnistyminen, teknologian ja globaalin toimintaympäristön muutos ovat kuitenkin tuoneet esiin muutostarpeita.

Eduskunta on hyväksynyt tiedustelulainsäädännöstä annetun valtioneuvoston selonteon (EK 70/2022 vp. – VNS 11/2021 vp.) johdosta hallintovaliokunnan mietinnön (HaVM 35/2022 vp.) mukaisen kannanoton. Kannanotossa eduskunta edellyttää, että hallitus muutoinkin tarkastelee tiedustelulainsäädännön toimivuutta, vaikutuksia ja mahdollisia muutostarpeita, huolehtii lainsäädännön ajantasaisuudesta muuttuvassa toimintaympäristössä sekä varmistaa tiedustelutoiminnan ja sen valvonnan riittävät resurssit.

Lisäksi lainsäädännön muutostarpeita on tunnistettu myös eduskunnalle toimitetussa selvityksessä siviilitiedustelulainsäädännön toimivuudesta.

Pääministeri Petteri Orpon hallituksen hallitusohjelmassa (jakso 10.1 Kansallista turvallisuutta ja yhteiskunnan kriisinkestävyyttä vahvistetaan) on useita tiedustelulainsäädännön kehittämistä koskevia kirjauksia. Tiedustelulainsäädäntö on osa maanpuolustusta ja kansallisen turvallisuuden suojaamista.

Hallitusohjelman mukaan hallitus kehittää tiedustelulainsäädäntöä viranomaisten toimintakyvyn turvaamiseksi tiedustelutoiminnasta saatujen kokemusten, teknologisen kehityksen ja Suomen Nato-jäsenyyden johdosta. Tiedustelulainsäädäntöä tarkistetaan tiedustelutoimivaltuuksien sekä tiedonsaanti- ja luovutusoikeuksien osalta vastaamaan muuttuneen turvallisuus- ja kybertoimintaympäristön vaatimuksia.

Hallitus varmistaa, että tiedustelutoimivaltuudet vastaavat teknologiseen kehitykseen. Mahdollistetaan muun muassa tiedustelu laite- ja järjestelmäketjuihin ja viestin sisältöön kohdistuvien hakuehtojen käyttö tiedustelutoiminnassa. Lisäksi hallitusohjelman mukaan arvioidaan tiedustelutoimivaltuuksien laajentaminen vakituiseen asumiseen käytettävään tilaan.

Hallitusohjelman mukaan arvioidaan viranomaisten avustamisvelvollisuuden laajentaminen Suomessa sijaitseville palveluntarjoajille, kuten konesaliyrityksille. Selvitetään mahdollisuus säätää toimivaltuus käsitellä ja hyödyntää avoimista lähteistä saatavia suuria tietovarantoja.

Hallitusohjelman mukaan hallituskauden aikana säädetään toimivaltuus vaikuttaa ulkomailla olevaan laitteeseen tai ohjelmistoon, jota käytetään Suomen kansallista turvallisuutta vaarantavaan kybervakoiluun tai -vaikuttamiseen.

Lisäksi hallitusohjelman mukaan säädetään Rajavartiolaitokselle oikeus käyttää suorituskykyä tiedusteluviranomaisen tukemiseen ja oikeus tietojen luovuttamiseen tiedusteluviranomaiselle.

Sisäministeriön ja puolustusministeriön yhteinen selvityshanke viranomaisten toimintaedellytysten arvioimiseksi kansallisen kyberturvallisuuden varmistamisessa, kyberrikollisuuden torjunnassa, kyberpuolustuksessa sekä nopeasti kehittyvissä yhteiskunnan kyberturvallisuutta uhkaavissa tilanteissa antoi raporttinsa ”Selvitys viranomaisten toimintaedellytyksistä kyberturvallisuudessa” 11.4.2023 (VN julkaisu 2023:31). Hankkeessa tunnistettiin useita kehittämistarpeita, joilla kyetään paremmin suojaamaan kansallista turvallisuutta. Muun muassa tiedusteluviranomaisten toimintaedellytyksiä kybertoimintaympäristössä tulisi kehittää luomalla edellytykset tiedustelumenetelmien kohdistamiseksi yksittäisten laitteiden sijasta virtuaalisten järjestelmien muodostamiin kokonaisuuksiin sekä kehittämillä tietoliikennetiedustelun teknisten tietojen käsittelyä.

1.2 Valmistelu

Sisäministeriö asetti 21.12.2023 ajalle 21.12.2023 – 31.7.2026 hankkeen VN/31244/2023, jonka tehtävänä on toteuttaa hallitusohjelman kirjaukset hanketta koskevin osin. Hankkeessa arvioidaan siviilitiedustelua koskevan poliisilain 5 a luvun ja tietoliikennetiedustelusta siviilitiedustelussa annetun lain säännösten muutostarpeet sekä henkilötietojen käsittelystä poliisitoimessa annetun lain (616/2019, poliisin henkilötietolaki) 7 luvun, joka koskee suojelupoliisin henkilötietojen käsittelyä, säännösten muutostarpeet suhteessa voimassa olevaan lainsäädäntöön ja nykyisen toimintaympäristön vaatimuksiin ja valmistellaan arvion pohjalta ehdotukset lainsäädäntömuutoksiksi. Hanke toteutetaan vaiheittain. Hanketta varten asetettiin työryhmä, johon kuuluivat sisäministeriön, puolustusministeriön, liikenne- ja viestintäministeriön sekä suojelupoliisin ja pääesikunnan edustajat. Työryhmän pysyvänä asiantuntijana oli edustaja tiedusteluvalvontavaltuutetun toiminnosta.

Hankkeen ensimmäisessä vaiheessa arvioitiin poliisilain 5 a luvun 44 §:n eli niin sanotun palomuurisääntelyn ja kansainvälisessä yhteistyössä henkilötietojen luovuttamista koskevan poliisin henkilötietolain 7 luvun 51 §:n sääntelyn sekä poliisilain 5 a luvun 57 §:n suojelupoliisin kansainvälistä yhteistyötä koskevan sääntelyn tarkistaminen (tiedonluovutus Natolle). Hankkeessa valmisteltiin ehdotukset tarvittaviksi lainsäädäntömuutoksiksi hallituksen esitykseksi HE 29/2025 vp. Eduskunta antoi vastauksen hallituksen esitykseen EV 2/2026 vp ja lait vahvistettiin 13.3.2026. Lait tulivat voimaan 20.3.2026.

Hankkeen toisessa vaiheessa arvioitiin ja tässä hallituksen esityksessä käsitellään muutostarpeita, jotka liittyvät tiedustelulainsäädännön toimivuuteen, ajantasaisuuteen ja teknologisiin vaatimuksiin. Lisäksi esitetään Rajavartiolaitokselle oikeutta käyttää suorituskykyään tiedusteluviranomaisen tukemiseen ja oikeus tietojen luovuttamiseen tiedusteluviranomaiselle. Hanke on toteutettu rinnakkain sotilastiedustelulain vastaavia muutoksia käsittelevän puolustusministeriön hankkeen VN/10644/2024 kanssa.

Ulkoministeriö on valmistellut julkisuuslain 31 §:ään julkisuuslain 24 §:n 1 momentin 1 ja 2 kohtiin liittyvät salassapitoajan pidentämistä koskevat muutokset. Sisäministeriö on valmistellut julkisuuslain 31 §:ään julkisuuslain 24 §:n 1 momentin 9 ja 10 kohtiin liittyen salassapitoajan pidentämistä koskevat muutokset.

Hallituksen esityksen luonnoksesta järjestettiin lausuntokierros XXxx. Lausuntokierros toteutettiin Lausuntopalvelu.fi -palvelun kautta. Hallituksen esitysluonnokseen annetut lausunnot ovat julkisesti saatavilla lausuntopalvelussa osoitteessa XX. Lisäksi luonnosta koskevat lausunnot ja muut hankkeen valmisteluasiakirjat ovat saatavilla valtioneuvoston verkkosivustolta tunnuksella SM040:00/2024.

2 Nykytila ja sen arviointi

Siviilitiedustelulainsäädännöllä parannettiin suomalaisen yhteiskunnan mahdollisuuksia suojautua kansalliseen turvallisuuteen kohdistuvilta vakavilta uhilta. Lainsäädännöllä parannettiin Suomen mahdollisuuksia suojautua esimerkiksi terrorismilta, vieraiden valtioiden Suomeen kohdistamalta vakoilulta tai elintärkeän infrastruktuurin lamauttamiselta. Uusien toimivaltuuksien avulla on ollut mahdollista tuottaa välttämätöntä tietoa kansallista turvallisuutta vakavasti uhkaavasta toiminnasta ylimmän valtiojohdon päätöksenteon tueksi sekä kansallisen turvallisuuden suojaamiseksi.

Siviilitiedusteluun liittyvät toimivaltuudet ovat olleet käytössä nyt kuusi vuotta. Tänä aikana ja käytännön soveltamisen kautta on tehty havaintoja lain uudistamisen tarpeista. Uudistamista puoltavat myös vaikeutunut turvallisuustilanne ja tekninen kehitys, joka jatkuvasti haastaa viranomaisten kyvykkyyttä vastata uhkiin.

2.1 Turvallisuusympäristön muutos

2.1.1 Selonteot

Suomen turvallisuusympäristön muutosta on kuvattu kattavasti keväällä 2022 julkaistussa valtioneuvoston ajankohtaisselonteossa turvallisuusympäristön muutoksesta[1] ja vuoden 2024 puolustusselonteossa[2]. Selontekojen mukaan Suomen ja Euroopan turvallisuus- ja toimintaympäristössä on tapahtunut perustavanlaatuinen ja pitkäkestoinen muutos Venäjän Ukrainaa vastaan käynnistämän hyökkäyssodan myötä. Yhteiskunnan kriisinsietokyvyn, kansallisen puolustuskyvyn ja sisäisen turvallisuuden ylläpitämisen merkitys Suomen turvallisuudelle korostuu.

Venäjän hyökkäyssodalla Ukrainaan on perustavanlaatuisia ja pitkäkestoisia vaikutuksia turvallisuusympäristöön Euroopassa ja Suomen lähialueilla. Venäjä on osoittanut, ettei se kunnioita toisten valtioiden suvereniteettia ja alueellista koskemattomuutta ja on toimillaan loukannut YK:n peruskirjaa sekä rikkonut eurooppalaista sopimuspohjaista turvallisuusjärjestystä.

Valtioneuvoston ajankohtaisselonteon (2022) mukaan Venäjän vaatimukset ja sotilaalliset toimet Euroopan turvallisuusarkkitehtuurin muuttamiseksi vaikuttivat myös Suomen ulko-, turvallisuus- ja puolustuspoliittiseen liikkumatilaan. Suomi haki puolustusliitto Naton jäsenyyttä 17.5.2022. Suomesta tuli Naton jäsen 4.4.2023. Edelleen selonteossa todetaan, että ”mikäli Suomi hakisi Naton jäsenyyttä, tulisi varautua laaja-alaiseen ja vaikeasti ennakoitavaan vaikuttamiseen ja riskeihin, kuten esimerkiksi jännitteiden kasvuun Suomen ja Venäjän välisellä rajalla. Suomi vahvistaa varautumistaan laaja-alaisten hybridivaikuttamisen keinojen kohteeksi joutumiseen sekä vaikuttamisen estämiseen ja siihen vastaamiseen.”

Valtioneuvoston sisäisen turvallisuuden selonteon (2025) mukaan Suomen ulkoinen turvallisuusympäristö on muuttunut perustavanlaatuisesti ja pitkäkestoisesti. Venäjän hyökkäyssota Ukrainaan ja maailman geopoliittinen murrosvaihe heijastuvat voimakkaasti myös Suomen sisäiseen turvallisuuteen ja heikentävät sen ennustettavuutta. Suomen Nato-jäsenyys lisää

[1] Ajankohtaisselonteko turvallisuusympäristön muutoksesta. Valtioneuvoston julkaisuja 2022:18. http://urn.fi/URN:ISBN:978-952-383-772-0

[2] Valtioneuvoston puolustusselonteko. Puolustusministeriön julkaisuja 2024:5. http://urn.fi/URN:ISBN:978-951-663-423-7

Suomen ulkoista turvallisuutta. Geopoliittisesti jännittyneessä tilanteessa jäsenyys myös lisää Suomeen kohdistuvaa vihamielistä toimintaa.

Venäjän hyökkäyksellä Ukrainaan on ollut laajamittaisia kielteisiä vaikutuksia globaalisti ja erityisesti Euroopan turvallisuuteen. Suomi on vastannut Venäjän hyökkäyssotaan osana Euroopan unionia. Venäjä on nostanut Ukrainan lisäksi viholliseksen kollektiivisesti ne länsimaat, jotka ovat mukana asetetuissa vastatoimissa. Vallitsevissa oloissa Suomen kriittiseen infrastruktuuriin kohdistuva tiedustelun ja vaikuttamisen uhka on kohonnut sekä fyysisessä että kyberympäristössä Venäjän Ukrainassa aloittaman hyökkäyssodan sekä Suomen Nato-jäsenyyden myötä. Kiinteistöjen merkitys kansalliselle turvallisuudelle vaihtelee merkittävästi kiinteistön käyttötarkoituksen, sijainnin, kiinteistöllä sijaitsevien rakennusten ja rakennelmien sekä kiinteistöllä tai niiden lähistöllä mahdollisesti sijaitsevan kriittisen infrastruktuurin ja strategisten kohteiden perusteella.

Turvallisuustilanne Euroopassa ja Suomen lähialueilla on epävakaa ja turvallisuusympäristön muutos heijastuu myös Suomen rajaturvallisuustilanteeseen, mikä on näkynyt esimerkiksi maahantulon välineellistämisenä Venäjän toimesta. Tämä on ollut yksi keinoista pyrkiä vaikuttamaan Suomen kansalliseen turvallisuuteen ja yleiseen järjestykseen. Suomen on varauduttava siihen, että painostaminen jatkuu pitkäaikaisesti, ja että se saa aiempaa laajempia ja vakavampia muotoja. Kansallisen turvallisuuden uhkiin tulee varautua riittävästi niitä ennalta ehkäisten.

Venäjä käyttää erilaisia vaikuttamisen keinoja kuten hybridivaikuttaminen edistääkseen strategisia tavoitteitaan. Tavoitteena on muun muassa vaikuttaa kohdemaan yhtenäisyyteen, päätöksentekoon ja kansalaismielipiteeseen sekä lisätä vastakkainasettelua, luoda pelkoa ja hämärtää tilannekuvaa. Poliittisten tavoitteidensa tukemiseksi Venäjä jatkaa aktiivista tiedustelu- ja vaikuttamistoimintaa perinteisen tiedonhankinnan ja agenttitoiminnan ohella myös tietoverkoissa. Venäjä hyödyntää toiminnassaan valtiollisten viranomaisten lisäksi yhtä lailla yrityksiä ja koulutus- ja tutkimuslaitoksia kuin rikollisryhmittymiä ja aktivisteja.

Mahdollisuudet hyödyntää kybertoimintaympäristöä vihamielisissä tarkoituksissa lisääntyvät, kun infrastruktuuri ja teknologia kehittyvät ja käyttäjämäärät kasvavat. Vihamieliset toimijat kohdistavat jatkuvasti länsimaihin tietoverkkotiedustelua, kybervakoilua ja kybervaikuttamista ja pyrkivät vaikuttamaan fyysisesti niiden kriittiseen infrastruktuuriin. Valtiollisten toimijoiden lisäksi vihamielisestä toiminnasta vastaavat entistä enemmän myös valtiollisesti ohjatut ei-valtiolliset toimijat.

Siviilitiedustelun toimivaltuudet sekä tiedustelukykyjen kehittäminen ovat edelleen parantaneet kykyä muodostaa tilannekuvaa. Suojelupoliisi on osallistunut Naton siviilitiedustelukomitean toimintaan. Suomen Nato-jäsenyys liitti Suomen sotilas- ja siviilitiedustelun osaksi liittokunnan tiedusteluyhteisöä. Suojelupoliisin ja sotilastiedustelun tiivis yhteistyö on vankka perusta suomalaiselle tiedustelulle kaikissa yhteyksissä.

Suomi huolehtii kansallisen tiedustelun kehittämisestä vastaamaan lisääntyneisiin vaatimuksiin ja turvallisuusympäristön muutoksiin. Suomella on valmius tunnistaa, ennaltaehkäistä ja torjua vakoilua, hybridivaikuttamista ja terrorismia

2.1.2 Tiedusteluviranomaisten katsaukset

Suojelupoliisin vuoden 2025 kansallisen turvallisuuden katsauksessa[3] on kuvattu toimintaympäristön muutosta tiedustelun osalta. Katsauksen mukaan Venäjä ja Kiina muodostavat merkittävimmän tiedustelullisen uhkan Suomelle. Venäjä on Suomelle keskeisin tiedustelun ja vaikuttamisen uhka lyhyellä ja pitkällä aikavälillä. Venäjä yrittää hankkia Suomesta tietoa niin henkilö- kuin kybertiedustelun keinoin. Vaikuttaminen on aina kuulunut Venäjän tiedustelu- ja turvallisuuspalveluiden toimintaan, mutta sen kohteet ja aktiivisuus ovat vaihdelleet maailmanpoliittisen tilanteen mukaan. Natoon kuuluvat Venäjän rajanaapurit ovat sen tiedustelun erityisen mielenkiinnon kohteena. Venäjän ja länsimaiden välien viilennyttyä Venäjän vaikuttaminen on muuttunut astetta vakavampaan suuntaan, josta esimerkkinä voidaan pitää Venäjän sabotaasitoimintaa Euroopassa.

Kansallisen turvallisuuden katsauksen mukaan Venäjän tiedustelupalveluiden Suomeen kohdistama toiminta kyberympäristössä on ollut jo vuosien ajan erittäin aktiivista, mutta se on lisääntynyt ja tarkentunut viime aikoina entisestään. Vaikka Venäjän henkilötiedustelu on vaikeutunut, henkilötiedustelun uhka ei kuitenkaan ole pitkällä aikavälillä vähentynyt, sillä Venäjän tiedontarpeet eivät ole kadonneet minnekään. Sekä tiedustelun että laaja-alaisen vaikuttamisen tilannekuvassa entistä suurempaan rooliin ovat nousseet eri valtioiden käyttämät sijaistoimijat. Valtiollinen toimija pyrkii häivyttämään jälkensä välikäsien kautta, oli kyse sitten Venäjän, Kiinan tai Iranin toiminnasta. Sijaistoimijoiden avulla itsevaltaisten maiden voimaviranomaiset haluavat hämärtää todellisuutta, helpottaa tekojen kiistettävyyttä ja luoda uudenlaista epävarmuutta. Rekrytointi voidaan hoitaa sosiaalisessa mediassa ja maksu kryptovaluutoilla. Tehtävän suorittaja ei aina välttämättä itsekään tiedä, kenen lukuun toimii.

Venäjän turvallisuus- ja tiedustelupalveluilla on perinteisesti ollut pysyvää läsnäoloa niin Suomessa kuin muissa maissa. Tiedustelupalvelujen edustajat ovat toimineet pääosin diplomaattisen peitteen suojassa, mutta Venäjä pyrkii aikaisempaa enemmän hyödyntämään välikäsiä sekä muita peitteitä kuin diplomaattipeitettä.

Venäjän tiedustelun läsnäolo Suomessa ja muualla Euroopassa on kuitenkin merkittävästi vähentynyt hyökkäyssodan vastineena toteutettujen diplomaattipeitteellä toimineiden tiedusteluupseerien karkotusten myötä. Tilanteeseen vaikuttavat myös matkustukseen kohdistuvat rajoitukset ja se, että yhä harvempi Suomessa haluaa sodan vuoksi olla tekemisissä venäläisten toimijoiden kanssa.

Venäjän henkilötiedustelun uhka ei kuitenkaan ole pitkällä aikavälillä vähentynyt.

Muuttunut toimintaympäristö on ajanut myös Venäjän tiedustelu- ja turvallisuuspalvelut muuttamaan toimintaansa. Venäjä pyrkii aikaisempaa enemmän hyödyntämään välikäsiä sekä muita peitteitä kuin diplomaattipeitettä. Ne eivät tule korvaamaan laajamittaisesti tai nopeasti diplomaattipeitteen hyödyllisyyttä. Venäjä yrittää myös edelleen sijoittaa tiedustelu-upseereitaan diplomaatin tehtäviin.

Venäjän tiedustelutoimijat joutuvat enenevässä määrin toimimaan Venäjältä käsin. Tiedustelua voi kohdistua Venäjällä oleviin tai matkustaviin, Suomessa asuviin henkilöihin. Myös epäasiallisten keinojen käyttö on mahdollista Venäjällä.

[3] Kansallisen turvallisuuden katsaus 2025. Supo. https://supo.fi/esitteet

Suojelupolisiin vuoden 2026 kansallisen turvallisuuden katsauksessa [4] on kuvattu globaalia turvallisuusympäristöä ja Suomea. Suomen turvallisuustilanne voi heiketä entisestään.

Ukrainan sodan taukoaminen tai päättyminen ei muuta Venäjän pitkäaikaisia suurvaltatavoitteita. Jännitteet Itämerellä ovat koholla ja Itämeri on Venäjälle elintärkeä ja sen talouden perusta. Kiina pyrkii omalta osaltaan globaaliin johtoasemaan ja muokkaamaan maailmanjärjestystä. Lähi-idän epävakaus vaikuttaa kansainväliseen politiikkaan ja talouteen. Valtiot kilpailevat resursseista talouden merkityksen kasvaessa kansalliselle turvallisuudelle ja resurssikilpailun kohdistuessa kriittisiin mineraaleihin. Venäjän ja Kiinan tiedustelu ja vaikuttaminen Suomea vastaan jatkuvat aktiivisina.

Venäjä muodostaa keskeisimmän tiedustelu-uhan Suomea vastaan. Venäjän tiedustelun toimintamallit monipuolistuvat, vaikka kaikki epäilyttävä ei ole Venäjän vaikuttamista. Kiinan tiedustelu hyödyntää eri toimintatapoja joustavasti luodessaan kontakteja kohteisiin. Kiinan kyberoperaatiot ovat maailmanlaajuisia ja kohdistuvat myös Suomeen. Kyberoperaatiot ovat keskittyneet yhä enemmän länsimaiseen kriittiseen infrastruktuuriin.

Vieraiden valtiollisten toimijoiden toimesta on viime vuosina myös suomalaisiin startup-yrityksiin on kohdistunut onnistuneita kybervakoiluoperaatioita.

Sotilastiedustelun julkisessa katsauksessa[5] vuodelta 2025 todetaan, että Suomen Nato-jäsenyys, tiivistynyt kansainvälinen puolustusyhteistyö sekä Euroopan turvallisuusympäristön muutos ovat lisänneet Venäjän tietotarpeita Suomesta. Tiedustelupalveluiden mielenkiinnon kohteita ovat etenkin Suomen Nato-politiikan toimeenpano, puolustusyhteistyön kehittyminen, kansainvälisten joukkojen toiminta Suomessa sekä Naton esikuntien ja joukkorakenteiden kehittäminen. Lisäksi Ukrainan sodan aikana on korostunut tarve hankkia tietoa puolustusvälineteollisuuden tuotantokapasiteetista ja Puolustusvoimien materiaalisen suorituskyvyn kehittymisestä. Puolustusjärjestelmään kohdistuva tiedustelun uhka kohdistuu ensisijaisesti Puolustusvoimien suorituskykyihin ja käyttöperiaatteisiin sekä valmiuteen.

Suomen lähialueilla Venäjälle keskeisiä asioita ovat Kuolan niemimaalle sijoitetut strategiset suorituskyvyt, rajoittamaton pääsy Atlantille pohjoisten merireittien kautta sekä arktinen alue. Se pyrkii myös rajoittamaan Naton toimintaa Itämeren alueella ja heikentämään Suomen ja Ruotsin integroitumista Natoon sekä vaikuttamaan maiden Nato-jäsenyyksien sisältöön.

Venäjä on aloittanut sotilaspiirejä koskevan asevoimareformin. Suomen suunnalla toimivaa Leningradin sotilaspiiriä vahvennetaan suunnitelmien mukaan merkittävästi tulevaisuudessa. Kun edellä kerrotut muutokset saadaan päätökseen, ne kasvattavat Suomen lähialueella olevien joukkojen vahvuutta todennäköisesti noin 30 000:sta noin 80 000 sotilaaseen. On kuitenkin todennäköistä, että niin kauan kuin Ukrainan sota jatkuu nykyisenkaltaisena kulutussotana, Suomen lähialueella oleva sotilaallinen voima ei kasva merkittävästi. Ukrainan sodan päättymisen jälkeen Venäjä kuitenkin todennäköisesti priorisoi luoteista suuntaansa ja pyrkii nopeuttamaan uudistusten toimeenpanoa.

Venäjä pyrkii vaikuttamaan Suomen turvallisuuspoliittisiin ratkaisuihin ja antaa ymmärtää, että Naton infrastruktuurin sijoittaminen Suomeen johtaisi jännitteiden lisääntymiseen. Venäjä

---

[4] Kansallisen turvallisuuden katsaus 2026. Supo. https://supo.fi/katsaus

[5] Sotilastiedustelun julkinen katsaus 2025. Pääesikunta. https://puolustusvoimat.fi/documents/1948673/2014902/PV_sotilastiedustelu_raportti_2025_web.pdf/4de8d666-6bff-642d-2d07-df71154b33bd?t=1737029070219

todennäköisesti lisää kaikkien laaja-alaisen vaikuttamisen keinojen käyttöä pyrkiessään aiheuttamaan hajaannusta Naton ja Euroopan unionin sisällä. Näihin keinoihin lukeutuvat kyber- ja informaatiovaikuttaminen, energiapolitiikka, vaikuttaminen energia- ja muuhun kriittiseen infrastruktuuriin, siirtolaisten ohjailu ja erilaiset tiedusteluoperaatiot.

Sotilastiedustelun julkisessa katsauksessa vuodelta 2026 todetaan, että Venäjä kohdistaa laaja-alaista vaikuttamista länsimaita kohtaan. Venäjän ja Suomen raja-alueella on välineellistetyn maahanmuuton uhka. Suomeen kohdistuviin tiedustelu-, vakoilu- ja tuhotöiden uhkiin vaikuttavat Euroopan kiristyneen turvallisuustilanteen lisäksi etenkin Suomen Ukrainaan antama tuki sekä lännen Venäjään kohdistamat pakotteet ja vientirajoitukset. Digitalisoitunut ympäristö tekee tapahtumat, kriisit ja konfliktit aiempaa läpinäkyvämmiksi.

2.1.3 Valtioneuvoston selonteko tiedustelulainsäädännöstä

Valtioneuvosto on antanut selonteon tiedustelulainsäädännöstä[6] vuonna 2021. Sen mukaan tiedustelulainsäädäntö on osa yhteensovitettua kansallisen turvallisuuden suojaamisen ja maanpuolustuksen tavoitteiden toteuttamista, ja se on ollut voimassa lyhyen aikaa.

Tiedustelutoimivaltuuksien käyttöä määrittävät tiedustelun tarkoitus ja kohde, yleiset ja erityiset edellytykset sekä toimintaa koskevat yleiset periaatteet.

Tiedustelua koskevan lainsäädännön keskeisin tavoite, kansallisen turvallisuuden parantaminen, on toteutunut, ja tiedonhankinta kansalliseen turvallisuuteen ja maanpuolustukseen kohdistuvista uhkista on uusien tiedustelutoimivaltuuksien myötä tehostunut. Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteinen kokous on tärkeä toimija ulko- ja turvallisuuspoliittisesti merkittävien kehityslinjojen huomioon ottamisessa tiedustelussa ja tiedustelun toteutumisen seurannassa. Suomen turvallisuusympäristö on tiedustelulainsäädännön hyväksymisen jälkeen ollut jatkuvassa muutoksessa. Muutokset muodostavat yhteiskunnalle, sen toiminnoille ja jäsenille uusia uhkia ja uhkien yhdistelmiä. Siten lainsäädännön arviointi on jatkuva, käynnissä oleva prosessi tiedustelulainsäädännön soveltamisesta saatujen kokemusten tullessa jatkuvasti laajemmiksi. Uusiin ja monesta suunnasta ilmeneviin uhkiin varaudutaan jatkossakin ajantasaisen lainsäädännön keinoin perustuslaista johtuvat edellytykset ja reunaehdot huomioon ottaen.

Selonteossa todetaan, että tietoliikennetiedustelu täydentää menetelmänä muiden tiedustelumenetelmien käyttöä. Kokonaisuutena tietoliikennetiedustelun voidaan katsoa sisältävän teknisten tietojen käsittelyn sekä valtiollisen ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvan tiedustelun. Tietoliikennetiedustelua koskeva sääntely kattaa nimenomaiset säännökset siitä, että se ei ole yleistä ja kohdentamatonta tietoliikenteen seurantaa. Tietoliikennetiedustelua ei saa kohdistaa viestiin, jonka lähettäjä ja vastaanottaja ovat Suomessa, jolloin tietoliikennetiedustelua suoritettaessa toisen osapuolen on oltava Suomen ulkopuolella.

Selonteossa todetaan myös, että sotilastiedustelusta annetun lain 66 §:ssä säädetään tietoliikenteen tiedonhankinnan teknisten tietojen käsittelystä, mikä edeltää varsinaista tietoliikennetiedustelua. Säännöksessä teknisten tietojen keräämisen hetkellisyyttä ei ole tarkemmin

[6] Valtioneuvoston selonteko tiedustelulainsäädännöstä. Valtioneuvoston julkaisuja 2021:94. http://urn.fi/URN:ISBN:978-952-383-500-9

määritelty, ja määrittelyä linjataan tuomioistuimessa. Hankittavien tietojen ja toiminnan luonne huomioon ottaen hetkellisyys on osoittautunut ongelmalliseksi.

Lisäksi teknisten tietojen keräämiseksi tarvittava lupa voi olla voimassa lyhyemmän aikaa kuin varsinainen tietoliikennetiedustelu, mikä johtaa lupahakemuksen uusimiseen. Luvan voimassaoloaika tulisi yhteensovittaa varsinaisen tietoliikennetiedustelun kuuden kuukauden lupa-aikaan. Tällä hetkellä teknisten tietojen käsittelyllä saatuja tietoja voidaan käyttää vain tietoliikennetiedustelun kannalta merkityksellisen viestintäverkon osan löytämiseen.

Teknisten tietojen käsittelyssä on tunnistettu kuitenkin saatavan tietoja, joita voitaisiin käyttää myös varsinaisessa tietoliikennetiedustelussa hakuehtoina sekä käytettävien hakuehtojen tarkentamisessa ja kehittämisessä.

Teknisten tietojen käyttö hakuehtoina rajaisi entisestään saatavaa tietoa, kohdistuisi tarkemmin kohteeseen ja tehostaisi toimintaa. Tämä vähentäisi tarpeetonta puuttumista yksilön oikeuksiin.

Lainsäädännön mukaisten toimivaltuuksien kehittämisessä on otettava huomioon uusien teknologioiden kehittyminen, jotka usein turvaavat entistä paremmin yksityisyyden suojaa, mutta toisaalta mahdollistavat myös laittoman toiminnan tai kansallista turvallisuutta vaarantavan toiminnan salaamisen.

2.1.4 Viestintäverkko, tietoliikenne ja tietoliikenteen tiedustelu

Viestintäverkon fyysinen rakenne

Digitalisoituneessa maailmassa ja yhteiskunnassa yhteiskunnan ja ihmisten toiminta ovat vahvasti riippuvaisia tietoliikennejärjestelmästä. Tietoliikennejärjestelmä koostuu lukuisista tietoliikenteen välittämiseen tarvittavista laitteista sekä välittämiseen tarvittavista suuremmista ja pienemmistä tietoliikennekaapeleista ja johdoista. Suurimmat kaapelit, kuten merikaapelit, koostuvat valokuitupareista (yksi kuitu vie ja toinen tuo), kun taas pienemmät johdot voivat olla kuparikaapeleita. Tavanomainen merikaapeli sisältää 48 kuituparia.

Valokuidussa liikkuva tieto on muunnettu valoksi, kun taas kuparijohdoissa tieto liikkuu sähkönä. Valokuidun tietoliikenteen tiedon siirron tehokkuus perustuu siihen, että valokuidussa tietoa siirretään laserilla ja yhdessä valokuidussa voidaan siirtää tietoa kymmenillä eri aallonpituuksilla, jotka näkyvät kuidussa eri värisinä valoina, multipleksaustekniikan (Dense Wavelenght Division Multiplexing Access, DWMA) avulla. Yksittäisen aallonpituuden tiedonsiirtokapasiteetti on vuonna 2025 Suomessa yleensä noin 100–400 Gbps. Näin ollen yksittäinen valokuitupari voi teoriassa kuljettaa tietoa kymmeniä terabittejä sekunnissa. Valokuiduissakin valo heikkenee, joten noin 80–100 kilometrin välein kuitupari on liitettävä kuitureitin varrella laitteistolle, joka vahvistaa signaalia.

Optisen siirtojärjestelmän päässä olevalla vastaanottimella aallonpituudet muunnetaan asiakassignaaleiksi, jotka ohjataan kytkimille tai reitittimille. Kytkimillä ja reitittimillä tietoliikenteen bittivirta käsitellään digitaalisella tasolla ja ohjataan seuraaville laitteille reititysohjeistuksen (reititysprotokollan) mukaisesti. Asiakassignaalin siirto optiselta lähettimeltä tai vastaanottimelta kytkimelle tai reitittimelle voi tapahtua joko valokuitua tai kuparikaapelia pitkin.

Tietoliikenne

Jotta tietokone tai muu päätelaite toimisi halutulla tavalla ja laitteet toimisivat niille annettujen komentojen mukaisesti, edellyttää se ihmiselle visuaalisesti tulkittavissa olevan tiedon

muuntamista binäärikoodiksi. Binääriluvut 1 ja 0 edustavat ”päällä” ja ”pois päältä” vaihtoehtoja. Binäärijärjestelmä on yksinkertaisin tapa käsitellä tietoa elektronisilla laitteilla. Tämä yksinkertaisuus tekee binäärijärjestelmästä luotettavan ja tehokkaan tavan toteuttaa digitaalista logiikkaa ja laskentaa.

Vastaavasti tietoliikenteessä on kyse ykkösistä ja nollista, ja tietoliikenne on käytännössä peräkkäisiä numeroita 1 ja 0. Numero 1 tai 0 muodostaa yhden bitin, ja kahdeksan bittiä muodostaa yhden tavun. Yksi tavu edustaa erilaisia arvoja tai merkkejä, kuten kirjainta, numeroa tai erikoismerkkiä.

Jotta tietoliikennejärjestelmässä olevat laitteet ja niissä käytettävät ohjelmat voisivat kommunikoida ja toimia yhdessä, vaatii tämä erilaisia teknisiä säännöstöjä ja standardeja, eli protokollia. Esimerkiksi tietoliikenneprotokollat (kuten web-sivustojen käyttämät HTTPS ja internetissä yleisesti käytettä TCP/IP) määrittävät, miten tietoa siirretään verkkojen välillä, kun taas salasanojen ja tietoturvan protokollat (kuten SSL/TLS) varmistavat, että tieto kulkee turvallisesti.

Tarkempana esimerkkinä voidaan tarkastella laajasti käytettyä IP-protokollaa (Internet Protocol). Se on tietoliikenneprotokolla, joka toimii internetin ja muiden tietoverkkojen perustana. IP-protokollan tarkoituksena on mahdollistaa tietojen siirto laitteiden välillä verkossa, riippumatta niiden fyysisestä sijainnista. IP-protokollan keskeisiä omaisuuksia ovat:

- IP-osoitteet: Jokaisella verkkoon liitetyllä laitteella on yksilöllinen IP-osoite, joka mahdollistaa sen tunnistamisen ja paikantamisen verkossa
- Pakettilähetys: IP-protokolla pilkkoo datan pieniin paketteihin, jotka kulkevat verkon kautta määränpäähän tehokkainta reittiä pitkin
- Reititys: Protokolla auttaa löytämään parhaan reitin, jota pitkin datapaketti kulkee lähettäjältä vastaanottajalle.

Esimerkiksi tilanteessa, jossa henkilö haluaa lähettää 2–3 megatavun kokoisen valokuvan, joudutaan kuvatiedosto tyypillisesti jakamaan noin 2000 pakettiin. Tiedon lähettäjän käyttämä laitteisto muodostaa paketin, johon merkitään tarvittavat tiedot paketin ohjaamiseksi vastaanottajalle. Näitä tietoja ovat muun muassa IP-osoite, jolla vastaanottava laite yksilöidään ja käytetty sovellus, kuten web-palvelu, sähköpostipalvelin, videopuhelun vastaanottava mobiililaite tai sisällönjakoalusta. Jokainen yksittäinen paketti kulkee yksittäiselle paketille nopeinta ja tehokkainta reittiä pitkin määränpäähänsä.

Usein tietoliikenteessä ei kuitenkaan käytetä vain yhtä protokollaa, vaan niitä tarvitaan useita luotettavan tiedonsiirron mahdollistamiseksi. Tämän takia IP-protokolla yhdistetään TCP-protokollaan (yhdessä TCP/IP-protokolla). TCP-protokolla käytöllä saadaan IP-protokollan ominaisuuksien lisäksi ominaisuuksina:

- Tiedonsiirron hallinta: TCP vastaa tiedon pilkkomisesta pienempiin paketteihin ja niiden kokoamisesta vastaanottajalle oikeaan järjestykseen
- Virheiden tarkistus: TCP tarkistaa, että kaikki paketit on vastaanotettu ja korjaa mahdolliset tiedonsiirrossa tapahtuneet virheet
- Luotettavuus: Jos jokin paketti katoaa matkalla, TCP lähettää sen uudelleen varmistaen tiedonsiirron täydellisyyden.

Näin ollen esimerkiksi tilanteessa, jossa käyttäjä haluaa avata verkkosivun, päätelaite lähettää pyynnön käyttäen TCP-protokollaa, joka pilkkoo pyynnön paketteihin. IP-protokolla huolehtii pakettien reitittämisestä oikealle verkkopalvelimelle. Verkkopalvelimen TCP-protokolla vastaanottaa paketit, kokoaa ne yhteen ja lähettää vastauksen samalla tavalla takaisin. Lukuisien protokollien käytön jälkeen ja laitteiden välisen tiedonvaihdon jälkeen käyttäjä näkee päätelaitteensa näytöllä halutun sivuston.

Kuten kuvatussa esimerkissä TCP/IP-protokollaparista, usein käytössä on lukuisia eri protokollia; tiedonsiirron sujuvoittamiseksi paketit muodostuvatkin useista protokollakerroksista. Eri kerroksilla on eri käyttötarkoituksia – yhdellä kerroksella saatetaan kuvata sitä, mille laitteelle viesti on tarkoitettu, toisella sitä, miten liikenne on salattu. Etenkin monimutkaisemmissa tiedonsiirtojärjestelmissä tai yhteyksien jälleenmyyntijärjestelyissä protokollakerroksia voi olla toistakymmentä kappaletta. Liikenteen ohjaaminen asiamukaisesti vastaanottajalle edellyttää kaikkien kerrosten käsittelyä. Eri järjestelmien välisen yhteensopivuuden varmistamiseksi protokollat noudattavat useimmiten kansainvälisiä standardeja.

Tietoliikenteen käsittely

Tietoliikenneverkon kuvauksessa todetusti nykyaikainen viestintäverkko koostuu useista tietoa kuljettavista kuiduista ja niitä yhdistävistä laitteistoista. Keskeisiä laitteistoja ovat reitittimet.

Useimmiten tietoliikennepaketin lähettäjä ja vastaanottaja eivät ole suorassa yhteydessä toisiinsa. Tällöin laitteiden välillä on yksi tai useampi reititin eli tietoliikenteen ohjaamiseen suunniteltu laite. Reitittimet tarkastelevat niille saapuvia tietoliikennepaketteja, ja joko siirtävät paketit niiden vastaanottajille, mikäli reititin on suoraan kytköksissä vastaanottajaan, tai ohjaavat paketit seuraavalle reitittimelle, joka on vastaanottajaa lähempänä. Reitittimet keskustelevat keskenään reititysprotokollien, kuten BGP (Border Gateway Protocol) tai IS-IS (Intermediate System to Intermediate System) avulla. Reititysprotokollilla vaihdetaan tietoa siitä, mitä kautta eri IP-osoitteet ovat parhaiten saavutettavissa. Tämä tarkoittaa sitä, että sähköisen viestinnän yksittäiseen viestiin, kuten lähetettyyn valokuvaan, liittyvät tietoliikennepaketit eivät kulkeudu samaa reittiä pitkin vastaanottajalle, vaan ne menevät jokaiselle yksittäiselle paketille tehokkainta ja nopeinta reittiä pitkin vastaanottajalle.

Tietoliikennetiedustelu

Tietoliikennetiedustelussa tiedonhankinta kohdistuu Suomen rajan ylittävään tietoliikennekaapeliin ja siinä kulkeviin valokuitupareihin. Fyysisesti tietoliikennejärjestelmään ohjataan toisin sanoen valokuitujen valoa, mikä vastaa ykkösiä ja nollia. Binäärikoodia tulkitsemalla laitteistot muodostavat tavuja ja tavuista paketteja. Paketit muodostavat loppujen lopuksi kokonaisen viestin, kuten kuvan, tai osan siitä. Ilman viestin sisältöäkin paketeista voidaan saada olennaista tietoa, kuten tietoja viestin lähettäjästä ja vastaanottajasta.

Varsinainen tietoliikennetiedustelu perustuu hakuehtojen käyttöön. Pohjimmiltaan hakuehto palautuu ykkösten ja nollien sarjaan, jota järjestelmässä verrataan järjestelmään tulleeseen tietoliikenteeseen. Jos numerosarjat ovat yhtenevät, voidaan kyseistä tietoliikennettä, tarkemmin sanottuna paketteja, tarkastella tarkemmin. Tarkastelun kohteena on esimerkiksi se, sisältääkö tietoliikennepaketti viestin, ketkä ovat olleet viestin osapuolina ja mistä viesti on peräisin. Sähköisen viestinnän ja salauksen lisääntyminen ovat johtaneet siihen, että tietoliikenteen pakettivirrasta enenevä määrä liittyy muuhun kuin viestin merkityssisältöön.

Tarkemman analyysin lopputulosta voidaan käyttää esimerkiksi tiedusteluraporteissa ja tiedustelun tarkemmassa kohdentamisessa sekä uusien hakuehtojen määrittämisessä.

2.1.5 Tietojärjestelmät

Tietojärjestelmä voidaan määritellä järjestelmäksi, jossa käsitellään ja käytetään tietoa tietyssä tarkoituksessa. Teknisesti tarkasteltuna se yhdistää laitteet, ohjelmistot ja säännöt niin, että tieto saadaan talteen, sitä voidaan käyttää ja sitä voidaan lähettää ja vastaanottaa. Tietojärjestelmä voi muodostua useiden eri laitteiden ja ohjelmistojen tai näiden osien muodostamasta maantieteellisesti ja loogisesti hajautetusta kokonaisuudesta.

Etenkin viimeisen 20 vuoden aikana teknologisen kehityksen kiihtyvä tahti on johtanut siihen, että ihmisten ja organisaatioiden käyttämä tieto ei ole käytännössä säilössä yksittäisellä laitteella. Nykyinen tietoyhteiskunta perustuu tietoverkkojen, tiedon säilömiseen ja käsittelyyn tarkoitettujen palvelimien, ihmisten käyttämien erilaisten päätelaitteiden sekä automaatioon tarkoitettujen sensoreiden ja pientietokoneiden muodostamasta kokonaisuudesta. Myös siviilistiedusteluviranomaisen torjumat uhat toimivat keskeisesti näitä järjestelmiä hyödyntäen.

Tietojärjestelmässä ei siis ole kyse vain yksittäisestä laitteesta tai ohjelmistosta, vaan nykymaailmassa kokonaisuudet koostuvat lukuisista yhteen toimivista laitteista ja ohjelmistoista. Viime kädessä yksittäisellä laitteella käytettävän palvelun takaa löytyy usein lukuisin laitteiden ja ohjelmistojen ketjuja.

2.1.6 Muutokset turvallisuustilanteessa

Kuten valtioneuvoston ulko- ja turvallisuuspoliittisen selonteossa on tuotu esiin maailmanpolitiikan valtasuhteiden murros vaikuttaa Suomen turvallisuusympäristöön. Kiihtyvä strateginen kilpailu ja demokratioiden ja autoritääristen valtioiden välinen globaali vastakkainasettelu ovat johtamassa monenkeskisen yhteistyön sirpaloitumiseen ja alueellistumiseen. Yhdysvaltojen ja Kiinan välillä käydään kilpailua poliittisesta, sotilaallisesta, taloudellisesta ja teknologisesta johtoasemasta maailmassa. Venäjä on puolestaan asemoinut itsensä vastakkainasetteluun Yhdysvaltoja ja muita länsimaita vastaan, osittain yhteistyössä Kiinan kanssa.

Laajalti digitalisoitunut ja verkottunut yhteiskunta on kiinteä osa kybertoimintaympäristöä. Tämä ympäristö on luonut uuden mahdollisuuden valtioille toteuttaa tavoitteitaan uusin keinoin. Näitä tavoitteita voivat olla mm. oman politiikan ja näkemyksen vahvistaminen, toisten valtioiden demokratian heikentäminen vaikuttamalla yhteiskunnan kriittisiin toimintoihin kuten vaaleihin, kriittiseen infrastruktuuriin tai tiedonvälitykseen. Tätä toimintaa kuvataan usein termeillä hybridivaikuttaminen tai laaja-alainen vaikuttaminen.

Tämän takia Suomen on huolehdittava kansallisen tiedustelun kehittämisestä vastaamaan lisääntyneisiin vaatimuksiin ja turvallisuusympäristön muutoksiin. Suomella on oltava valmius tunnistaa, ennaltaehkäistä ja torjua vakoilua, hybridivaikuttamista, terrorismia ja muita kansallisen turvallisuuden uhkia ja sotilaallista uhkaa niin fyysisessä kuin kybermaailmassa. Jo vakiintuneen kansainvälisen tiedusteluyhteistyön lisäksi Suomi osallistuu aktiivisesti Naton tiedusteluyhteistyöhön.

2.2 Lainsäädäntö ja käytäntö

Tiedustelulainsäädäntö, jolla tarkoitetaan siviili- ja sotilastiedustelulainsäädäntöä, tuli voimaan 1. kesäkuuta 2019. Sen antaminen mahdollistettiin säätämällä luottamuksellisen viestinnän suojaa koskeva perustuslain 10 §:n 4 momentti sekä laki tiedustelutoiminnan valvonnasta (121/2019). Siviilitiedustelutoimintaa koskevat keskeiset säännökset sisältyvät poliisilain 5 a lukuun ja tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin.

Seuraavassa arvioidaan turvallisuusympäristön sekä teknologian kehittymisen myötä syntyneitä uusia tarpeita sekä voimassa olevan siviilitiedustelulainsäädännön nykytilaa.

2.2.1 Tietojärjestelmätiedustelua koskevan toimivaltuuden lisääminen poliisilain 5 a lukuun

Siviilitiedustelulainsäädäntö mahdollistaa suojelupoliisille sähköisiin viestintä- ja tiedonkäsittelyvälineisiin ja näiden väliseen viestintään kohdistuvan tiedonhankinnan käyttäen telekuuntelua (PolL 5 a:6), televalvontaa (PolL 5 a:7), teknistä kuuntelua (PolL 5 a:11) ja teknistä laitetarkkailua (PolL 5 a:14) sekä näitä tukevia toimivaltuuksia, kuten edellä mainittuihin tiedustelumenetelmiin käytettävän laitteen, menetelmän tai ohjelmiston sijoittamista muun muassa tietojärjestelmään (PolL 5 a:16). Luottamuksellisen viestin salaisuuden suojaan puuttuvien menetelmien kasuistisesta sääntelystä johtuen edellä mainittuja menetelmiä on välttämätöntä käyttää samanaikaisesti riittävän tiedon hankkimiseksi uhkasta kuten vieraan valtion kyberuhkatoiminasta. Menetelmien rinnakkaiskäytölle voi muodostaa esteen se, että eri menetelmien kohdistaminen on määritelty toisistaan poikkeavalla tavalla.

Poliisilain 5 luvun 5 §:n 1 momentin mukaan telekuuntelulla tarkoitetaan teleosoitteeseen tai telepäätelaitteeseen vastaanotettavan taikka siitä lähetetyn sähköisen viestinnän palveluista annetun lain (917/2014) 3 §:n 43 kohdassa tarkoitetussa *yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa välitettävänä olevan viestin* kuuntelua, tallentamista ja muuta käsittelyä viestin sisällön ja siihen liittyvien välitystietojen selvittämiseksi. Poliisilain 5 a luvun 6 §:n 3 momentin 2 kohdan mukaan telekuuntelua koskevassa vaatimuksessa ja päätöksessä on mainittava *toimenpiteen kohteena oleva henkilö, osoite tai telepäätelaite.*

Poliisilain 5 luvun 8 §:n mukaan televalvonnalla tarkoitetaan sähköisen viestinnän palveluista annetun lain 3 §:n 36 kohdassa tarkoitetun viestinnän välittäjän hallussa olevien välitystietojen hankkimista viestistä, joka on lähetetty poliisilain 5 luvun 5 §:ssä tarkoitettuun viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen, sekä telepäätelaitteen tai teleosoitteen sijaintitiedon hankkimista taikka osoitteen tai laitteen käytön tilapäistä estämistä. Poliisilain 5 a luvun 7 §:n 5 momentin 2 kohdan mukaan televalvontaa koskevassa vaatimuksessa ja päätöksessä on mainittava, vastaavasti kuin telekuuntelua koskevassa vaatimuksessa ja päätöksessä, *toimenpiteen kohteena oleva henkilö, teleosoite tai telepäätelaite*.

Poliisilain 5 luvun 23 §:n 1 momentin mukaan 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. Poliisilain 5 a luvun 14 §:n 3 momentin 2 kohdan mukaan teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava *toimenpiteen kohteena oleva tekninen laite tai ohjelmisto*. Sääntely on käytännössä puutteellinen, sillä tuomioistuimen siviilitiedustelun kohteeksi hyväksymän yksittäisen teknisen laitteen takaa paljastuu säännönmukaisesti kymmeniä tai jopa satoja muita laitteita, jolloin tiedonhankinnan eteneminen edellyttää runsaasti toistuvia uusia tuomioistuinratkaisuja. Muun muassa vieras valtiollinen toimija voi hyödyntää laitteita Suomeen kohdistuvan vakoilun ketjutuksessa. Lisäksi vihamielisessä valtiollisessa kybertoiminnassa hyväksi käytettävien laitteiden väliset yhteydet ja ketjut rakentuvat ja häviävät erittäin nopeasti, minkä takia niihin kohdistuvaan tiedusteluun ei ole mahdollista saada tuomioistuimelta lupaa käytettävissä olevan aikaikkunan puitteissa. Globaaliin tietoverkkoon liitetyn laitteen yksilöinti laitetasolla on haastavaa, ja laite saattaa olla sijoitettuna fyysisesti mihin tahansa päin maailmaa. Edelleen valtiolliset toimijat, organisaatiot ja yhä enenevässä määrin myös yksityiset tahot kykenevät suojaamaan tietojärjestelmiään rakentamalla niitä kerroksittaisiksi ja siten ketjuttamalla niitä ja niiden välisiä yhteyksiä. Esimerkkejä tällaisista ovat mm. organisaatioita suojaavat sisäverkon ja julkisen

Internet-verkon välissä toimivat palomuurit ja edustapalvelimet sekä yksityistenkin henkilöiden käytettävissä olevat VPN-palvelut ja Tor-verkon kaltaisten anonymisointiverkkojen palvelut.

Nykylainsäädännön laitekeskeinen lähestymistapa muodostaa ongelman esimerkiksi seuraavan kaltaisissa tilanteissa:

- erilaisiin sosiaalisen median palveluihin ja pilvipalveluihin tallennetun tiedon hankkiminen;

- muut sellaiset verkon palvelut, joihin kommunikointi ja käyttäjäinteraktio tapahtuu yhden teleosoitteen kautta, mutta taustalla palvelua on toteuttamassa useampi palvelin;

- kyberuhkatoimijoiden moniosaisten, ketjutettujen ja maantieteellisesti hajautettujen Internetin päälle rakennettujen hyökkäysinfrastruktuureiden ja anonymisointiverkkojen tiedustelu;

- ulkomaantiedustelu, jossa toimintaympäristön rajoitteet vähentävät suojelupoliisin mahdollisuutta yksilöidä laitetta, jossa hankittava tieto on tallennettuna.

Poliisilain 5 luvun 17 §:n 1 momentin mukaan teknisellä kuuntelulla tarkoitetaan rikoslain 24 luvun 5 §:n estämättä tapahtuvaa tietyn henkilön sellaisen keskustelun tai viestin, joka ei ole ulkopuolisten tietoon tarkoitettu ja johon keskusteluun kuuntelija ei osallistu, kuuntelua, tallentamista ja muuta käsittelyä teknisellä laitteella, menetelmällä tai ohjelmistolla keskustelun tai viestin sisällön tai sen osapuolten taikka 4 momentissa tarkoitetun henkilön toiminnan selvittämiseksi. Luvun 17 §:n 4 momentin mukaan teknisen kuuntelun edellytyksenä on lisäksi, että henkilön lausumien, uhkausten tai käyttäytymisen perusteella taikka muutoin voidaan perustellusti olettaa hänen syyllistyvän säännöksessä mainittuihin rikoksiin. Poliisilain 5 a luvun 11 §:n 4 momentin mukaan teknistä kuuntelua koskevassa vaatimuksessa ja päätöksessä on mainittava *toimenpiteen kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä taikka tila tai muu paikka*.

Teknisen kuuntelun toimivaltuutta voitaneen luonnehtia luottamuksellisen viestin suojaa nauttivaan viestintään kohdistuvan tiedon hankkimisen mahdollistavaksi yleistoimivaltuudeksi. Teknisen kuuntelun soveltamisalaa ei ole suoraan rajoitettu kyseisen toimivaltuuden määritelmäsäännöksessä. Sen sijaan sen soveltamisalaa on kavennettu säätämällä erikseen telekuuntelusta, televalvonnasta ja teknisestä laitetarkkailusta sekä niiden määritelmistä. Telekuuntelun ja televalvonnan määritelmäsäännöksistä ilmenee, että kyseisiä toimivaltuuksia sovelletaan silloin, kun tiedonhankinta kohdistuu yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa välitettävänä olevaan viestiin. Telekuuntelu ja televalvonta lienee ollut välttämätöntä erottaa teknisen kuuntelun alasta pääasiassa siksi, että ne muusta viestintään kohdistuvasta tiedonhankinnasta poiketen on pääsääntöisesti välttämätöntä toteuttaa viestinnän välittäjän (teleyrityksen) avustuksella, ja viestinnän välittäjän velvollisuudesta avustaa viranomaista telekuuntelun ja -valvonnan toteuttamisessa on siksi ollut tarve säätää erikseen.

Teknisen laitetarkkailun määritelmäsäännöksen mukaan, jos viestintää koskeva tieto tai muu tieto sijaitsee teknisessä laitteessa, sovelletaan teknisen kuuntelun toimivaltuuden sijasta teknisen laitetarkkailun toimivaltuutta. Poliisilain 5 luvun 23 §:n 2 momentissa, jota sovelletaan myös poliisilain 5 a luvun nojalla toteutettavaan tekniseen laitetarkkailuun, on erikseen säädetty, että teknistä laitetarkkailua ei saa kohdistaa sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta kuin laitetarkkailusta säädetään poliisilain 5 luvussa.

Edellä esiin tuodusta seuraa, että yhtä ja samaa tietoa koskeva tiedonhankinta pirstaloituu usean eri toimivaltuuden alle siitä riippuen, sijaitseeko tieto tiedonhankinnan hetkellä jossain

teknisessä laitteessa, yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa taikka muussa viestintäverkossa kuin yleisessä viestintäverkossa tai siihen liitetyssä verkossa.

Tiedon hankkiminen *viestin sisällöstä* tapahtuu telekuuntelulla, teknisellä laitetarkkailulla tai teknisellä kuuntelulla, riippuen siitä, sijaitseeko tieto tiedonhankinnan hetkellä jossain teknisessä laitteessa, yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa taikka muussa viestintäverkossa kuin yleisessä viestintäverkossa tai siihen liitetyssä verkossa.

Yksilöintitiedon hankkiminen tapahtuu televalvonnalla tai teknisellä laitetarkkailulla riippuen siitä, sijaitseeko tieto yleisessä viestintäverkossa tai siihen liitetyssä viestintäverkossa taikka teknisessä laitteessa tai sen sisältämässä ohjelmistossa. Yksilöintitietojen hankkimisesta muussa kuin yleiseen viestintäverkkoon liitetyssä viestintäverkossa ei ole säädelty.

Tiedon hankkiminen *laitteen tai ohjelmiston toiminnasta* tapahtuu teknisellä laitetarkkailulla, jos tieto sijaitsee jossakin teknisessä laitteessa tai sen sisältämässä ohjelmistossa. Tiedon hankkimisesta laitteen tai ohjelmiston toiminnasta viestintäverkossa ei ole säädelty.

Telekuuntelu, televalvonta ja tekninen kuuntelu voidaan vaatia kohdistettavan henkilöön yksittäisen teleosoitteen tai telepäätelaitteen sijasta. Tällöin tuomioistuimen telekuuntelua tai -valvontaa varten myöntämä lupa kattaa kaikki ne telepäätelaitteet ja -osoitteet, jotka luvan voimassaoloaikana ovat kohdehenkilön hallussa tai käytössä. Päätöksen yksittäisen telepäätelaitteen tai -osoitteen kuulumisesta tuomioistuimen myöntämän luvan piiriin tekee suojelupoliisin päällystöön kuuluva poliisimies. Sääntely mahdollistaa nopean päätöksenteon.

Teknisen laitetarkkailun käyttöä koskeva tuomioistuimelle esitettävä vaatimus ja tuomioistuimen päätös sen sijaan eivät voi koskea henkilöä, vaan ne koskevat nykysääntelyn nojalla aina yksittäistä laitetta tai laitteen sisältämää ohjelmistoa.

Varsinkin kybervakoilun ja –vaikuttamisen selvittämisessä ratkaisu, jossa kohteena olevat laitteet ja ohjelmistot on yksitellen yksilöitävä, on toimimaton, koska tuomioistuimen siviilitiedustelun kohteeksi hyväksymän yksittäisen teknisen laitteen takaa säännönmukaisesti paljastuu kymmeniä tai jopa satoja muita laitteita, joita vieras valtio hyödyntää Suomeen kohdistuvan vakoilunsa ketjutuksessa. Vihamielisessä valtiollisessa kybertoiminnassa hyväksi käytettävien laitteiden väliset yhteydet ja ketjut rakentuvat ja häviävät erittäin nopeasti, mistä johtuen niihin kohdistuvaan tiedusteluun ei ole mahdollista saada tuomioistuimelta lupaa käytettävissä olevan aikaikkunan puitteissa.

Ratkaisu on toimimaton myös suojelupoliisin muun kansallisen turvallisuudelle uhan muodostaviin organisaatioihin kohdistamassa tiedonhankinnassa, ja jopa yksittäisiin henkilöihin kohdistuvassa tiedonhankinnassa. Toimimattomuus johtuu siitä, että lähes poikkeuksetta nykyaikaiset digitaaliseen kommunikointiin ja tietojen käsittelyyn tai säilömiseen tarkoitetut tietojärjestelmät koostuvat useista eri yhdessä toimivista laitteista ja ohjelmistoista (esimerkiksi yksittäisen tietokoneen hyödyntämät pilvitallennustilat tai jonkin organisaation sähköpostiviestintään käyttämät palvelimet, tietoliikennelaitteet ja asiakasohjelmistot).

Tietojärjestelmätiedustelun määritelmän piiriin tulisi kuulua sellaista tiedonhankintaa, johon nykyisin sovelletaan telekuuntelua, televalvontaa, teknistä laitetarkkailua ja teknistä kuuntelua koskevaa sääntelyä. Edellä mainittuja muita tiedustelumenetelmiä koskevaa sääntelyä ei tulisi kumota. Siltä osin kuin tietojärjestelmätiedustelun piiriin kuuluu toimenpiteitä, jotka ovat päällekkäisiä telekuuntelu- tai televalvontatoimivaltuuden käytön kanssa, tulisi viestinnän välittäjille säätää kyseisiä toimenpiteitä koskeva avustamisvelvollisuus. Viestinnän välittäjille tulisi säätää velvollisuus ilman aiheetonta viivytystä tehdä televerkkoon tietojärjestelmätiedustelun edellyttämät kytkennät välitettävänä olevan viestinnän kuuntelemiseksi, tallentamiseksi ja muuksi käsittelemiseksi sekä annettava tätä tarkoitusta varten suojelupoliisin käyttöön tarpeelliset tiedot, välineet ja henkilöstö.

Poliisilain 5 a luvussa tulisi näin ollen säätää uudesta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla saataisiin hankkia tietoteknisin menetelmin tietoa kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta, sen sisältämistä tiedoista, tietojärjestelmän osien välillä liikkuvista viesteistä sekä tietojärjestelmään saapuvista tai siitä lähtevistä viesteistä. Tietojärjestelmätiedustelulla tietoa voisi hankkia joko kokonaisesta tietojärjestelmästä tai jostain tietojärjestelmän sellaisesta loogisesta tai fyysisestä osasta, joka toteuttaa tietojärjestelmän jotakin toiminnallisuutta tai joka muutoin voidaan määrittää tietojärjestelmässä omaksi osakseen perustuen tietojärjestelmän käyttäjään tai tietojärjestelmän osan perustellusti oletettuun tietosisältöön.

2.2.2 Kansallista turvallisuutta vaarantavaan tietojärjestelmän toimintaan puuttuminen; tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi

Poliisilain 5 a luvussa tai sotilastiedustelulaissa ei ole säädetty tiedusteluviranomaisille oikeutta puuttua sellaisen ulkomailla sijaitsevan verkkolaitteen tai tietojärjestelmän toimintaan, jota käytetään Suomeen kohdistuvaan ja sen kansallista turvallisuutta uhkaavaan toimintaan, kuten vihamieliseen kybervaikuttamiseen tai -vakoiluun.

Suomessa sijaitsevan laitteen toimintaan puuttuminen on mahdollista sekä poliisilain sääntelyn että sähköisen viestinnän palveluista annetun lain nojalla. Poliisin toimesta tapahtuva laitteen käytön estäminen voinee perustua joko 5 luvun mukaiseen televalvontaan – jonka yksi muoto televalvonnan määritelmäsäännöksen mukaan on teleosoitteen tai telepäätelaitteen käytön tilapäinen estäminen – taikka 2 luvun 17 §:n voimankäyttösääntelyyn. Poliisilain 5 luvun 8 §:n 4 momentin mukaan poliisilla on oikeus lyhytaikaisesti estää teleosoitteiden tai telepäätelaitteiden käyttö tietyllä alueella. Toimenpiteen käytön on oltava välttämätön henkeä tai terveyttä uhkaavan vakavan vaaran torjumiseksi, eikä sillä saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Poliisilain säännöksen yksityiskohtaisten perustelujen mukaan (HE 224/2010 vp, s. 98/II) kysymyksessä ei ole voimassa olevaan televalvontaan kuuluva tietyn teleosoitteen tai telepäätelaitteen käytön tilapäinen estäminen, vaan ennalta määrittämättömän teleosoitteiden ja telepäätelaitteiden joukon käytön lyhytaikainen estäminen vaaran torjumiseksi. Poliisilain esitöissä (HE 224/2010 vp, s. 98/II–99/I) mainitaan esimerkkeinä toimivaltuuden käytöstä tilanteet, jossa on esimerkiksi uhattu räjäyttää pommi tietyssä paikassa tai kansainväliseen huippukokoukseen osallistuvaan henkilöön tiedetään kohdistuvan vakava uhka. Tällaisissa tilanteissa poliisi voisi estää teleosoitteiden ja telepäätelaitteiden käytön hetkellisesti, jotta räjähdettä ei kyettäisi laukaisemaan. Toimenpiteelle asetettaisiin kuitenkin telekuuntelun kaltainen vaaraedellytys. Toimenpiteen tulisi olla välttämätön ja vaaran tulisi olla vakava. Suojattavina intresseinä olisivat vain henki ja terveys. Toimenpiteellä ei saisi myöskään aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi. Tällä korostettaisiin vähimmän haitan periaatteen merkitystä toimivaltuuden käytössä.

Yksityiskohtaisten perustelujen mukaan toimivaltuuden käytölle on asetettu siten varsin tiukat edellytykset, joten sen käyttö olisi vain poikkeuksellisesti mahdollista. Yksittäisten teleosoitteiden tai telepäätelaitteiden käytön tilapäinen estäminen määräytyisi pykälän 1 ja 2 momenttien mukaisesti.

Poliisilain televalvontaa koskeva säännös ei ota suoranaisesti kantaa siihen, voidaanko sillä estää telepäätelaitteen tai teleosoitetta käyttävän laitteen toiminta, vaan yksityiskohtaistenkin perustelujen perusteella vaikuttaisi siltä, että kyse on ennemminkin telepäätelaitteen tai teleosoitten käyttämiseksi tarvittavien sähkömagneettisten aaltojen estämisestä. Näin ollen vaikuttaisi siltä, että toimivaltuutta ei voisi käyttää esimerkiksi tietystä telepäätelaitteesta lähtöisin olevan valokuidussa liikkuvan tietoliikenteen estämiseen tai tämän telepäätelaitteen sulkemiseen viestintäverkkojen kautta viranomaisen toimesta etenkään tilanteessa, jossa toimija on Suomen rajan ulkopuolella.

Tosin säännöksen sanamuoto ei ota varsinaisesti kantaa siihen, miten telepäätelaitteen tai teleosoitteen käyttö estetään. Estäminen on kuitenkin sidottu tiettyyn alueeseen, mikä viitanne yksityiskohtaisten perustelujen mukaisesti nimenomaisesti sähkömagneettisten aaltojen estämiseen.

Liikenne- ja viestintävirasto saa sähköisen viestinnän palveluista annetun lain 273 §:n nojalla päättää merkittävää haittaa aiheuttavan laitteen irrottamisesta viestintäverkosta. Saman lain 172 §:ssä säädetään liikenne- ja viestintävirastolle oikeus mm. fi-verkkotunnukseen suuntautuvan liikenteen estämiseen ja rajoittamiseen, jos se on tarpeen merkittävän tietoturvaloukkauksen estämiseksi.

Jos valtiolliseen kybervakoiluun tai muuhun vihamieliseen toimintaan käytetty laite tai tietojärjestelmä sijaitsee ulkomailla, on tilanne kokonaan toinen. Lähtökohtaisesti tällaisiin tilanteisiin pyritään puuttumaan kansainvälisen oikeusavun kautta tai hyödyntämällä kansainvälisiä yhteistyöverkostoja. Jos lähtömaalla ei ole halukkuutta tai tulkintansa mukaan toimivaltaa tai käytännön mahdollisuutta puuttua Suomen turvallisuutta vahingoittavaan toimintaan, ovat Suomen viranomaisten toimintamahdollisuudet heikot. Viranomaiset eivät voi käyttää toimivaltuuksiaan toisen valtion alueella. Poikkeuksen muodostavat tiedusteluviranomaiset, jotka voivat käyttää tiedustelumenetelmiä tiedon hankkimiseksi myös Suomen rajan ulkopuolella.

Vaikka Suomi voi nykytilassa suojautua vaikuttamisyrityksiltä ja vastata niihin erilaisilla tavoilla kuten hyödyntämällä diplomatiaa, asettamalla pakotteita tai suorittamalla rikostutkintaa, kaikissa tapauksissa nämä keinot eivät ole riittäviä eikä niillä saavuteta haluttua lopputulosta. Näissä tapauksissa valtiolla olisi oltava mahdollisuus vaikuttaa suoraan kyseiseen sitä uhkaavaan toimintaan soveltuvilla keinoilla.

Nyt ei ole mahdollisuutta tietojärjestelmän toiminnan estämiseen tilanteessa, jossa tietojärjestelmää käytettäisiin esimerkiksi Suomen elintärkeiden toimintojen toiminnan lamauttamiseen. Kansalliseen turvallisuuteen liittyvien vakavien vaarojen tehokkaaksi torjumiseksi suojelupoliisille on välttämätöntä säätää tietojärjestelmän käytön estämisen tai sen toiminnan haittaamisen toimivaltuus.

Toimivaltuuden välttämätön tarve liittyy siihen, että tietojärjestelmien ja -verkkojen globaali levinneisyys muodostaa uudenlaisen haasteen kansallisen turvallisuuden uhkien torjumiselle. Kyberuhkatoimijat sekä muut kansallista turvallisuutta uhkaavat toimijat, jotka toiminnassaan hyödyntävät tietoverkkoja ja -järjestelmiä, toimivat pääsääntöisesti ulkomailla, mutta voivat tietoverkkoja pitkin vaikuttaa ja vakoilla Suomen alueella ja Suomen kansalaisten ja organisaatioiden käyttämissä tietojärjestelmissä.

Selkeä toimivalta, päätöksentekojärjestelmä ja kyky vastata Suomeen kohdistuviin uhkiin normaalioloissa on oleellinen osa kansallista turvallisuutta ja yhteiskunnan elintärkeiden toimintojen turvaamista. Useilla länsimailla on vastaava toimivalta vastata niihin kohdistuviin uhkiin ja kansainvälisellä yhteistyöllä osana myös liittoumaa (NATO) on erittäin suuri merkitys uhkiin vastaamisessa. Tulevaisuudessa liittokunnan viitekehyksessä voi ilmetä jäsenmaiden kategorisointia sen suhteen, millä jäsenmailla on toimivalta ja kyky vaikuttaa kybertoimintaympäristössä ja millä ei. Tehokkaan kansainvälisen yhteistyön edellytyksenä on selkeä ja toimiva kansallinen lainsäädäntö.

2.2.3 Peitetoimintavaltuuden kehittäminen; tietoverkot

Poliisilain 5 luvun 28 §:n 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.

Poliisilain 5 a luvun 18 §:ssä säädetään peitetoiminnasta päättämisestä siviilitiedustelussa. Pykälän 3 momentin 5 kohdan mukaan peitetoimintapäätöksessä on mainittava tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä. Poliisilain 5 a luvun 9 §:n 4 momentin mukaan henkilöryhmällä tarkoitetaan vähintään kolmen hengen muodostamaa tietyn ajan koossa pysyvää ja rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin tai yhteisen tavoitteen saavuttamiseksi. Siinä missä perinteisen peitetoiminnan kohdehenkilö tai kohteena oleva ryhmä on yleensä jokseenkin selkeästi rajattavissa, on yksinomaan tietoverkossa tapahtuvalle peitetoiminnalle leimallista se, että siihen liittyviä henkilöitä voi olla erittäin runsaasti, että verkossa toimitaan nimimerkkien turvin, ja että yksittäisten henkilöiden liityntä tiedonhankinnan kohteena olevaan toimintaan ei ole yksiselitteinen tai selvä. Kohdehenkilöiden yksilöinti peitetoimintapäätökseen voi tästä johtuen olla vaikeaa tai mahdotonta.

Myös poliisilain 5 a luvun 9 §:n 4 momentissa määritellyn henkilöryhmän käsitteen soveltuvuus verkossa tapahtuvaan kansallista turvallisuutta uhkaavaan toimintaan voi olla heikko. Verkossa toimivat ryhmittymät eivät aina ole edellä mainitussa määritelmäsäännöksessä tarkoitetulla tavalla jäsentyneitä taikka pysyviä, eivätkä niiden jäsenten motiivit ole kaikilta osin yhdenmukaisia. Tästä huolimatta kysymys voi olla hyvinkin vakavasta radikalisoitumisesta kuten akselerationismista, rotusodan ihannoinnista taikka ääri-islamistisen iskujen ihannoinnista.

Kansallisen turvallisuuden uhkien tunnistamisen tarkoituksessa tietoverkoissa toteutettavaa peitetoimintaa tulisi voida toteuttaa pitkäkestoisesti suojelupoliisin toimialan kannalta olennaisissa ympäristöissä ilman pakotettua henkilöyhteyttä. Näitä ympäristöjä ovat esimerkiksi äärioikeistolaiset, ääri-islamistiset ja valtiollisen vaikuttamisen kannalta merkitykselliset foorumit.

2.2.4 Paikkatiedustelua koskevan sääntelyn täydentäminen näytteenottoa ja esineen/omaisuuden/asiakirjan tilapäistä haltuunottoa koskevalla sääntelyllä

Paikkatiedustelusta säädetään poliisilain 5 a luvun 26 §:ssä. Pykälän mukaan paikkatiedustelulla tarkoitetaan muussa kuin pysyväisluonteiseen asumiseen käytettävässä paikassa tai sellaisessa paikassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon

tai seikan löytämiseksi. Poliisilain 5 a luvun 28 §:ssä säädetään jäljentämisestä siviilitiedustelussa. Pykälän mukaan suojelupoliisilla on oikeus siviilitiedustelussa jäljentää asiakirja tai esine. Jäljentäminen voidaan toimittaa ja usein toimitetaankin paikkatiedustelun yhteydessä. Jäljentäminen voi tulla kyseeseen myös esimerkiksi suunnitelmallisen tarkkailun toimivaltuuden käytön yhteydessä.

Jäljentämissäännöksen yksityiskohtaisissa perusteluissa (HE 202/2017 vp, s. 202) mainitaan esimerkkeinä asiakirjan jäljentämisestä siitä valokuvan ottaminen ja sen skannaaminen puhelimeen asennetulla skannausohjelmalla, sekä esimerkkinä esineen jäljentämisestä 3D-skannerin käyttäminen. Jäljentämissäännös ei mahdollista joissakin tilanteissa tarpeellista näytteiden ottamista paikkatiedustelun tai muun tiedustelumenetelmän yhteydessä löytyvistä aineesta, omaisuudesta tai esineestä. Näytteenottotoimivaltuus on merkityksellinen paitsi sinänsä siviilitiedustelutehtävän näkökulmasta, myös esimerkiksi erittäin vakavien terroristisessa tarkoituksessa tehtävien rikosten estämisen ja sellaisten rikosten rangaistavaksi säädettyyn valmisteluun kohdistuvan esitutkinnan mahdollistamiseksi. Poliisi voisi saamansa palomuuri-ilmoituksen perusteella ryhtyä välttämättömiin toimenpiteisiin ja valmistelurikosta koskevaan esitutkintaan

Jäljentämissäännös ei mahdollista ottaa näytteitä paikkatiedustelun tai muun tiedustelumenetelmän yhteydessä löytyvistä aineesta, omaisuudesta tai esineestä eikä myöskään sellaisten haltuunottoa näytteenottoa tai vaarattomaksi tekemistä varten. Paikkatiedustelusäännöksen yksityiskohtaisten perustelujen mukaan myöskään paikkatiedustelussa ei saada ottaa haltuun tilassa olevia esineitä, asiakirjoja tai muuta omaisuutta, vaan niitä koskevat tarvittavat tiedot tulee tallentaa esimerkiksi valokuvaamalla tai jäljentämällä. Jos tilassa oleva esine on tarpeen jäljentää, se tulee jäljentää sellaisella teknisellä laitteella tai menetelmällä, joka ei edellytä esineen haltuun ottamista. Esitöiden mukaan syy siihen, että asiakirja tai esine tulee jäljentää ilman haltuun ottamista, on siviilitiedusteluoperaation paljastumisriskin minimoiminen.

Siviilitiedustelun kohteina ovat poliisilain 5 a luvun 3 §:n mukaan muun muassa terrorismi ja ulkomainen tiedustelutoiminta. On ilmeistä, että esimerkiksi terroristiseen toimijaan kohdistettavan paikkatiedustelun yhteydessä voi löytyä sellaisia aineita, joita mahdollisesti voidaan käyttää räjähteiden valmistukseen, tai esimerkiksi myrkyllisiä kemikaaleja. Löydettyjä aineita ei kuitenkaan yleensä ole mahdollista tunnistaa tai niiden vaarallisuutta arvioida pelkästään visuaalisesti paikkatiedustelun yhteydessä. Esimerkiksi ulkomaiseen tiedustelutoimijaan kohdistettavan paikkatiedustelun yhteydessä taas voi löytyä sellaisia asiakirjoja, joiden osalta oletettavissa, että niihin sisältyy kemiallisen käsittelyn avulla näkymättömäksi tehtyä kirjoitusta. Omaisuus tai erä siitä tulisi voida ottaa haltuun laboratorio-olosuhteissa suoritettavan analysoinnin mahdollistamiseksi ja aineen tunnistamiseksi. Esimerkiksi räjähteen lähtöaineeksi tai toksiiniksi epäillystä aineesta voitaisiin monessa tapauksessa ottaa niin pieni näyte, ettei omaisuuden väheneminen ole silmin havaittavissa. Vaikka aine, esine tai omaisuus olisi tarpeen ottaa haltuun kokonaisuudessaan, olisi se ainakin osassa tapauksista ilmeisesti mahdollista vaihtaa ulkoisesti sitä muistuttavaan mutta vaarattomaan aineeseen, esineeseen tai omaisuuteen, jolloin uhkan aiheuttava taho ei ainakaan välittömästi havaitsisi haltuunottoa.

Haltuunotto- ja näytteenottotoimivaltuus on tarpeen esimerkiksi erittäin vakavien hybridivaikuttamisen tai laaja-alaisen vaikuttamisen pyrkimysten estämiseksi ja näihin liittyvien rikosten rangaistavaksi säädettyyn valmisteluun kohdistuvan esitutkinnan mahdollistamiseksi. Haltuunotto- ja näytteenottotoimivaltuus on tarpeen esimerkiksi erittäin vakavien terroristisessa tarkoituksessa tehtävien rikosten estämisen ja sellaisten rikosten rangaistavaksi säädettyyn valmisteluun kohdistuvan esitutkinnan mahdollistamiseksi. Poliisilain 5 a luvun 44 § (ns. palomuuripykälä) säätää niistä edellytyksistä, joilla suojelupoliisilla on oikeus tai velvollisuus ilmoittaa siviilitiedustelumenetelmän käytön avulla tietoon tulleesta rikoksesta poliisille. Jo tapahtuneen rikoksen ilmoittamiskynnys on palomuurisääntelyssä sidottu ilmaisuun ”voidaan olettaa

tehdyksi rikos", kun taas vielä estettävissä olevan rikoksen ilmoittaminen edellyttää tietoa rikoksen hankkeilla olosta. Pelkästään siitä seikasta, että esimerkiksi paikkatiedustelun yhteydessä löydetään jokin sellainen aine, esine tai omaisuus, jota ei voida tunnistaa, ei voine synnyttää sellaista olettamaa rikoksen tapahtumisesta tai sellaista tietoa rikoksen hankkeilla olosta, että palomuuri-ilmoituksen tekeminen poliisille olisi mahdollista. Koska asiasta ei voida ilmoittaa poliisille, tulisi suojelupoliisin voida ottaa haltuun aine, omaisuus tai esine sen analysoimiseksi. Sikäli kuin analyysi osoittaisi, että aine, omaisuus tai esine on rikoksentekoon ilmeisesti käytettävä, tulisi palomuurisääntely sovellettavaksi. Poliisi voisi saamansa palomuuri-ilmoituksen perusteella ryhtyä terroristisen rikoksen torjumiseksi välttämättömiin toimenpiteisiin ja valmistelurikosta koskevaan esitutkintaan.

2.2.5 Poliisilaki 5 a luku – siviilitiedustelu; säännöskohtaisia tarkistustarpeita

2 § Tiedustelumenetelmät siviilitiedustelussa

Poliisilain 5 a luvun 2 §:ssä säädetään tiedustelumenetelmistä siviilitiedustelussa. Tiedustelumenetelmiä ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja ohjattu tietolähdetoiminta. Tiedustelumenetelmiä ovat myös 5 a luvussa tarkoitetut paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten. Tarve uusille toimivaltuuksille on noussut toimintaympäristön ja teknisen kehityksen vuoksi. Säännöstä tulisi ajantasaistaa.

4 § Tiedustelumenetelmien käytön edellytykset

Poliisilain 5 a luvun 4 §:ssä säädetään kaikille tiedustelumenetelmille yhteisistä käyttöedellytyksistä. Poliisilain 5 a luvussa ei ole säädöstä pelkästään määritelmille, mutta luvussa toistuva valtiollinen tai siihen rinnastuva toimija on nähty tarpeelliseksi määritellä, vaikka käytännön toiminnassa asiasta ei ole epäselvyyttä. Valtiollisen toiminnan määritelmä sisältyy kuitenkin tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin. Sen mukaan v*altiollisella toimijalla* vieraan valtion tunnistettua viranomaista tai sellaiseen rinnastuvaa toimijaa sekä tarkoitetun tahon palveluksessa olevaa tai sen määräyksessä ja ohjauksessa toimivaa tahoa.

6 § Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättäminen

Poliisilain 5 a luvun 6 §:ssä säädetään telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättämisestä. Telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta päättää tuomioistuin suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Poliisilain 5 a luvun säädellyistä tiedustelumenetelmistä tuomioistuimen päätösvaltaan kuuluvat kokonaan tai osittain 1) telekuuntelu, 2) televalvonta 3) tietojen hankkiminen telekuuntelun sijasta, 4) tukiasematietojen hankkiminen, 5) tekninen kuuntelu, 6) tekninen katselu, 7) tekninen seuranta,8) tekninen laitetarkkailu, 9) paikkatiedustelu ja 10) lähetyksen jäljentäminen. Myös tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa säädetystä tietoliikennetiedustelusta päättäminen kuuluu tuomioistuimen toimivaltaan.

Kaikkiin edellä mainittuihin tiedustelumenetelmiin, telekuuntelu ja tietojen hankkiminen sen sijasta pois lukien, on liitetty mahdollisuus suojelupoliisin kiirepäätökseen. Kiirepäätössäännösten mukaan, jos kyseessä olevaa tiedustelumenetelmää koskeva asia ei siedä viivytystä, suojelupoliisin päällikkö tai tiedustelumenetelmän käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää tiedustelumenetelmän käytöstä siihen asti, kunnes tuomioistuin on ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia on tällöin saatettava tuomioistuimen ratkaistavaksi heti kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua menetelmän käytön aloittamisesta.

Telekuuntelu ja muusta vastaavasta tietojen hankkiminen on ainoa tiedustelutoimivaltuus, jossa kiirepäätöksen tekeminen ei ole mahdollista. Suomeen kohdistuvassa kybervakoilussa hyödynnetään toistensa kanssa kommunikoivien laitteiden ketjuja, jotka muuttuvat hyvinkin nopeasti. Ketjutuksessa tapahtuvien nopeiden muutosten takia, tuomioistuimelta saattaa olla mahdotonta saada nykyisin lupaa telekuunteluun sen aikaikkunan puitteissa, jolloin telekuuntelu pitäisi voida toteuttaa.

Kiirepäätösmahdollisuuden puuttuminen telekuuntelussa ei ole perusteltavissa telekuuntelun sisältämällä muita tiedustelumenetelmiä suuremmalla puuttumisella luottamuksellisen viestin salaisuuden suojaan. Telekuuntelulla puututtaneen kyseiseen perusoikeuteen samassa määrin kuin teknisellä kuuntelulla ja teknisellä laitetarkkailulla, joiden molempien osalta kiirepäätösmahdollisuudesta on säädetty. Kiirepäätösmahdollisuudesta on myös säädetty tietoliikennetiedustelun osalta, ja tietoliikennetiedustelun katsottaneen menetelmän viimesijaisuudesta päätellen puuttuvan luottamuksellisen viestin suojaan laajemmin ja syvällisemmin kuin telekuuntelun.

Telekuuntelun ja sen sijasta tapahtuvan tietojen hankkimisen kiiretilanteen päätöksentekomenettelystä olisi tarkoituksenmukaista säätää samalla tavalla kuin siitä on säädetty muidenkin tiedustelumenetelmien osalta.

14 § Teknisestä laitetarkkailusta siviilitiedustelussa päättäminen

Poliisilain 5 a luvun 14 §:ssä säädetään teknisestä laitetarkkailusta siviilitiedustelussa päättämisestä.

Poliisilain 5 luvun 23 §:n 1 momentin mukaan 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.

Poliisilain 5 a luvun 14 §:n 3 momentin 2 kohdan mukaan teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva tekninen laite tai ohjelmisto.

Teknisen laitetarkkailun käyttöä koskeva tuomioistuimelle esitettävä vaatimus ja tuomioistuimen päätös eivät voi koskea henkilöä, vaan ne koskevat voimassa olevan sääntelyn nojalla aina yksittäistä laitetta tai laitteen sisältämää ohjelmistoa. Teknologinen kehitys on aiheuttanut ongelmia toimivaltuuden soveltamiselle ja sitä kautta tiedon hankinnalle, joten teknisen laitetarkkailun kohdentaminen tulisi muuttaa televalvontaa ja -kuuntelua vastaavasti siten, että tekninen laitetarkkailu voitaisiin kohdistaa myös henkilöön, jolloin tarkkailussa olevan kohdehenkilön käyttämiä laitteita voitaisiin tuomioistuimen myöntämän luvan puitteissa lisätä tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen päätöksellä.

Vertailuna todettakoon, että poliisilain 5 a luvun 6 §:ssä säädetään telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättämisestä ja 7 §:ssä televalvonnasta siviilitiedustelussa päättämisestä. Sekä telekuuntelu että televalvonta voidaan kohdistaa joko henkilöön, teleosoitteeseen tai telepäätelaitteeseen. Kun telekuuntelu- tai televalvontalupa kohdistetaan henkilöön, lupa käsittää telekuuntelu- tai televalvontaluvan kohteena olevan henkilön hallussa olevat tai luvan voimassaoloaikana haltuunsa tulevat tai hänen oletettavasti muuten käyttämänsä teleosoitteet tai telepäätelaitteet. Luvan hakijan on kuitenkin kyettävä osoittamaan perusteet sille, miksi kyseisen henkilön hallussa on kansallisen turvallisuuden kannalta merkityksellistä tietoa. Kun tuomioistuimen luvassa määritelty toimenpiteen kohteena oleva henkilö ottaa käyttöönsä tai hänen oletetaan ottavan käyttöönsä uusia teleosoitteita tai telepäätelaitteita taikka ilmenee, että hänen hallussaan on teleosoite tai telepäätelaite, joita ei ole jo tuomioistuimelle toimitetussa lupahakemuksessa yksilöity, niin tiedusteluviranomainen voi kohdistaa toimenpiteen näihin tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen päätöksellä. Teleosoitteiden tai telepäätelaitteiden lisäämisestä tehdään ilmoitus tiedusteluvalvontavaltuutetulle.

Nykyisen teknisen laitetarkkailun kohdentamisvaatimuksen täyttäminen vaatii suojelupoliisilta edeltävää muuta kuin tekniseen laitetarkkailuun perustuvaa tiedonhankintaa, jotta jokin tietojärjestelmän laite voidaan tunnistaa teknisen laitetarkkailun kohteeksi, ja jotta se voidaan yksilöidä tuomioistuimelle esitettävään vaatimukseen teknistä laitetarkkailua koskevan sääntelyn mukaisesti. Laitekeskeisen sääntelyn ongelmia on tuotu esiin edellä tämän esityksen kohdassa 2.2.1. (tietojärjestelmätiedusteluna koskevan toimivaltuuden lisääminen poliisilakiin). Arvioitaessa teknisen laitetarkkailun soveltuvuutta suojelupoliisin kohteena olevien digitaalisissa ympäristöissä toimivien tai näitä hyödyntävien uhkatoimijoiden tiedustelussa ja torjumisessa on huomioitava, että lainsäädännössä kuten pakkokeinolaissa ja poliisilaissa ajatusmalli teknisestä laitetarkkailusta on lähtenyt siitä, että tiedon hankinnan kohteena on jokin yksittäinen tietokoneen kaltainen laite, jonka toimintaa tarkkaillaan, ja josta tiedonhankinnassa etsittävä tieto löytyy. Lisäksi on vahvasti läsnä oletus, että laite on fyysisesti toimenpidettä suorittavan henkilön saavutettavissa. Teknologinen kehitys on kuitenkin viimeisen 20 vuoden aikana yhä enenevässä määrin ja kiihtyvässä tahdissa johtanut siihen, että ihmisten ja organisaatioiden käsittelemä tieto ei ole säilössä yksittäisellä laitteella. Nykyinen tietoyhteiskunta perustuu tietoverkkojen, tiedon säilömiseen ja käsittelyyn tarkoitettujen palvelimien, ihmisten käyttämien erilaisten päätelaitteiden sekä automaatioon tarkoitettujen sensoreiden ja pientietokoneiden muodostamasta kokonaisuudesta. Myös suojelupoliisin torjumat uhat toimivat enenevissä määrin näissä ympäristöissä.

Tiedonhankinta teknisen laitetarkkailun kohdentamisvaatimusta noudattaen vaikeutuu huomattavasti, estyy tai vaatii pitkälle menevää laintulkintaa. Näin käy erityisesti sellaisissa tilanteissa, joissa tiedonhankinta ei kohdistuisi yksittäiseen laitteeseen tai sen ohjelmistoon, vaan useiden laitteiden, esimerkiksi useiden Internet-palvelimien, ja useiden ohjelmistojen muodostamaan kokonaisuuteen. Tällaisia kokonaisuuksia ovat useimmat nykyaikaiset viestinvaihtoon ja tietojen tallentamiseen tarkoitetut yleisölle saataville saatetut tai organisaatioiden käyttämät järjestelmät.

Teknisen laitetarkkailun kohdemäärittely vastaa käytännössä telekuuntelun ja televalvonnan kohteiden määrittelyä. Näin ollen myös toimivaltuuksien tulisi tältä osin olla yhteneväisiä.

16 § Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa

Poliisilain 5 a luvun 16 §:ssä säädetään laitteen, menetelmän tai ohjelmiston asentamisesta ja poisottamisesta siviilitiedustelussa. Pykälän mukaan suojelupoliisin palveluksessa olevalla

virkamiehellä on oikeus siviilitiedustelussa 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 tai 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 ja kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä.

Pykälän mukaisen asentamisen toteuttajana tulee edellä ilmenevästi olla suojelupoliisin palveluksessa oleva virkamies. Käytännön tiedustelutoiminnassa on kuitenkin havaittu tarve käyttää myös suojelupoliisin ulkopuolista toimenpiteen suorittajana. Tämä liittyy ennen kaikkea toimivaltuuden tehokkaaseen käyttämiseen sekä tiedustelumenetelmän käytön paljastumisen estämiseen.

Teknologian kehittymisen myötä siviilitiedustelumenetelmien käytön paljastumisen estäminen vaatii myös suojelupoliisin toiminnan kehittämistä. Käytännön tiedustelutoiminnassa on havaittu, että pykälässä tarkoitetun toimenpiteen tehokas suorittaminen ja tiedustelumenetelmän käyttäminen voi edellyttää myös ulkopuolisen laitteen tai tietojärjestelmän käyttämistä, jotta suojelupoliisi saa pääsyn siihen kohteeseen, johon toimenpiteen ja tiedustelumenetelmän käyttäminen liittyy. Voimassa olevan sääntelyn perusteella tämä ei ole mahdollista, jolloin suojelupoliisin tehtävän kannalta tarpeellinen tai välttämätön tieto voi jäädä katveeseen.

Poliisilain 5 a luvun 16 §:ää olisi perusteltua tehdä lisäys, joka mahdollistaisi yksityisen henkilön avustaa suojelupoliisia tiedustelumenetelmän käytön edellyttämän asennustoimenpiteen toteuttamisessa.

Tietojärjestelmätiedustelusta säätämisen yhteydessä tulisi samalla ottaa huomioon, että poliisilain 5 a luvun 16 §:ssä säädettäisiin oikeudesta sijoittaa tietojärjestelmätiedusteluun käytettävä laite, menetelmä tai ohjelmisto toimenpiteen kohteena olevaan tietojärjestelmään.

17 § Peitetoimintaa siviilitiedustelussa koskeva esitys ja suunnitelma

Peitetoimintaa siviilitiedustelussa koskevasta esityksestä sekä sen yksilöidystä sisällöstä säädetään poliisilain 5 a luvun 17 §:n 1 momentissa. Esityksessä on mainittava

1) toimenpiteen esittäjä;
2) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöityinä;
3) 3 §:ssä tarkoitettu toiminta;
4) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat;
5) peitetoiminnan tavoite;
6) peitetoiminnan tarpeellisuus;
7) muut peitetoiminnan edellytysten arviointia varten tarvittavat tiedot.

Pykälän 2 momentin mukaan peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma.

Poliisilain 5 a luvun 18 §:ssä säädetään peitetoiminnasta päättämisestä. Peitetoimintaa koskevan esityksen ja 18 §:n mukaisen päätöksen sisältövaatimukset ovat pitkälti yhteneväiset, joskin päätöstä koskevan asiakirjan sisällölle on asetettu yksityiskohtaisempia vaatimuksia kuin esitysasiakirjan sisällölle. Kahden eri asiakirjan laatimista koskevan vaatimuksen taustalla

näyttäisi olevan se, että pakkokeinolain 10 luvun ja poliisilain 5 luvun mukaisessa ns. avoimen poliisin peitetoiminnassa esityksen laatimisvastuu ja peitetoimintaa koskeva päätöksenteko on eriytetty eri poliisiyksiköille. Muun poliisiyksikön kuin suojelupoliisin kohdalla peitetoiminnasta päättää keskusrikospoliisin päällikkö paikallisen poliisilaitoksen esityksestä ja peitetoiminnan toteuttaa keskusrikospoliisi. Suojelupoliisissa erillisen peitetoimintaesityksen laatiminen ja esittely ovat jokseenkin näennäisiä toimenpiteitä, koska peitetoimintaa koskeva päätöksenteko on viraston sisäistä toimintaa.

Peitetoimintaa koskevasta erillisestä esityksestä säätäminen pykälän ensimmäisessä momentissa olisi perusteltua kumota. Pykälän sisällöksi jäisi peitetoiminnan toteuttamista koskevan kirjallisen suunnitelman vaatimus, kun päätöksenteosta säädetään luvun 18 §:ssä. Suojelupoliisin tarvitsemasta peitetoiminnasta päättää suojelupoliisin päällikkö.

18 § Peitetoiminnasta siviilitiedustelussa päättäminen

Poliisilain 5 a luvun 18 §:ssä säädetään peitetoiminnasta päättämisestä siviilitiedustelussa.

Pykälän ensimmäisessä momentissa säädetään sekä poliisilain 5 a luvun 17 §:ssä tarkoitetusta peitetoiminnasta päättämisestä (reaalimaailma) että yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättämisestä.

Reaalimaailman ja tietoverkoissa tapahtuvan peitetoiminnan luonteen eroavaisuuden vuoksi ja toiminnasta saatujen kokemusten nojalla olisi tarkoituksenmukaista, että yksinomaan tietoverkossa toteutettavasta peitetoiminnasta ja siitä päättämisestä säätämisestä säädettäisiin erikseen.

Poliisilain 5 a luvun 18 §:n 4 momentin mukaan peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös. Laissa ei aseteta lopettamispäätökselle sisältövaatimuksia, eikä siinä myöskään säädetä päätöksentekijästä. Olettavaa on, että päätösvallan on ajateltu kuuluvan suojelupoliisin päällikölle, joka myös päättää peitetoiminnan aloittamisesta. Näin ollen kirjallisen lopettamispäätöksen tekemistä koskeva säännös tulisi poistaa laista tarpeettomana.

25 § Tietolähteen turvaaminen siviilitiedustelussa

Yhtenä keskeisenä tiedustelumenetelmänä voidaan pitää tietolähdetoimintaa. Parhaat tietolähteet pystyvät tuottamaan kaikkein syvällisintä tietoa ja tietoa kaikkein salaisimmista asioista. Tietolähteet myös saattavat oman henkensä ja terveytensä usein alttiiksi toimiessaan tietolähteenä. Tämän takia tiedusteluviranomaisen on pidettävä riittävissä määrin huolta tietolähteen turvallisuudesta.

Poliisilain 5 a luvun 25 §:ssä säädetään tietolähteen turvaamisesta. Pykälän 5 momentin mukaan suojelupoliisin päällikkö saa päättää, että tietolähteelle annetaan yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

Tietolähteen turvaaminen ulkomailla tilanteessa, jossa tietolähde on toimittanut ulkomailta käsin tietoja suojelupoliisille, voi olla haastavaa, jolloin tietolähteen saaminen pois kyseisestä maasta voisi olla tarkoituksenmukaisin keino tietolähteen turvaamiseksi. Tietyissä tilanteissa voi olla tarpeen myös järjestää tietolähde Suomen rajan yli myös muita kuin virallisia

rajanylityspaikkoja hyödyntäen tai virallisen rajanylityspaikan kautta peitellysti. Tietolähde ei luonnollisestikaan hengen ja terveyden vaarannuttua voi saapua Suomeen virallisia reittejä pitkin, mistä syystä suomalaisen tiedusteluviranomaisen on avustettava esimerkiksi tietoja antamalla tai vääriä asiakirjoja toimittamalla tietolähteelle tämän rajanylityksessä.

Nykytilassa vaikuttaisi siltä, että viranomaisen avustaessa tietolähteen epätavallisessa rajanylityksessä, syyllistyisi viranomaisen virkamies rikoslain 17 luvun 8 §:ssä tarkoitettuun rikokseen. Esimerkiksi kylmän sodan aikana toteutetussa KGB:n kaksoisagentin Gordievskin pelastamisoperaatiossa keskeinen tietolähde kuljetettiin rajaviranomaisten tietämättä Suomen kautta Norjaan ja edelleen Yhdistyneeseen kuningaskuntaan. Voimassa olevan rikoslain kannalta järjestelyissä avustaneet joutuisivat rikosvastuuseen avustettuaan kaksoisagentin laittomassa maahantulossa. Edellä kuvatussa esimerkissä, jossa Suomea käytettiin kauttakulkuun, tietolähde olisi myös syyllistynyt rikoslain 17 luvun 7 §:ssä tarkoitettuun valtionrajarikokseen, sillä henkilöllä ei ollut asianmukaista asiakirjaa Suomen rajan ylittäessään.

Rikoslain 17 luvun 7 §:ssä säädetään valtionrajarikoksesta. Sen 1 momentin mukaan, joka 1) ylittää tai yrittää ylittää Suomen rajan ilman siihen oikeuttavaa matkustusasiakirjaa, viisumia, oleskelulupaa tai matkustusasiakirjaan rinnastettavaa muuta asiakirjaa tai muualta kuin luvallisesta maahantulo- tai maastalähtöpaikasta tai vastoin lakiin perustuvaa muuta kieltoa kuin maahantulokieltoa, 2) muuten rikkoo rajan ylittämisestä annettuja säännöksiä tai 3) oleskelee tai liikkuu rajavyöhykkeellä tai ryhtyy siellä kiellettyyn toimeen rajavartiolain 51 §:n vastaisesti tai ilman mainitun lain 52 §:ssä edellytettyä lupaa, on tuomittava *valtionrajarikoksesta* sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

Pykälän 2 momentin mukaan valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena.

Rikoslain 17 luvun 8 §:ssä säädetään laittoman maahantulon järjestämisestä. Muun muassa sen 1 momentin 2 kohdan mukaan, joka tuo tai yrittää tuoda Suomeen tai Suomen kautta muuhun maahan ulkomaalaisen, jonka 1 kohdassa tarkoitettu asiakirja on väärä, väärennetty, myönnetty toiselle henkilölle taikka saatu viranomaiselta asiakirjan myöntämisen kannalta merkityksellisen totuudenvastaisen tai harhaanjohtavan tiedon avulla, lahjomalla viranomainen tai virkamiehen väkivaltaisella vastustamisella.

Siviilitiedustelutoiminnan luonteen takia tietolähteen suojaa tulisi vahvistaa tapauksissa, joissa tietolähde saapuu Suomen rajan yli. Jotta suomalainen tiedusteluviranomainen voisi luoda luottamukselliset suhteet kaikista merkittävimpiin tietolähteisiin, voidaan arvioida, että tietolähteen turvallisuudesta huolehtimista pitää merkittävänä edellytyksenä suhteen luomiselle ja syventymiselle. Tilannetta, jossa suomalainen viranomainen saisi tietolähteeltä merkittäviä tietoja ja jättäisi tietolähteen oman onnensa varaan tämän hengen ja terveyden vaarannuttua, voidaan pitää epätoivottavana.

27 § Paikkatiedustelusta siviilitiedustelussa päättäminen

Poliisilain 5 a luvun 26 §:n mukaan paikkatiedustelulla tarkoitetaan muussa kuin pysyväisluonteiseen asumiseen käytettävässä paikassa tai sellaisessa paikassa, jossa tiedustelun kohteeksi on syytä olettaa joutuvan tietoa, josta oikeudenkäymiskaaren 17 luvun 11, 13, 14, 16, 20 tai 21 §:n tai 22 §:n 2 momentin mukaan on velvollisuus tai oikeus kieltäytyä todistamasta, toimitettavaa tiedustelua esineen, omaisuuden, asiakirjan, tiedon tai seikan löytämiseksi.

Poliisilain 5 a luvun 27 §:ssä säädetään paikkatiedustelusta siviilitiedustelussa päättämisestä. Pykälän 1 momentin mukaan tuomioistuin päättää paikkatiedustelusta, jos se kohdistuu muuhun kotirauhan suoiaamaan paikkaan kuin pysyväisluonteiseen asumiseen käytettävään paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana. Pykälän 2 momentti koskee kiiretilanteissa päättämistä. Pykälän 3 momentin mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.

Säännöksen yksityiskohtaisten perusteluiden (HE 202/2017 vp, s. 201-202) mukaan: ”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.”. Voimassa säännöksen sanamuoto ja hallituksen esityksessä aikanaan esitetyt perustelut ovat ristiriidassa. Koska ajoneuvo on paikka, johon ei ole yleistä pääsyä paikkatiedustelun ajankohtana, päättää siitä säännöksen mukaan tuomioistuin. Säännöksen esityöt näyttävät tarkoittavan, että päätösvalta olisi suojelupoliisin virkamiehellä.

Kulkuneuvoon kohdistuvasta paikkatiedustelusta olisi näin ollen perusteltua säätää omana paikkatiedustelun alalajina. Siitä päättäväksi tahoksi olisi perusteltua säätää suojelupoliisin päällystöön kuuluva poliisimies.

39 § Tiedustelumenetelmän käytöstä päättäminen eräissä tilanteissa.

Säännös koskee ulkomaan tiedustelua. Voimassa olevan pykälän 1 momentin mukaan muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättää suojelupoliisin päällikkö. Voimassa olevan säännöksen mukaan ei ole ollut selvää, saako yksittäisen tiedustelumenetelmän käytöstä ulkomailla päättää tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Tämä voinut luoda käytännön ongelman ulkomailla toteuttavien tiedusteluoperaatioiden suorittamisessa, jos yksittäisen tiedustelumenetelmän käyttö edellyttää aina suojelupoliisin päällikön tekemää päätöstä.

41 § Kuuntelu- ja katselukiellot siviilitiedustelussa

Poliisilain 5 a luvun 41 §:ssä säädetään kuuntelu- ja katselukielloista siviilitiedustelussa.

Tässä esityksessä ehdotetaan säädettäväksi poliisilain 5 a lukuun uudesta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla saataisiin hankkia tietoteknisin menetelmin tietoa kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta, sen sisältämistä tiedoista, tietojärjestelmän osien välillä liikkuvista viesteistä sekä tietojärjestelmään saapuvista tai siitä lähtevistä viesteistä. Poliisilain 5 a luvun 41 §:ssä säädetyt kuuntelukiellot tulisi ulottaa koskemaan tietojärjestelmätiedustelua vastaavalla tavalla kuin ne voimassa olevassa sääntelyssä koskevat telekuuntelua ja sen sijasta tapahtuvaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua ja teknistä laitetarkkailua.

46 § Kiiretilanteessa saadun tiedon hävittäminen

Poliisilain 5 a luvun 46 §:n 1 momentissa säädetään tuomioistuimen kumoaman suojelupoliisin virkamiehen tekemän kiirepäätöksen vaikutuksista. Momentin nojalla, jos suojelupoliisin

päällystöön kuuluva poliisimies on 7 §:n 1 momentissa (televalvonta) , 8 §:n 1 momentissa (tukiasematietojen hankkiminen), 11 §:n 1 momentissa (tekninen kuuntelu), 12 §:n 1 momentissa (tekninen katselu), 13 §:n 1 momentissa (tekninen seuranta), 14 §:n 1 momentissa (tekninen laitetarkkailu) tai 27 §:n 2 momentissa (paikkatiedustelu) 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 hankkeilla on rikos, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta, ja rikos on vielä estettävissä.

Telekuuntelun ja sen sijasta tapahtuvan tietojen hankkimisen kiiretilanteen päätöksentekomenettelystä ja tietojen hävittämisestä tulisi säätää vastaavan kaltaisesti kuin niistä on säädetty muiden tiedustelumenetelmien osalta. Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelusta päättämisestä säädetään poliisilain. 5 a luvun 6 §:ssä.

47 § Tiedustelumenetelmän käytöstä ilmoittaminen

Poliisilain 5 a luvun 47 §:ssä säädetään tiedustelumenetelmän käytöstä ilmoittamisesta. Pykälän 3 momentissa säädetään siitä, että 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. Henkilöllisyyden tietäminen ei yksinään riitä kirjallisen ilmoituksen tekemiseen, vaan tiedossa olisi oltava oleskelupaikka tai muu osoite, jonne ilmoitus voidaan toimittaa.

51 § Teleyrityksen velvollisuus avustaa siviilitiedustelussa

Poliisilain 5 a luvun 51 §:ssä teleyrityksen avustamisvelvollisuudesta säädetään viittaamalla poliisilain 5 luvun 61 §:ään. Poliisilain 5 luvun 61 §:ssä on perinteisesti säädetty teleyrityksen ns. avustamisvelvollisuudesta rikoksen estämisessä ja paljastamisessa. Vuonna 2023 poliisilain 5 luvun sääntelyä muutettiin niin, että avustamisvelvolliseksi tahoksi määriteltiin teleyrityksen sijasta viestinnän välittäjä. Samansisältöinen muutos toteutettiin myös pakkokeinolain avustamispykälään (PKL 10:63).

Poliisilain 5 luvun 61 §:n 1 momentti kuuluu nykyisin seuraavasti:

> *”Viestinnän välittäjän on ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun ja televalvonnan edellyttämät kytkennät sekä annettava poliisiviranomaisen käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa telekuuntelu tai televalvonta toteutetaan poliisiviranomaisen toimesta teknisellä laitteella. Viestinnän välittäjän on lisäksi annettava pidättämiseen oikeutetun poliisimiehen tai suojelupoliisin päällystöön kuuluvan poliisimiehen käyttöön hallussaan olevat teknisen seurannan toimeenpanoa varten tarpeelliset tiedot.”*

Muutoksella on korjattu ongelmallisuus, jossa yksityisten yritysten velvollisuus avustaa viranomaista telekuuntelussa ja –valvonnassa sekä avustamisesta seuraava oikeus korvauksen

saamiseen oli säädetty ainoastaan perinteisille teleyrityksille, vaikka nyky-yhteiskunnassa viestinnän välittäjien joukko niitä huomattavasti suurempi ja heterogeenisempi. Valtiollisten kyberuhkien torjunnassa esimerkiksi konesaliyritysten rooli telekuuntelussa ja -valvonnassa avustamisessa olisi keskeinen ja viestintäteknologioiden kehittyessä yhä kasvava, mutta avustamisvelvollisuutta ei ole ulotettu niihin. Poliisilain 5 luvussa jo huomioitu ongelmallisuus koskee yhtä lailla siviilitiedustelua, joten olisi välttämätöntä muuttaa myös poliisilain 5 a luvun 51 §:ää. Vaikka kyse onkin viittaussäännöksestä, joka saa asiallisen sisältönsä 5 luvun 61 §:stä, osoittaa se oman sanamuotonsa perusteella avustamisvelvollisuuden aiempaan tapaan pelkästään teleyrityksille. Viittaussäännöksen ei voida katsovan laajentavan avustamisvelvollisuutta viestinnän välittäjiin, vaikka viittauksen kohteena olevassa pykälässä avustamisvelvollisuus kohdistetaankin niihin.

52 § Korvaus teleyritykselle siviilitiedustelussa avustamisesta ja tietojen antamisesta

Poliisilain 5 a luvun 52 §:ssä säädetään teleyrityksen korvausoikeudesta ja tietojen antamisesta siviilitiedustelussa avustamisesta viittaamalla poliisilain 5 luvun 62 §:ään (korvaus teleyritykselle). Säännös liittyy 51 §:ssä säädettyyn velvollisuuteen avustaa siviilitiedustelussa. Korvausoikeutta koskeva sääntely tulisi muuttaa viittaussäännöksestä täsmälliseksi säädöstekstiksi liittyen esille tuotuun tarpeeseen muuttaa 51 §:ää.

Poliisilain 5 luvussa ja pakkokeinolain 10 luvussa avustamisvelvollisuus on kohdistettu yleisesti kaikkiin viestinnän välittäjiin, mutta oikeus korvauksen saamiseen avustamisesta on säädetty pelkästään teleyrityksille. Poliisi- ja pakkokeinolakien muuttamista koskeviin hallituksen esityksiin HE 217/2022 vp ja 275/2022 vp ei sisältynyt ehdotusta, jonka mukaan avustamisvelvollisiksi tahoiksi tulisi teleyritysten sijasta säätää viestinnän välittäjät, vaan kyse oli lakiehdotuksiin niiden eduskuntakäsittelyn aikana tehdyistä muutoksista (LaVM 30/2022 vp ja HaVM 42/2022 vp). Korvaukseen oikeutettujen tahojen määrittely lienee jäänyt tuossa yhteydessä epähuomiossa yhdenmukaistamatta avustamisvelvollisten tahojen uudelleenmäärittelyn kanssa. On vaikea nähdä perusteita sille, että teleyrityksiä kohdellaan edullisemmin kuin muita viestinnän välittäjiä.

57 § Kansainvälinen yhteistyö

Poliisilain 5 a luvun 57 §:ssä säädetään kansainvälisestä yhteistyöstä siviilitiedustelussa. Pykälän 3 momentin mukaan suojelupoliisin päällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja siihen liittyvästä tiedustelumenetelmien käytöstä. Pykälän sanamuodon mukaan suojelupoliisin päällikön päätöksellä voidaan sallia myös vieraan valtion toimivaltaiselle viranomaiselle sallia oikeus toimimiseen Suomen alueella kansallisen turvallisuuden suojaamiseksi yhteistyössä suojelupoliisin kanssa. Nykyisessä turvallisuuspoliittisessa keskustelussa termi vieras valtio on vakiintunut tarkoittamaan Suomen kansallista turvallisuutta uhkaavaa valtiota. Pykälässä tarkoitettu yhteistyö tapahtuu kuitenkin Suomelle ei-vihamielisen valtion toimivaltaisen viranomaisen kanssa. Asiantilan selventämiseksi vieraan valtion termi tulisi muuttaa termiksi ulkomainen, joka on edellistä neutraalimpi ilmaus.

Edelleen pykälän 3 momentin mukaan vieraan valtion toimivaltaisella virkamiehellä on oikeus suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää niitä tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä. Sääntelyn alkuperäisenä tarkoituksena on ollut, että vieraan valtion viranomainen voisi käyttää mainittuja tiedustelumenetelmiä, koska ne merkitsevät vain vähäistä puuttumista perusoikeuksiin, eikä yhdelläkään niistä

kajottaisi luottamuksellisen viestin salaisuuden suojaan. Suojelupoliisin ohjauksessa ja valvonnassa toimiva vieraan valtion eli ulkomainen virkamies toimii suojelupoliisin tiedonhankinta-operaatiossa avustavassa roolissa. Ulkomaisella virkamiehellä voi olla sellaista osaamista tai muita ominaisuuksia, joita suomalaisella virkamiehellä ei ole ja jota tarvitaan operaation onnistuneeksi toteuttamiseksi. Kansainvälisen yhteistyön käytännössä on kuitenkin havaittu, että ulkomaisen toimivaltaisen viranomaisen avustamismahdollisuutta tarvitaan myös muissa kuin voimassa olevassa laissa lueteltujen tiedustelumenetelmien käytössä. Yhteistyössä toteutettavien tiedustelumenetelmien luettelo tulisi korvata yleisemmällä ilmauksella, joka mahdollistaisi kaikkien tiedustelumenetelmien käytön yhteisissä tiedusteluoperaatioissa.

2.2.6 Laki tietoliikennetiedustelusta siviilitiedustelussa

4 § Tietoliikennetiedustelun käytön edellytykset

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 4 §:ssä säädetään tietoliikennetiedustelun käytön edellytyksistä. Pykälän 1 momentin mukaan tietoliikennetiedustelun käytön yleisenä edellytyksenä on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta, eikä tietoja ole hankittavissa muulla tiedustelumenetelmällä.

Pykälän 2 momentin mukaan, jos tietoliikennetiedustelun *hakuehtojen käyttö koskee ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon* tietoliikennettä, tietoliikennetiedustelun tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Se, sovelletaanko tietoliikennetiedusteluun matalampaa vai korkeampaa edellytyskynnystä, ratkeaa näin ollen sen perusteella, katsotaanko hakuehtojen käytön koskevan ”ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä”. Ilmaisun merkityssisältöä selostetaan hallituksen esityksessä HE 202/2017 vp seuraavasti: ”Pelkän [4 §:n] 1 momentin mukaisen tuloksellisuusodotuksen soveltaminen edellyttäisi käytännössä, että sen vieraan valtion tai sellaiseen rinnastuvan tahon tietoliikenne, johon hakuehtoja käytetään, liikkuu viestintäverkossa muusta tietoliikenteestä erillään. Kyse olisi siis tilanteista, joissa 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 lisäksi sovellettavaksi myös 2 momentissa säädettäväksi ehdotettu välttämättömyysedellytys”.

Nykyinen verkonosien jako ei ole teknisesti sellainen, että sitä voitaisiin käyttää erittelemään valtiollisia tietoliikenneverkkoja. Tietoliikennetiedustelulain 4 §:n 2 momentissa säädetyn matalamman edellytyskynnyksen soveltamisala on tällä hetkellä määritelty sellaisella tavalla, että säännös on käytännössä merkityksetön. Sääntelyä tulisi muuttaa niin, että tietoliikennetiedustelun käytön matalampaa edellytyskynnystä voitaisiin soveltaa tilanteissa, joissa tietoliikennetiedustelun tarkoituksena on kerätä vieraan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä tiedon saamiseksi kansallista turvallisuutta uhkaavasta toiminnasta eli tiedonhankinnan kohteena on valtiollinen toimija. Merkitystä tuomioistuimen edellytysharkinnassa ei tulisi olisi sillä, voiko siinä tietoliikenteessä, johon hakuehtoja vertaillaan, kulkea muutakin kuin valtiollista tietoliikennettä. Merkitystä tulisi olla ainoastaan sillä, koskeeko tuomioistuimen lupa valtiollisen toimijan ja sen tietoliikenteen tietoliikennetiedustelua. Laajempi tietoliikennevirta, johon hakuehtoja verrataan, ja joka ei ohjaudu jatkokäsittelyyn, ei päädy tiedusteluviranomaisten haltuun.

5 § Tietoliikennetiedustelun kohdistaminen

Sisällöllisen hakuehdon kielto tietoliikennetiedustelussa

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain *5 §:n 1 momentin* mukaan tietoliikennetiedustelu kohdistetaan tietoliikenteen automatisoidun erottelun avulla. Automatisoitu erottelu perustuu 7 tai 9 §:n mukaisessa menettelyssä hyväksyttyjen hakuehtojen käyttöön.

Pykälän 2 momentin mukaan 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.

Pykälän 3 momentin mukaan hakuehtona ei saa käyttää Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 2 §:n 4 kohdan mukaan hakuehdolla tarkoitetaan tietoa, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne, ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään.

Lain 5 §:n 2 momentissa säädetty sisällöllisen hakuehdon käytön kielto haittaa merkittävästi tietoliikennetiedustelun tehokkuutta ja se johtaa tilanteisiin, joissa tiedusteluviranomaisten haltuun tarpeettomasti päätyy tiedustelun kohteena olevan uhkan kannalta epäolennaista sivullista viestintää. Muun muassa momentin 2 kohdan nojalla viestin sisältöä kuvaavaa hakuehtoa saadaan käyttää, jos hakuehto kuvaa haitallisen tietokoneohjelman tai -käskyn sisältöä. Muissa tapauksissa viestin sisältöä koskevan hakuehdon käyttö tietoliikenteen automaattisessa erottelussa on kielletty.

Edellä mainitun ns. sisällöllisen hakuehdon käytön kiellon todetaan lain esitöissä (HE 202/2017 vp s. 124) tarkoittavan sitä, että luottamuksellisen viestin sisältöä kuvaavan hakuehdon käyttö on tietoliikennetiedustelussa täysin kielletty, eikä hakuehtoina siten saada käyttää luottamuksellisen viestin semanttiseen sisältöön kuuluvia ilmaisuja tai henkilöiden nimi- tai yksilöintietoja. Lain esitöiden mukaan ”kyse olisi tiedustelutoiminnalle asetetusta merkittävästä rajoituksesta, jonka tarkoituksena olisi mahdollisimman pitkälle turvata sivullisen asemassa olevien henkilöiden viestintäsalaisuuden ydinalue”. Kielto haittaa merkittävästi tietoliikennetiedustelun tehokkuutta ja sen on todettu johtavan lainsäätäjän nimenomaisen tarkoituksen vastaisesti tilanteisiin, joissa tiedusteluviranomaisten haltuun tarpeettomasti päätyy sellaista tiedustelun kohteena olevan uhkan kannalta epäolennaista sivullista viestintää, joka nauttii luottamuksellisen viestin salaisuuden suojaa. Asiantila on noteerattu hallitusohjelmassa, joka edellyttää viestin sisältöön kohdistuvien hakuehtojen käytön mahdollistamisen tiedustelutoiminnassa.

Viestien semanttiseen sisältöön kohdistuvat hakuehdot ovat monessa tapauksessa mahdollista muotoilla sellaisiksi, että ne erottelevat vähemmän ja kohdennetummin tietoliikennettä tietoliikennetiedustelun automaattisen ja manuaalisen käsittelyn piiriin kuin nykyisin nimenomaisesti sallitut, esimerkiksi ip-osoitealueita, autonomisten järjestelmien numeroita ja domain-nimiä koskevat hakuehdot. Salauksen yleistymisestä huolimatta viestin sisällön käyttäminen hakuehtona mahdollistaa keräyksen tarkentamisen. Tällöin tiedusteluviranomaisten analyysijärjestelmiin ei edes väliaikaisesti päätyisi niin useasti sellaisia viestejä, jotka eivät ole tiedustelutiedon hankinnan kannalta relevantteja.

Siviilitiedustelulainsäädännön esitöissäkin todetusti tietoliikennetiedustelusta säätäneiden eurooppalaisten vertailuvaltioiden lainsäädännöissä ei ole asetettu rajoituksia tai esteitä käyttää sisällöllisiä hakuehtoja, vaan ”sisällöllisten hakuehtojen käytölle asetetut rajoitukset ovat omintakeinen suomalainen ratkaisu”. Kyseinen ratkaisu toimii tällä hetkellä nimenomaisten tarkoitusperiensä vastaisesti.

Edellä käsitelty sisällöllisen hakuehdon käytön kielto olisi perusteltua kumota.

Kielto käyttää Suomessa olevan telepäätelaitteen tai teleosoitteen yksilöiviä tietoja -hakuehtona (5 § 3 mom.)

Tietoliikennetiedustelusta siviilitiedustelussa annetun *lain 5 §:n 3 momentin* mukaan hakuehtona ei saa käyttää Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Hallituksen esityksessä HE 202/2017 vp edellä mainittua säännöstä perustellaan sillä, että jos telepäätelaitteen tai telepäätelaitteen haltija olisi Suomessa ja kyseisen telepäätelaitteen tai -osoitteen yksilöintitiedot suojelupoliisin tiedossa, olisi tiedonhankinta suoritettava poliisilain 5 a luvussa säädettyjen tiedustelumenetelmien – telekuuntelun, tietojen hankkimisen telekuuntelun sijasta tai televalvonnan – avulla, sikäli kuin niille säädetyt edellytykset täyttyvät. Hallituksen esityksen mukaan tällä tavalla pystyttäisiin minimoimaan vaikutus sivullisten tietoliikenteeseen.

Lain 4 §:ssä säädetään tietoliikennetiedustelun käytön edellytyksistä. Pykälän 1 momenttia täydennettiin lakiehdotuksen eduskuntakäsittelyn aikana niin, että tietoliikennetiedustelun käyttö edellyttää muun ohella myös, että hankittavat tiedot eivät ole hankittavissa muulla tiedustelumenetelmällä (viimesijaisuusedellytys). Koska kyseisen ns. viimesijaisuusedellytyksen soveltaminen ratkaisee kysymyksen tietoliikennetiedustelun ja teletiedustelumenetelmien (ynnä kaikkien muidenkin tiedustelumenetelmien) välisestä suhteesta, on lain 5 §:n 3 momentissa säädetty erillinen kielto käyttää hakuehtona Suomessa olevan telepäätelaitteen tai teleosoitteen yksilöivää tietoa tarpeeton.

Lisäksi on tilanteita, joissa teletiedustelumenetelmien kuten telekuuntelun käyttäminen on mahdotonta, mutta telepäätelaitteen tai teleosoitteen yksilöivää tietoa olisi mahdollista käyttää tietoliikennetiedustelun hakuehtona sikäli kuin tämä olisi sallittua. Esimerkiksi sähköpostiosoite on oikeudelliselta luonteeltaan tietoliikennetiedustelulain 5 §:n 3 momentissa mainittu teleosoite. Telekuuntelua ei ole mahdollista kohdentaa ja toteuttaa pelkästään sähköpostiosoitetta koskevan tiedon avulla, mutta tietoliikennetiedustelussa sähköpostiosoitetta koskevan tiedon käyttö hakuehtona olisi mahdollista. Lain 5 §:n 3 momentin nimenomainen kielto käyttää Suomessa olevan henkilön hallussa olevaa teleosoitetta hakuehtona estää tämän.

Edellä käsiteltyä tietoliikennetiedustelusta siviilitiedustelussa annetun lain 4 §:n 1 momentin ns. viimesijaisuusedellytystä ei sovelleta sellaiseen tietoliikennetiedusteluun, joka kohdistuu yksinomaan valtiollisiin toimijoihin. Pykälän 2 momentin mukaan, jos tietoliikennetiedustelun hakuehtojen käyttö koskee ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, tietoliikennetiedustelun käytön tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tällaisessa tietoliikennetiedustelussa se seikka, että telekuuntelua olisi mahdollista käyttää, ei sulje pois tietoliikennetiedustelun käytön mahdollisuutta. Lain 5 §:n 3 momentissa säädetty kielto kuitenkin estää tietoliikennetiedustelun käytön.

Lain 5 §:n *3 momentissa* säädetty kielto käyttää telepäätelaitteen tai teleosoitteen yksilöiviä tietoja tietoliikennetiedustelun hakuehtona tulisi poistaa. Telepäätelaitteen tai teleosoitteen yksilöivä tieto lienee tarkin ajateltavissa oleva hakuehto.

10 § Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 10 §:ssä säädetään tietoliikennetiedustelun teknisestä toteuttamisesta ja muusta yhteistyöstä sotilastiedusteluviranomaisen kanssa.

Sotilastiedusteluviranomainen on suojelupoliisin tarvitseman tietoliikennetiedusteluun liittyvän teknisten tietojen käsittelyn tekninen toteuttaja. Lain 10 §:n 2 momentin mukaan suojelupoliisi voi antaa Puolustusvoimien tiedustelulaitokselle toimeksiannon sotilastiedustelulain 66 §:ssä tarkoitettuun teknisten tietojen käsittelyyn. Puolustusvoimien tiedustelulaitos hakee suojelupoliisin puolesta sotilastiedustelulain 67 §:n mukaisen luvan (tuomioistuimelta) teknisten tietojen käsittelyyn sekä toimittaa mainitun lain 66 §:n 2 momentissa tarkoitetun tilastollisen analyysin tuloksen suojelupoliisille sen jälkeen, kun se on saanut luvan teknisten tietojen käsittelyyn ja toteuttanut luvan mukaiset toimenpiteet.

Sotilastiedustelulain 73 §:n 1 momentin mukaan tietoliikennetiedustelun teknisellä toteuttamisella suojelupoliisin puolesta tarkoitetaan 1) suojelupoliisin Puolustusvoimien tiedustelulaitokselle antamaan toimeksiantoon perustuvaa teknisten tietojen tilastollista analyysia ja analyysin toimittamista suojelupoliisille sekä 2) tuomioistuimen suojelupoliisille myöntämän luvan mukaista Suomen rajan ylittävässä viestintäverkon osassa liikkuvan tietoliikenteen hankkimista automatisoidun tietojen käsittelyn avulla ja hankittujen tietojen luovuttamista edelleen suojelupoliisille.

Puolustusvoimien tiedustelulaitos ei saa selvittää viestin sisältöä.

Säännellyssä järjestelyssä on käytännössä havaittu haasteita, joiden vuoksi sääntely ei palvele varsinaisen tietoliikennetiedustelun kohdentamista ja toteuttamista. Tarkennustarve koskisi muun muassa teknisten tietojen käsittelyä viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamisessa.

Lainsäädäntöratkaisun tulisi mahdollistaa molempien osapuolten osallistumisen toimenpiteiden suorittamiseen siltä osin kuin se on niiden yhteisten etujen mukaista ja palvelee niiden tietoliikennetiedustelun kohdistamista.

13 § Tallenteiden ja asiakirjojen tarkastaminen

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 13 §:ssä säädetään tietoliikennetiedustelussa kertyneiden tallenteiden ja asiakirjojen tarkastamisesta. Pykälän mukaan poliisilain 5 luvun 7 §:ssä tarkoitetun suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen on ilman aiheetonta viivytystä tarkastettava tietoliikennetiedustelun käytössä kertyneet tallenteet ja asiakirjat.

Pykälä vastaa asiallisesti voimassa olevaa poliisilain 5 a luvun 42 §:n sääntelyä, jonka mukaan suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen on ilman aiheetonta viivytystä tarkastettava tiedustelumenetelmän käytössä siviilitiedustelussa kertyneet tallenteet ja asiakirjat.

Tallenteiden tarkastamisvelvollisuus kytkeytyy siviilitiedustelulainsäädännössä säädettyjen hävittämisvelvollisuuksien toteuttamiseen. Tietoliikennetiedustelulla hankitun tiedon hävittämisestä säädetään tietoliikennetiedustelusta siviilitiedustelussa annetun lain 15 §:ssä. Tiedot on hävitettävä viipymättä, jos käy ilmi, että

- viestinnän molemmat osapuolet olivat Suomessa silloin, kun viestintä tapahtui
- lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta lain 12 §:ssä tarkoitetulla tavalla
- tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi. Tällä kohdin tietyissä tapauksissa tietoa voidaan kuitenkin säilyttää.

Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 14 § asettaa suhteellisen aikarajan tallenteiden tutkimiselle. Sitä, missä ajassa tutkiminen tulisi viimeistään tehdä, määrittää valtioneuvoston siviilitiedustelusta antaman asetuksen (709/2019) 1 §, jonka mukaan tiedustelumenetelmän käytön lopettamisen jälkeen on laadittava pöytäkirja ilman aiheetonta viivytystä, kuitenkin viimeistään 90 päivän kuluessa. Koska asetuksesta myös tulee esille, että pöytäkirjassa on tehtävä selkoa muun muassa tietoliikennetiedustelulla hävitettyjen tietojen määrästä, hävittämistapahtumasta, hävittämisajankohdasta ja hävittämisperusteesta yksilöitynä sekä tiedon säilyttämisestä, on lähtökohtana, että tarkastaminen on tullut suorittaa ennen pöytäkirjan laatimista.

Tarkastamissäännöksen voidaan katsoa soveltuvan erittäin huonosti kyberympäristössä käytettäviin tiedustelumenetelmiin kuten tietoliikennetiedustelu. Tietoliikennetiedustelulle leimallinen piirre on, että sen avulla saadut datamäärät voivat olla erittäin suuria. Hankitun aineiston tarkastaminen kohtuullisessa ajassa siten, että se systemaattisesti käytäisiin läpi ja siitä eroteltaisiin tiedustelukieltojen alaiset ja siviilitiedustelun kannalta merkityksettömät tiedot, on suurista datavolyymeista johtuen osin mahdotonta ja siihen pyrkiminen vie kohtuuttoman paljon voimavaroja.

Tietoliikennetiedustelulla kerätään aina tietoja tiettyyn nimenomaiseen tarkoitukseen, joka ilmenee kyseessä olevan tiedustelumenetelmän käyttöä koskevasta vaatimuksesta ja päätöksestä. Vertailun vuoksi voidaan todeta, että tiedustelu poikkeaa esitutkinnasta siten, että sillä ei ole samanlaista loppupistettä kuin rikoksen selvittämiseen tähtäävällä esitutkinnalla, joka päätetään esitutkintalaissa (805/2011) säädetyin menettelyin. Tiedustelun avulla hankitun tiedon todellisen merkityksen tunnistaminen siinä vaiheessa, kun aineisto tulisi tarkastaa, ei välttämättä ole mahdollista. Aineiston tarkastamisvelvollisuudesta erillinen vaade on lakisääteinen hävittämisvelvollisuus, jos hallussa havaitaan olevan hävittämisvelvollisuuden alaista tietoa. Jo edellä mainittu tietoliikennetiedustelusta siviilitiedustelussa annetun lain 15 §:n mukainen tiedon hävittämisvelvollisuus koskee suojelupoliisin hallussa olevaa tietoa, jossa viestinnän molemmat osapuolet olivat Suomessa, lähettäjällä tai vastaanottajalla taikka tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta kyseisestä tiedosta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla taikka tietoa ei tarvita kansallisen turvallisuuden suojaamiseksi. Tietyin laissa säädetyin edellytyksin tietoa voidaan luovuttaa rikostorjuntaan ja tallettaa rekisteriin.

Lain 13 §:n tarkastamisvelvollisuus tulisi kumota edellä todetun johdosta. Tämä ei vaikuttaisi hävittämisvelvollisuuteen.

20 § Tietoliikennetiedustelun käytöstä ilmoittaminen

Tietoliikennetiedustelun käytöstä ilmoittamisesta säädetään tietoliikennetiedustelusta siviilitiedustelussa annetun lain 20 §:ssä.

Säännöksen mukaan, jos 6 §:ssä tarkoitetussa käsittelyssä on manuaalisesti selvitetty Suomessa tietoliikennetiedustelun käytön aikana olleen henkilön luottamuksellisen viestin tai tallentaman tiedon sisältö tai poliisilain 5 luvun 8 §:ssä tarkoitettu tunnistamistieto, ilmoitetaan hänelle tietoliikennetiedustelusta noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelun ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan ole, jos tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

Tietoliikennetiedustelusta ilmoittamiseen sovelletaan osittain telekuuntelusta ilmoittamista siten kuin siitä on säädetty poliisilain 5 a luvun 47 §:ssä. Mainitun 47 §:n nojalla telekuuntelusta on viipymättä ilmoitettava tiedonhankinnan kohteena olleelle henkilölle kirjallisesti sen jälkeen, kun tiedustelumenetelmän käytön tarkoitus on saavutettu, viimeistään kuitenkin vuoden kuluttua telekuuntelun käytön lopettamisesta. Pykälä sisältää säännökset tuomioistuimen luvalla tapahtuvasta telekuuntelusta ilmoittamisen lykkäämisestä ja kokonaan ilmoittamatta jättämisestä, jota myös sovelletaan tietoliikennetiedustelusta ilmoittamiseen.

Siviilitiedustelulainsäädäntöä koskeneessa hallituksen esityksessä HE 202/2017 vp ehdotettiin, että tietoliikennetiedustelusta olisi ilmoitettu vain sellaiselle Suomessa tietoliikennetiedustelun käytön hetkellä olleelle henkilölle, jonka luottamuksellisen viestin tai tallentaman tiedon sisältö on selvitetty manuaalisesti. Perustuslakivaliokunta piti hallituksen esityksestä antamassaan lausunnossa (PeVL 35/2018 vp) tätä ratkaisua riittämättömänä. Valiokunta piti tämän vuoksi välttämättömänä, että ilmoittamisvelvollisuus ulotetaan myös viestin tunnistamistietoihin kohdistuvaan manuaaliseen käsittelyyn, ja asetti tällaisen muutoksen tekemisen edellytykseksi lain käsittelylle tavallisen lain säätämisjärjestyksessä (PeVL 35/2018 vp, s. 23-24).

Voimassa oleva sääntely näyttäisi tarkoittavan, että ilmoitusvelvollisuus kohdistuu tiedonhankinnan mahdollisen kohdehenkilön ohella hyvin laajasti myös sellaisiin henkilöihin, jotka eivät ole olleet tiedonhankinnan kohteena vaan jotka joko kommunikoivat tiedonhankinnan kohteen kanssa tai ovat tiedonhankintatehtävän näkökulmasta varsinaisia sivullisia. Tietoliikennetiedustelun käyttöä koskeva ilmoitusvelvollisuus poikkeaa täysin muiden tiedustelumenetelmien käyttöä koskevasta ilmoitusvelvollisuudesta, joka kohdistuu vain siihen henkilöön, joka on tiedustelumenetelmää koskevassa vaatimuksessa ja päätöksessä mainittu kyseisen tiedustelumenetelmän kohdehenkilönä. Nykyinen ilmoitusvelvollisuus vertautuu siihen, että suunnitelmallisesta tarkkailusta olisi velvollisuus ilmoittaa kaikille niille henkilöille, joita koskien tarkkailua suorittava poliisimies on tehnyt näköhavainnon puolen vuoden mittaisen tarkkailun aikana, ja siihen, että tilaan kohdistuvasta teknisestä katselusta olisi velvollisuus ilmoittaa kaikille niille henkilöille, jotka sattumalta ovat lyhytaikaisesti katselun aikana käyneet katselun kohteena olevassa tilassa. Tietoliikennetiedustelun osalta ongelma voi kuitenkin kertautua monikymmenkertaiseksi johtuen siitä tietoliikenteen volyymista, joka menetelmän avulla voidaan saada.

Sääntelyn kasuistisuus johtaa siihen, että sitä on erittäin vaikeaa soveltaa käytännössä. Ilmoittamisvelvollisuuden olemassaolon edellytyksenä on, että a) henkilö on ollut Suomessa tietoliikennetiedustelun hetkellä, b) että hänen viestinsä tai tallentamansa tiedon sisältö taikka tunnistamistieto on selvitetty, c) että edellä mainittu selvittäminen on tehty manuaalisesti, d) että kyseiset selvitetyt tiedot ovat nauttineet luottamuksellisen viestin suojaa, ja e) että tietoja ei ole hävitetty tiedustelukiellon alaisina tai irrelevanssiperusteella. Sääntely johtaa monipolvisuutensa seurauksena vaikeisiin tulkintatilanteisiin koskien sitä, keitä henkilöitä ilmoittamisvelvollisuus periaatteessa koskee ja ketkä henkilöt kullakin hetkellä tosiasiassa ovat ilmoitusvelvollisuuden piirissä. Sääntely myös edellyttää, että suojelupoliisi jatkuvasti seuraa tilannetta ja sen kehittymistä jopa satojen sellaisten tunnistamistietojen osalta, jotka eivät ole olleet tiedonhankinnan varsinaisina kohteina.

Tietoliikennetiedustelulla ei välttämättä ole henkilöllistä kohdetta.

Tietoliikennetiedustelulla tietoon voi tulla eri tahojen tietoliikenneyhteyksiin liittyviä tunnistamistietoja, jotka on tarpeen säilyttää. Kansallisen turvallisuuden suojaaminen ei välttämättä kuitenkaan edellytä sen selvittämistä, onko kunkin tunnistamistiedon taustalla luonnollinen henkilö vai ei, kuka kyseinen luonnollinen henkilö siinä tapauksessa on, ja nauttiiko se viesti, johon tunnistamistieto liittyy, luottamuksellisen viestin salaisuuden suojaa. Tietoliikennetiedustelun ilmoitusvelvollisuutta koskeva sääntely näyttäisi johtavan velvollisuuteen selvittää poliisilain toimivaltuuksia, esimerkiksi lain 4 luvun 3 §:ssä säädettyä tiedonsaantioikeutta, käyttäen edellä mainitut seikat pelkästään ilmoitusvelvollisuuden toteuttamiseksi. Tämä johtaa siihen, että henkilöiden henkilöllisyys täysin tarpeettomasti selviää suojelupoliisille. Tämän voitaneen katsoa loukkaavan heidän yksityisyyttään olennaisesti enemmän kuin se, että heidän käyttämänsä verkkotunniste on osunut tietoliikennetiedustelun hakuehdon perusteella seulottuun liikenteeseen**.**

Suomen ratkaisu ilmoitusvelvollisuuden suhteen myös poikkeaa esimerkiksi Sveitsin tai Ruotsin ratkaisuista. Sveitsin tiedustelulaissa (*Nachrichtendienstgesetz*) tietoliikennetiedustelusta ei ole lainkaan säädetty velvollisuutta ilmoittaa, mikä johtuu siitä, että kyseisellä menetelmällä ei sen luonteesta johtuen katsota ylipäätään olevan selvästi eroteltavissa olevia henkilöllisiä kohteita. Ruotsin signaalitiedustelulain (*Lag om signalspaning i* ***f****örsvarsunderrättelseverksamhet)* 11 a-b §:issä ilmoitusvelvollisuudesta säädetään **s**euraavasti

> **11 a §**
>
> ***Om det vid signalspaning enligt denna lag har använts sökbegrepp som är direkt hänförliga till en viss fysisk person, ska personen underrättas om detta, om inte annat följer av 11 b §. Underrättelsen ska innehålla uppgift om när inhämtningen skett och syftet med inhämtningen.***
>
> ***En underrättelse ska lämnas så snart det kan ske utan men för försvarsunderrättelseverksamheten, dock senast en månad efter att det inhämtningsuppdrag som föranlett inhämtningen avslutades.***
>
> **11 b §**
>
> ***Underrättelse enligt 11 a § får skjutas upp, om sekretess hindrar att underrättelsen lämnas. Har det på grund av sekretess inte kunnat lämnas någon underrättelse inom ett drån det att inhämtningsuppdraget avslutades, behöver någon underrättelse inte lämnas.***

Sääntelyä tulisi tarkistaa. Ilmoitusvelvollisuudesta säätämisen tarkoituksena on mahdollistaa se, että salaisen tiedonhankinnan kohteena ollut henkilö voi saattaa tutkittavaksi tiedonhankinnan lainmukaisuuden. Tiedustelutoiminnan valvonnasta annetun lain 12 §:n mukaan tiedustelutoiminnan kohteena ollut tai henkilö, joka epäilee, että häneen on kohdistettu tiedustelua, voi pyytää tiedusteluvalvontavaltuutettua tutkimaan häneen kohdistuneen tiedustelumenetelmän lainmukaisuuden. Lisäksi saman lain 11 §:n mukaan jokainen, joka katsoo, että tiedustelutoiminnassa on rikottu hänen oikeuksiaan tai menetelty muutoin lainvastaisesti, voi kannella tiedusteluvalvontavaltuutetun valvontavaltaan kuuluvassa asiassa.

2.2.7 Rajavartiolaki

Turvallisuusympäristön muutoksen ja tehokkaan resurssien käytön sekä viranomaisyhteistyön takia on noussut esiin tarve siitä, että Rajavartiolaitos osallistuisi suojelupoliisin pyynnöstä siviilitiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä suojelupoliisin tiedustelutehtävien tukemiseksi.

2.3 Laki viranomaisten toiminnan julkisuudesta

Julkisuuslain 31 §:ssä säädetään viranomaisen asiakirjan salassapidon lakkaamisesta.

Julkisuuslain 31:n *1 momentin* mukaan viranomaisen asiakirjaa ei saa pitää salassa, kun salassapidolle laissa säädetty tai lain nojalla määrätty aika on kulunut tai kun asiakirjan salassa pidettäväksi määrännyt viranomainen on peruuttanut salassapitoa koskevan määräyksen.

Pykälän *2 momentin* mukaan viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty tai lain nojalla määrätty. Yksityiselämän suojaamiseksi 24 §:n 1 momentin 24–32 kohdassa salassa pidettäväksi säädetyn asiakirjan tai niitä vastaavan muussa laissa salassa pidettäväksi säädetyn tai muun lain nojalla salassa pidettäväksi määrätyn asiakirjan salassapitoaika on 50 vuotta sen henkilön kuolemasta, jota asiakirja koskee tai, jollei tästä ole tietoa, 100 vuotta.

Pykälän *3 momentin mukaan* kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan turvallisuusluokiteltua tietoa, tai tietoa sellaisesta kiinteistöstä, rakennuksesta, rakennelmasta, järjestelmästä, laitteesta tai menetelmästä, joka on käytössä 2 momentissa tarkoitetun 25 vuoden määräajan jälkeenkin, samoin kuin sellainen maanpuolustusta tai väestönsuojelua tai poikkeusoloihin varautumista varten laadittu suunnitelma ja arvio, jonka tietoja sisältyy voimassa olevaan vastaavaan suunnitelmaan, on kuitenkin pidettävä salassa 1 momentissa tarkoitetun ajan jälkeenkin, jos tiedon antaminen asiakirjasta aiheuttaisi edelleen tämän lain 24 §:n 1 momentin 2, 7 ja 8 tai 10 kohdassa tarkoitetun seurauksen. Tällaiset asiakirjat tulevat julkisiksi, kun kiinteistöä, rakennelmaa tai laitetta ei enää käytetä sellaiseen käyttötarkoitukseen, jonka johdosta asiakirjat ovat olleet salassa pidettäviä, taikka kun tiedot eivät enää sisälly voimassa olevaan suunnitelmaan taikka kun turvallisuusluokitus on kumottu.

Pykälän *4 momentin* mukaan, jos on ilmeistä, että asiakirjan tuleminen julkiseksi aiheuttaisi tässä pykälässä tarkoitetun määräajan päätyttyäkin merkittävää haittaa niille eduille, joiden suojaamiseksi salassapitovelvollisuus on säädetty, valtioneuvosto voi pidentää määräaikaa enintään 30 vuodella. Mitä edellä säädetään, ei kuitenkaan sovelleta 3 momentissa tarkoitettuihin asiakirjoihin.

Tasavallan presidentin kansliasta annetun lain (100/2012) 83 §:n mukaan tasavallan presidentin ja kanslian asioiden ja asiakirjojen julkisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään.

Ulkopolitiikan toimialueen asiakirjat

Julkisuuslain 24 §:n 1 momentin 1 kohdan nojalla salassa pidettäviä viranomaisen asiakirjoja ovat valtioneuvoston ulkopoliittisia asioita käsittelevän valiokunnan asiakirjat, jollei valiokunta toisin päätä, sekä ulkoasioita hoitavan ministeriön ja Suomen edustustojen poliittiset tilannearvioinnit, poliittisista tai taloudellisista suhteista toisen valtion kanssa käytyjä neuvotteluja koskevat asiakirjat ja ulkoasiainhallinnon alaan kuuluvat salakirjoitetut viestit, jollei asianomainen ministeriö toisin päätä.

Kohta koskee perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvia asiakirjoja, ja ne ovat pääsäännön mukaan salassa pidettäviä. Valtioneuvoston ulkopoliittisia asioita käsittelevällä valiokunnalla tarkoitetaan nykyisin ulko- ja turvallisuuspoliittista ministerivaliokuntaa. Käytännöksi on muodostunut ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteiset kokoukset (TP UTVA). Kyseinen 1 kohta suojaa siten ensinnäkin TP UTVA-asiakirjoja. Lisäksi 1 kohdassa säädetyillä ”ulkoasioita hoitavan ministeriön ja Suomen

edustustojen poliittisilla tilannearvioinneilla sekä poliittisista tai taloudellisista suhteista toisen valtion kanssa käytyjä neuvotteluja koskevilla asiakirjoilla" tarkoitetaan käytännössä ulkoministeriössä tai Suomen edustustoissa laadittuja raportteja, kokousmuistioita, neuvotteluasiakirjoja ja muita vastaavia perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvia asiakirjoja.

Julkisuuslain 24 §:n 1 momentin 1 kohdassa on kyse ehdottomasta salassapidosta. Näiden asiakirjojen salassapitovelvollisuus on siten riippumaton asiakirjan antamisesta aiheutuvista tapauskohtaisista vaikutuksista. TP UTVA sekä ulkoministeriö voivat kuitenkin "päättää toisin" eli ne voivat päätöksellään antaa tietoja kohdassa tarkoitetuista asiakirjoistaan.

Julkisuuslain 24 §:n 1 momentin 2 kohdan nojalla salassa pidettäviä ovat muut kuin 1 kohdassa tarkoitetut asiakirjat, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, asiakirjat, jotka liittyvät kansainvälisessä lainkäyttö- tai tutkintaelimessä tai muussa kansainvälisessä toimielimessä käsiteltävään asiaan, ja asiakirjat, jotka koskevat Suomen valtion, Suomen kansalaisten, Suomessa oleskelevien henkilöiden tai Suomessa toimivien yhteisöjen suhteita toisen valtion viranomaisiin, henkilöihin tai yhteisöihin, jos tiedon antaminen niistä aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai edellytyksille toimia kansainvälisessä yhteistyössä.

Ulkoministeriössä on tunnistettu tarve pidentää viranomaisten 24 §:n 1 momentin 1 kohdassa salassa pidettäväksi säädettyjen asiakirjojen salassapitoaikaa. Samalla on tunnistettu tarve pidentää 24 §:n 1 momentin 2 kohdassa salassa pidettäväksi säädettyjen asiakirjojen salassapitoaikaa siltä osin, kun kyse on ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjoista, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön. Molemmat lainkohdat sääntelevät näiltä osin – eli ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian osalta – perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvia asiakirjoja, ja niissä on syytä olla yhdenmukaiset salassapitoajat.

Ensinnäkin tarve perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvien asiakirjojen pidennetylle salassapidolle korostuu nykyisessä kiristyneessä turvallisuusympäristössä ja Suomen Nato-jäsenyyden myötä. Kansainvälisiltä järjestöiltä, kuten Natolta, tai toisilta valtioilta saatuja turvaluokiteltuja asiakirjoja suojataan Suomessa hyväksyttyjen ja voimaansaatettujen kansainvälisten tietoturvasopimusten nojalla 25 vuoden yleisen salassapitoajan jälkeenkin (ks. julkisuuslain 31 §:n 3 momentti ja laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004), sekä HE 20/2005 vp, s. 14). Natolta, muilta kansainvälisiltä järjestöiltä tai toisilta valtioilta saatua salassa pidettävää tietoa voi kuitenkin ilmetä myös Suomen omista kansallisista asiakirjoista, esimerkiksi sellaisista asiakirjoista, joita Suomen virkahenkilöt laativat Suomen sisäistä käyttöä varten. Suomen virkahenkilöiden laatimat Naton tai muiden kansainvälisten kokousten ja neuvotteluiden muistiinpanot, kokousraportit tai TP UTVA:lle niistä laaditut asiakirjat voivat siten sisältää tällaista kansainvälisiltä järjestöiltä tai toisilta valtioilta saatua tietoa, joka niiden mukaan tulisi pitää salassa kauemmin kuin 25 vuotta. Tällaisten tietojen tuleminen julkisiksi Suomessa vastoin toisen valtion tai kansainvälisen järjestön tahtoa vahingoittaisi Suomen etua kansainvälisessä yhteistyössä. Suomen asema luotettavana yhteistyökumppanina ja Nato-liittolaisena edellyttää näin ollen, että toisilta valtioilta tai kansainvälisiltä järjestöiltä saatu salassa pidettävä tieto pidetään myös Suomessa salassa eli ettei tieto tule julkiseksi Suomessa aikaisemmin kuin muissa valtioissa tai kansainvälisissä järjestöissä. Edellä todettu koskee myös tasavallan presidentin ja tasavallan presidentin kanslian asiakirjoja, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön.

Toiseksi julkisuuslain voimaantulosta (1.12.1999) on nyt kulunut yli 25 vuotta, mutta osa 25 vuotta sitten laadituista TP UTVA-asiakirjoista sekä UM:n ja edustustojen raporteista ja

neuvotteluasiakirjoista, samoin kuin tasavallan presidentin tai tasavallan presidentin kanslian asiakirjoista, on kuitenkin sellaisia, että niiden salassapidolle on edelleen tarvetta. Muuttuneessa turvallisuusympäristössä julkisen viranomaistiedon epäasiallisen hyödyntämisen riskit ovat kasvaneet. Julkisuuslain 24 §:n 1 momentin 1 kohdassa tarkoitettujen asiakirjojen ja 2 kohdassa tarkoitettujen Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevien ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjojen julkiseksi tulemiseen liittyy mahdollisuus käyttää niitä väärin sellaisiin tarkoituksiin, jotka ovat omiaan vaikeuttamaan Suomen kansainvälisiä suhteita. Ulkovallat ovat myös vuosien varrella saattaneet kehittää keinoja löytää näistä asiakirjoista Suomen haavoittuvuuksia. Turvallisuusympäristön muutoksen johdosta nykyistä 25 vuoden salassapitoaikaa voidaan siten pitää liian lyhyenä tällaisten asiakirjojen kohdalla.

Kolmanneksi julkisuuslain yleisen 25 vuoden salassapitoajan on katsottu voivan osoittautua liian lyhyeksi myös tilanteessa, jossa ulkoministeriön virkahenkilön laatiman raportin tiedot tulisivat julkisiksi henkilön uran aikana. Suomi saa nimittää suurlähettiläänsä toiseen valtioon vain tämän toisen valtion suostumuksella (agrementti). Suomen ulkomaanedustuston henkilökunta voi myös tarvita viisumin kyseiseen kohdevaltioon. Raporttien julkiseksi tuleminen liian aikaisin voisi aiheuttaa siten joissakin tilanteissa haittaa suomalaisten diplomaattien maahanpääsylle ja toimintaedellytyksille. Tämä puolestaan voisi vaarantaa Suomen kansainvälisiä suhteita ja asemaa kansainvälisessä yhteisössä. Myös tällaisissa tilanteissa olisi siten tarve 25 vuotta pidemmälle salassapitoajalle.

Edellä selostettuun perustuen ulkoministeriössä on tunnistettu tarve pidentää viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 1 kohdassa tarkoitettujen asiakirjojen ja 2 kohdassa tarkoitettujen ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevien asiakirjojen salassapitoaikaa nykyisestä 25 vuodesta 40 vuoteen.

Kansallinen turvallisuus (valtion turvallisuus) ja maanpuolustus

Julkisuuslain 24 §:n 1 momentin 9 kohdan mukaan salassa pidettäviä viranomaisen asiakirjoja ovat, jollei erikseen toisin säädetä, suojelupoliisin ja muiden viranomaisten asiakirjat, jotka koskevat valtion turvallisuuden ylläpitämistä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna valtion turvallisuutta. Muihin viranomaisiin kuuluu myös sisäministeriö.

Julkisuuslain 24 §:n 1 momentin 10 kohdan mukaan salassa pidettäviä ovat asiakirjat, jotka koskevat sotilastiedustelua, puolustusvoimien varustamista, kokoonpanoa, sijoitusta tai käyttöä taikka muuta sotilaallista maanpuolustusta taikka maanpuolustusta palvelevia keksintöjä, rakenteita, laitteita tai järjestelmiä taikka maanpuolustuksen kannalta muutoin merkityksellisiä kohteita taikka puolustusvalmiuteen varautumista, jollei ole ilmeistä, että tiedon antaminen niistä ei vahingoita tai vaaranna maanpuolustuksen etua.

<u>Suojelupoliisi</u>

Suojelupoliisin valtion turvallisuuden vuoksi salassa pidettävien asiakirjojen 60 vuoden salassapitoaika perustui ennen 1.12.2024 valtioneuvoston 16.6.1981 tekemään päätökseen 1049/401/81 ja voimassa olevan julkisuuslain 37 §:n 4 momentin voimaantulosäännökseen. Kyseinen vuoden 1981 valtioneuvoston päätös koski etsivän keskuspoliisin, valtiollisen poliisin ja suojelupoliisin arkistoihin kuuluvien, eräitä poikkeuksia yleisten asiakirjain julkisuudesta sisältävän asetuksen (22.12.1951/650) mukaan salassa pidettävien asiakirjojen salassapitoajan pidentämistä 35 vuodella. Valtioneuvoston päätöstä muutettiin 29.4.1992 niin, että etsivän

keskuspoliisin ja valtiollisen poliisin arkistoihin kuuluvien asiakirjojen salassapito lakkasi 1.5.1992 lukien. Vuoden 1992 päätös ei koskenut suojelupoliisia.

Suojelupoliisin asiakirjojen salassapitoaika on ollut 1.12.2024 alkaen valtioneuvoston 28.11.2024 tekemän päätöksen nojalla 55 vuotta. Päätöksellä pidennetään valtion turvallisuuden ylläpitämistä koskevien suojelupoliisin asiakirjojen salassapitoaikaa 30 vuotta siitä ajankohdasta, mitä säädetään viranomaisten toiminnan julkisuudesta annetun lain 31 §:n 2 momentissa. Julkisuuslain 31 §:n 4 momentin mukaan, jos on ilmeistä, että asiakirjan tuleminen julkiseksi aiheuttaisi tässä pykälässä tarkoitetun määräajan päätyttyäkin merkittävää haittaa niille eduille, joiden suojaamiseksi salassapitovelvollisuus on säädetty, valtioneuvosto voi pidentää määräaikaa enintään 30 vuodella.

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. Suojelupoliisi suorittaa tiedonhankintaa ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

Salassapitoajan säätäminen lain tasolla on välttämätöntä, koska on ilmeistä, että merkittävää haittaa aiheuttaisi esimerkiksi sellaisten suojelupoliisin asiakirjojen julkiseksi tulo, jotka koskevat suojelupoliisin omaa tiedonhankintaa, tietolähdetoimintaa, toista valtiota koskevat ja vakoiluun tai vastatiedusteluun liittyvät asiakirjat, terrorismin torjuntaan liittyvät asiakirjat, kansainvälistä yhteistyötä koskevat asiakirjat mukaan lukien kansainvälisessä yhteistyössä saadut asiakirjat, suojelupoliisin henkilöstöä koskevat asiakirjat ja asiakirjat, jotka sisältävät tietoa suojelupoliisin suorituskyvystä ja kyvykkyydestä sekä näiden ylläpitoon liittyvät asiakirjat, jolleivat ne sisälly jo edellä oleviin ryhmiin.

On ilmeisestä, että mikäli suojelupoliisin salassa pidettäviä ja sensitiivisiä tietoa ei voitaisi suojata riittävän pitkään, suojelupoliisin edellytykset hankkia tietoa kansallisen turvallisuuden suojaamiseksi ja torjua Suomeen kohdistuvia kansallisen turvallisuuden uhkia heikkenisi merkittävästi.

Suojelupoliisin asiakirjojen julkiseksi tuleminen ennenaikaisesti tarkoittaisi, että suojelupoliisin tekemä tiedonhankinta tulisi tiedonhankinnan kohteiden ja myös vieraiden valtioiden tietoon. Suojelupoliisi ei siten voisi tehdä pitkäaikaista tiedonhankintaa, jos olisi vaara, että tiedot tulisivat julkiseksi sellaisena ajankohtana, kun tietoa olisi edelleen välttämätöntä hankkia. Näin ollen on ilmeistä, että asiakirjojen julkituleminen aiheuttaisi merkittävää haittaa kansalliselle turvallisuudelle, valtio- tai yhteiskuntajärjestykselle.

Kansainvälisen tiedusteluyhteistyön kannalta tiedusteluyhteistyössä saatuja tietoja ei voida ilman toisen valtion suostumusta tai toisen valtion puolesta julkistaa Suomessa. Tämä tietojen ja yhteistyön suojaamisvelvollisuus on myös laajempi kuin yksittäisiä asiakirjoja koskeva salassapito, koska yhteistyö itsessään kuuluu luottamuksellisuuden ja siten salassapidon piiriin.

Salassapitoajasta tulisi säätää lain tasolla ja, kuten ennen 1.12.2024, tarve salassapitoaikaan olisi 60 vuotta.

<u>Maanpuolustus</u>

Puolustusvoimien tehtävistä säädetään laissa puolustusvoimista. Lain 2 §:n mukaan Puolustusvoimien tehtävänä on muun muassa Suomen sotilaallinen puolustaminen, Pohjois-Atlantin liiton yhteinen puolustus, muiden viranomaisten tukeminen, osallistuminen Euroopan unionin toiminnasta tehdyn sopimuksen 222 artiklaan tai Euroopan unionista tehdyn sopimuksen 42 artiklan 7 kohtaan perustuvaan apuun tai muuhun kuin 2 kohdassa tarkoitettuun tehtävään sisältyvään kansainvälisen avun antamiseen, yhteistoimintaan ja muuhun kansainväliseen toimintaan sekä osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan ja sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa.

Sotilastiedustelun tarkoituksena on hankkia ja käsitellä tietoa Suomeen kohdistuvasta tai Suomen turvallisuusympäristön kannalta merkityksellisestä sotilaallisesta toiminnasta taikka sotilastiedustelulain 4 §:n 2 momentissa tarkoitetusta toiminnasta ylimmän valtiojohdon päätöksenteon tukemiseksi ja sotilastiedustelualaissa säädettyjen Puolustusvoimien tehtävien suorittamiseksi.

Julkisuuslain 31 §:n 4 momentin mukaan, jos on ilmeistä, että asiakirjan tuleminen julkiseksi aiheuttaisi tässä pykälässä tarkoitetun määräajan päätyttyäkin merkittävää haittaa niille eduille, joiden suojaamiseksi salassapitovelvollisuus on säädetty, valtioneuvosto voi pidentää määräaikaa enintään 30 vuodella. Säännöksen mukaan tätä ei kuitenkaan sovelleta 3 momentissa tarkoitettuihin asiakirjoihin. Siten pykälän 4 momentin mukainen mahdollisuus määräajan pidennykseen ei koske julkisuuslain 24 §:n 1 momentin 10 kohdassa tarkoitettuja maanpuolustusta koskevia asiakirjoja; niiden salassapitoaikaa arvioidaan tapauskohtaisesti.

Heikentyneessä turvallisuusympäristössä sotilastiedustelun kyky tuottaa tietoa sotilaallisesta toimintaympäristöstä suunnittelun ja päätöksenteon tueksi sekä ja kyky ennakoida toimintaympäristön kehityskulkuja on tärkeää ja toimintaa on suojattava. On ilmeisestä, että mikäli sotilastiedustelun julkisuuslain 24 §:n 1 momentin 10 kohdassa tarkoitettuja merkityksellisiä salassa pidettäviä ja sensitiivisiä tieoja ei voitaisi suojata riittävän pitkään, vaarantaisi se maanpuolustuksen etuja. Edelleen on ilmeisestä, että edellytykset hankkia tietoa ja torjua Suomeen kohdistuvia kansallisen turvallisuuden uhkia heikkenisi merkittävästi. Tapauskohtaisen tarkastelun ja tapauskohtaisten salassapitoajan jatkamisen sijasta olisi perusteltua katsoa asiaa kokonaisvaltaisesti muun muassa asioiden tai tekijöiden keskinäisriippuvuuksien takia. Salassapitoajasta tulisi sotilastiedustelun kohdalla säätää vastaavasti kuin siviilitiedusteluviranomaisen eli suojelupolisin kohdalla. Salassapitoaika olisi molempien kohdalla 60 vuotta. Suojelupoliisi ja sotilastiedusteluviranomainen toimivat myös yhteistyössä.

3 Tavoitteet

Esityksen tavoitteena on päivittää vuonna 2019 uutena voimaan tullutta siviilitiedustelulainsäädäntöä hallitusohjelmakirjausten ja käytännön soveltamistoiminnassa havaittujen tarpeiden mukaisesti. Esityksen tavoitteena on mahdollistaa ja turvata suojelupoliisin tarkoituksenmukainen ja tehokas toiminta sekä kansallisesti että kansainvälisesti.

Tavoitteena on ylläpitää ja parantaa kansallista turvallisuutta, kun siviilitiedustelun kohteista saataisiin entistä tarkemmin ja kohdennetummin tietoa, ja kun analysoitua tietoa pystyttäisiin aiempaa paremmin jakamaan sitä tarvitseville. Keskeinen tavoite on vieraista valtiollisista toimijoista tiedon hankkiminen entistä tehokkaammin. Lisäksi esitys parantaa tietoliikennetiedustelun osalta yksityisen viestin salaisuuden suojaa parantamalla samalla kuitenkin siviilitiedustelun tiedonhankintaa.

Tavoitteena on lisäksi mahdollistaa Rajavartiolaitokselle suojelupoliisin tukeminen tietyissä rajatuissa tilanteissa.

Esityksen tavoitteena on myös pidentää eräiden julkisuuslaissa salassa pidettäväksi säädettyjen asiakirjojen salassapitoaikaa. Tavoitteena on sitä kautta turvata Suomen kansainvälisiä suhteita, kansallista turvallisuutta ja maanpuolustusta.

4 Ehdotukset ja niiden vaikutukset

4.1 Keskeiset ehdotukset

4.1.1 Siviilitiedustelu

Tässä esityksessä ehdotetaan säädettäväksi keskeisesti kolmesta uudesta toimivaltuudesta siviilitiedusteluun: valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta, yksinomaan tietoverkossa toteutettavasta peitetoiminnasta sekä Suomen rajojen ulkopuolella sijaitsevan laitteen ja tietojärjestelmän toimintaan puuttumisesta.

Valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu

Poliisilain 5 a luvussa säädettäisiin uudesta tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla voitaisiin hankkia tietoteknisin menetelmin tietoa kansallista turvallisuutta vakavasti uhkaavaan toimintaan hyödynnettävän tietojärjestelmän toiminnasta, sen sisältämistä tiedoista, tietojärjestelmän osien välillä liikkuvista viesteistä sekä tietojärjestelmään saapuvista tai siitä lähtevistä viesteistä.

Tietojärjestelmällä tarkoitettaisiin tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoa käsittelevistä ohjelmista ja tietojen käsittelysäännöistä muodostuvaa kokonaisuutta. Tietojärjestelmä voi muodostua useiden eri laitteiden ja ohjelmistojen tai näiden osien muodostamasta maantieteellisesti ja loogisesti hajautetusta kokonaisuudesta. Tietojärjestelmä voi kattaa osia, jotka kuuluvat samanaikaisesti johonkin toiseen tietojärjestelmään. Tietojärjestelmätiedustelu kohdistuisi toistensa kanssa tietyssä kansallista turvallisuutta uhkaavassa tarkoituksessa kommunikoivien laitteiden ja virtuaalisten järjestelmien muodostamaan loogiseen kokonaisuuteen, jolloin lupaa ei edellytettäisi vaadittavan erikseen jokaiseen sellaiseen laitteeseen, joka kuuluu kokonaisuuteen.

Tietojärjestelmätiedustelulla tietoa voisi hankkia joko kokonaisesta tietojärjestelmästä tai jostain tietojärjestelmän sellaisesta loogisesta tai fyysisestä osasta, joka toteuttaa tietojärjestelmän jotakin toiminnallisuutta tai joka muutoin voidaan määrittää tietojärjestelmässä omaksi osakseen perustuen tietojärjestelmän käyttäjään tai tietojärjestelmän osan perustellusti oletettuun tietosisältöön.

Tietojärjestelmätiedustelun voidaan kokonaisuutena katsoa kattavan voimassa olevista toimivaltuuksista muun muassa telekuuntelun ja teknisen laitetarkkailun. Tämän takia päätöksentekijänä olisi oltava tuomioistuin. Tuomioistuimen myöntämän luvan tulisi koskea tietojärjestelmää, jolloin yksittäisen teleosoitteen, tiedonkäsittelylaitteen, tiedonsiirtolaitteen tai tietoa käsittelevän ohjelman ja tietojen käsittelysäännön kuulumisesta kohteena olevaan tietojärjestelmään päättäisi erityisesti tiedustelumenetelmien käyttöön perehtynyt muu virkamies. Päätösten tulisi olla perusteltuja ja niihin tulisi kohdistaa laillisuusvalvontaa.

Tietojärjestelmätiedustelua koskevassa vaatimuksessa ja päätöksessä olisi tehtävä muiden seikkojen ohella selkoa toimenpiteen kohteena olevan tietojärjestelmän rajauksesta perustuen kuvaukseen tietojärjestelmän toiminnasta, sen tietojenkäsittelysäännöistä, siihen kuuluvien

laitteiden tai ohjelmien tunnisteista, sen käyttämistä teleosoitteista, sen käyttäjien teleosoitteista tai muista käyttäjätiedoista tai jostakin näiden yhdistelmistä siten, että tiedon hankinta voidaan kuvauksen perusteella teknisesti rajata.

Laissa säädetyt kuuntelukiellot ulotettaisiin koskemaan myös tietojärjestelmätiedustelua vastaavalla tavalla kuin ne nykytilassa koskevat telekuuntelua ja sen sijasta tapahtuvaa tietojen hankkimista, teknistä kuuntelua ja teknistä laitetarkkailua.

Puuttuminen Suomen rajojen ulkopuolella sijaitsevan laitteen ja tietojärjestelmän toimintaan

Poliisilaissa säädettäisiin toimivaltuudesta puuttua Suomen rajojen ulkopuolella sijaitsevan laitteen ja tietojärjestelmän toimintaan, jota käytetään Suomen kansallista turvallisuutta vakavasti vaarantavaan toimintaan. Tietojärjestelmien ja -verkkojen globaali levinneisyys muodostaa uudenlaisen haasteen kansallisen turvallisuuden uhkien torjumiselle. Kyberuhkatoimijat sekä muut kansallista turvallisuutta uhkaavat toimijat, jotka toiminnassaan hyödyntävät tietoverkkoja ja -järjestelmiä, toimivat pääsääntöisesti ulkomailla, mutta voivat tietoverkkoja pitkin vaikuttaa ja vakoilla Suomen alueella ja Suomen kansalaisten ja organisaatioiden käyttämissä tietojärjestelmissä.

Teknisen laitetarkkailun kohdistaminen myös henkilöön

Poliisilain 5 a luvun 14 §:ää täydennettäisiin siten, että teknistä laitetarkkailua voitaisiin kohdistaa tuomioistuimen päätöksellä yksittäisen laitteen tai laitteen sisältämän ohjelmiston lisäksi myös laitetta tai ohjelmistoa käyttävään henkilöön, jolloin tarkkailu ei keskeytyisi laitteiden tai ohjelmistojen vaihtamisen takia.

Tietoliikennetiedustelu

Tietoliikennetiedustelusta siviilitiedustelussa annettua lakia muutettaisiin siten, että tietoliikennetiedustelun käytön matalampaa edellytyskynnystä voitaisiin soveltaa tilanteissa, joissa tietoliikennetiedustelun tarkoituksena on kerätä vieraan valtiollisen toimijan tai siihen rinnastuvan toimijan tietoliikennettä.

Tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa säädettäisiin tietoliikennetiedustelusta hakuehtojen määrittämiseksi. Hakuehtojen määrittämisestä tietoliikenteen virrasta kohteena olevan tahoon liittyvien tietoliikenteen säännönmukaisuuksien ja ominaispiirteiden avulla pyrittäisiin löytämään tietoja, joita voidaan käyttää edelleen varsinaisessa tietoliikennetiedustelussa hakuehtona. Laissa säädetty hakuehdon määritelmä ohjaa siihen, että hakuehtojen olisi rajattava tiedon määrä välttämättömään.

Hakuehtojen määrittämisessä ei saisi käsitellä viestin merkityssisällössä olevia tietoja. Käytäntö on osoittanut, että sähköisen viestinnän teknisiksi tiedoiksi katsottavat tiedot eivät pysty kaikissa tilanteissa rajaamaan tietomassaa tarkoitetulla tavalla, vaan järjestelmään tullutta tietoa olisi voitu rajata esimerkiksi tiettyä erityistä sisällössä olevaa sanaa käyttämällä. Toisaalta tietoliikenteen tekninen tieto, kuten puhelinnumero, voi olla myös viestin sisällössä.

Tietoliikennetiedustelusta poistettaisiin myös kielto käyttää Suomessa olevaa tai oletettavasti olevaa telepäätelaitetta tai -osoitetta hakuehtona. Tiedustelun kohteena oleva toimija saattaa saapua tietoliikennetiedustelun käytössä olon aikana Suomeen, ja tahoa olisi välttämätöntä pystyä seuraamaan, kunnes kohdennetumpia tiedustelumenetelmiä päästään käyttämään.

Tietoliikennetiedustelun ilmoittamisesta luopuminen

Tietoliikenteeseen kohdistuvasta tiedustelusta ilmoittamisvelvollisuudesta luovuttaisiin. Kohteeksi itsensä epäilevä voi edelleen pyytää tiedusteluvalvontavaltuutettua tarkastamaan, onko henkilö joutunut tiedustelumenetelmän kohteeksi ja onko asiassa menetelty lainmukaisesti.

Suojelupoliisi ja tehtävien tukeminen

Rajavartiolaitokselle ehdotetaan säädettäväksi toimivalta avustaa suojelupoliisia, joka on siviilitiedusteluviranomainen, tiettyjen tiedustelumenetelmien käytössä.

Muuta

Poliisilakiin ehdotetaan tehtäväksi muutoksia käytännön tiedustelutoiminnassa havaituista tarkennustarpeista, ja toisaalta muusta lainsäädännöstä johtuvia muutoksia.

Julkisuuslaki

Esityksessä ehdotetaan myös julkisuuslakiin muutoksia. Julkisuuslain 31 §:n 2 momenttiin ehdotetaan otettavaksi säännökset asiakirjojen salassapitoajan pidentämisestä eräissä tilanteissa niin, että salassapitoaika olisi 40 vuotta yleisen 25 vuoden salassapitoajan asemasta julkisuuslain 24 §:n 1 momentin 1 kohdassa tarkoitetuissa tapauksissa ja 2 kohdassa tarkoitetuissa tapauksissa siltä osin, kun kyse on ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjoista, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, sekä 60 vuotta julkisuuslain 24 §:n 1 momentin 9 ja 10 kohdassa tarkoitetuissa eräissä tapauksissa. Valtion turvallisuuden ylläpitämiseksi 24 §:n 1 momentin 9 kohdassa säädetyn suojelupoliisin ja sisäministeriön asiakirjan salassapitoaika olisi 60 vuotta. Salassa pidettäväksi 24 §:n 1 momentin 10 kohdassa säädetyn sotilastiedustelua koskevan asiakirjan salassapitoaika olisi myös 60 vuotta.

4.2 Pääasialliset vaikutukset

4.2.1 Taloudelliset vaikutukset

Ehdotetuilla muutoksilla ei ole merkittäviä taloudellisia vaikutuksia voimassa olevaan valtion talouden kehyksiin. Lähtökohtaisesti viranomaiset toimivat päätettyjen taloudellisten kehysten puitteissa. Määrärahatarpeita käsitellään julkisen talouden suunnitelmassa ja vuosittaisissa talousarvioprosesseissa.

Suojelupoliisille lisättiin kehyspäätöksessä 2025 määrärahoja 9,8 milj. eurolla vuodesta 2026 eteenpäin. Lisäys mahdollistaa suojelupoliisin nykyisen toiminnan turvaamisen ja ennakoivan strategisen suorituskyvyn kehittämisen tulevaisuudessa.

Esitetyillä muutoksilla arvioidaan olevan kuitenkin jonkin verran taloudellisia vaikutuksia kehysten puitteissa. Esitettyjen muutosten arvioidaan tehostavan suojelupoliisin resurssien käyttöä, kun esimerkiksi tietoliikennetiedustelua voitaisiin toteuttaa entistä tarkemmin kohdistamalla sitä tarkoituksenmukaisemmin. Toisaalta suojelupoliisille säädettäväksi esitetty uusi toimivaltuus tietojärjestelmän käytön estämiseksi tai sen toiminnan haittaamiseksi edellyttää henkilötyövuosien kohdentamista tähän toimintaan. Taloudellisia vaikutuksia voi olla myös mahdollisilla järjestelmäinvestoinneilla tai sillä, että laajennetaan korvaukseen oikeutettujen tahojen joukko yhdenmukaiseksi siviilitiedustelussa avustamisvelvollisten tahojen kanssa.

Esitys aiheuttaa tarvetta kouluttaa suojelupoliisin ja Rajavartiolaitoksen virkamiehiä. Jo nykyisellään kouluttaminen on suojelupoliisissa osa normaalia toimintaa, eikä esityksestä aiheudu tämän takia mainittavia taloudellisia vaikutuksia.

Esityksessä ehdotettu avustamisvelvollisuuden laajennus teleyrityksistä viestinnän välittäjiin voi aiheuttaa uusia kustannuksia. Kustannusten määrä riippuu toimivaltuuden käytön laajuudesta.

4.2.2 Muut ihmisiin kohdistuvat ja yhteiskunnalliset vaikutukset

4.2.2.1 Perus- ja ihmisoikeudet

Siviilitiedustelulainsäädännön vaikutuksia perus- ja ihmisoikeuksiin on arvioitu laajemmin poliisilain 5 a luvun ja tietoliikennetiedustelusta siviilitiedustelussa säätämiseen johtaneessa hallituksen esityksessä (HE 202/2017 vp). Ehdotetut muutokset ovat merkityksellisiä usean perusoikeuden kannalta. Näitä ovat yhdenvertaisuus (PL 6 §), oikeus elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen (PL 7 §), yksityiselämän suoja (PL 10§), sananvapaus ja julkisuus (PL 12 §), omaisuuden suoja (PL 15 §), oikeus työhön ja elinkeinovapaus (PL 18 §) sekä oikeusturva (PL 21 §).

Ehdotetuilla muutoksilla olisi lähtökohtaisesti myönteisiä vaikutuksia perustuslain 7 §:n mukaiseen oikeuteen elämään sekä henkilökohtaiseen vapauteen ja koskemattomuuteen, sillä suojelupoliisin toiminnan turvaamiselle muuttuvassa turvallisuus- ja teknologiaympäristössä pystyttäisiin suojaamaan paremmin Suomen kansallista turvallisuutta ja yhteiskunnan turvallisuutta sekä niiden alaan kuuluvia suojattavia oikeushyviä.

Ehdotetuilla muutoksilla, erityisesti tietoliikennetiedustelun hakuehtojen määrittämisellä, sisällöllisten hakuehtojen kiellon poistamisella ja ilmoitusvelvollisuudesta luopumisella on merkitystä yksityiselämän suojan kannalta. Hakuehtojen määrittämisellä voidaan katsoa osaltaan parantavan yksityisyyden suojaa tietoliikennetiedustelun tarkemman kohdentumisen myötä.

Ehdotetulla laitteen, menetelmän tai ohjelmiston asentamisella ja poisottamisella on vaikutusta perustuslaissa turvattuun omaisuuden suojaan. Lakiehdotuksen mukaan suojelupoliisi voisi käyttää myös sivullisten laitteita tai tietojärjestelmiä, jos se olisi välttämätöntä menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi. Yksittäisen toimenpiteen ei arvioida puuttuvan merkittävästi omaisuuden suojaan, sillä toimenpiteen keston voidaan katsoa olevan varsin vähäinen. Suojelupoliisin on pyrittävä peittämään jälkensä mahdollisimman hyvin, ettei toiminnan mahdollinen paljastuminen aiheuta haittaa sivullisen laitteelle tai tietojärjestelmälle. Ulkopuolinen henkilö voisi suojelupoliisin pyynnöstä ja valvonnassa toteuttaa toimenpiteitä. Tämä tarkoittaa myös sitä, että toiminta ei saisi aiheuttaa vähäistä suurempaa vahinkoa kyseiselle henkilölle tai toiminnalle. Vähäisyydellä tarkoitettaisiin lähinnä tietoliikenneyhteyden hetkellistä hidastumista.

Ehdotetuilla muutoksilla on siten liittymäpintaa oikeusturvan toteutumiseen, mutta ehdotetun muutoksen ei katsota heikentävän oikeutta oikeusturvaan. Esityksessä ei ehdoteta muutoksia tiedustelutoiminnan valvonnasta annettuun lakiin eli henkilöt voivat edelleen tehdä joko lain 12 §:n mukaisen tutkimispyynnön tai lain 11 §:n mukaisen kantelun riippumatta siitä, onko henkilö saanut ilmoituksen vai ei. Toimintaa valvotaan suojelupoliisin sisäisen valvonnan lisäksi hallinnonalalla sisäministeriön toimesta ja ulkoisesti eduskunnan tiedusteluvalvontavaliokunnan, eduskunnan oikeusasiamiehen ja tiedusteluvalvontavaltuutetun toimesta. Tiedusteluvalvontavaltuutetun valvonta tapahtuu etukäteen, reaaliaikaisesti ja jälkikäteisesti, jolloin valvonnassa pystytään kiinnittämään huomiota toimintaan myös yksityisten henkilöiden näkökulmasta.

Lisäksi ilmoitusvelvollisuuden piirissä olevien tiedustelumenetelmien käytöstä päättää tuomioistuin, joka ottaa tarvittavat näkökohdat huomioon päätöstä tehdessään. Myös tietosuojavaltuutettu kohdistaa valvontaa suojelupoliisiin.

Henkilöllä, joka kokee joutuneensa tiedustelumenetelmän käytön kohteeksi tai epäilee suojelupoliisin toiminnan lainmukaisuutta, voi myös tehdä edelleen kantelun oikeusasiamiehelle ja viime kädessä nostaa kanteen EIT:ssä.

Ehdotetuilla muutoksilla on vaikutusta perustuslaissa turvattuun julkisuusperiaatteen toteutumiseen. Julkisuuslain osalta ehdotettu salassapitoajan pidentäminen vaikuttaa kansalaisten mahdollisuuksiin saada tietoja eräiden viranomaisten ja tasavallan presidentin toiminnasta ja yhteiskuntaoloista. Julkisuuslain salassapitoajan pidentäminen 25 vuodesta 40 vuoteen ulkoasiainhallinnon, TP_UTVA:n, tasavallan presidentin ja tasavallan presidentin kanslian kohdalla ja 60 vuoteen sisäministeriön, suojelupoliisin ja sotilastiedustelun kohdalla rajoittaa siten perustuslain 12 §:n 2 momentissa säädettyä kansalaisten oikeutta saada tietoa. Toisaalta sääntelyn taustalla vaikuttaa painava yhteiskunnallinen intressi, joka edellyttää julkisuusperiaatteesta rajattua poikkeamista.

4.2.2.2 Vaikutukset viranomaisiin

Ehdotetulla sääntelyllä ei ole vaikutusta viranomaisten keskinäisiin toimivaltasuhteisiin, vaikka viranomaisten yhteistyömahdollisuuksia lisätään. Rajavartiolaitokselle ehdotetaan säädettäväksi uusi tehtävä, siviilitiedusteluun osallistuminen. Rajavartiolaitokselle säädettäisiin mahdollisuus tukea suojelupoliisia suorittamalla tiettyihin tiedustelumenetelmiin liittyviä yksittäisiä toimenpiteitä suojelupoliisin pyynnöstä. Suojelupoliisi toimii siviilitiedusteluviranomaisena, jonka vastuuta ei siirrettäisi Rajavartiolaitokselle, mutta jota Rajavartiolaitos voi tukea. Rajavartiolaitokselle säädettävän uuden tehtävän arvioidaan vaikuttavan vähäisessä määrin henkilöstön työmääriin, koska toimenpiteitä suoritettaisiin Rajavartiolaitoksen muiden lakisääteisten tehtävien yhteydessä. Uudet toimivaltuudet edellyttävät Rajavartiolaitoksen henkilöstön täydennyskoulutusta. Rajavartiolaitoksen osallistumisesta tiedusteluun ei arvioida aiheutuvan merkittäviä taloudellisia vaikutuksia.

Tietoliikennetiedustelun teknistä toteuttamista koskevan sääntelyn tarkentamisella mahdollistettaisiin suojelupoliisin osallistuminen teknisten tietojen käsittelyyn Puolustusvoimien tiedustelulaitoksen rinnalla ja apuna. Ratkaisulla tuetaan molempien osapuolten osallistumisen toimenpiteiden suorittamiseen siltä osin kuin se on niiden yhteisten etujen mukaista ja palvelee niiden tietoliikennetiedustelun kohdistamista.

Tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa säädetyt hävittämisvelvollisuudet jäisivät kuitenkin yhä voimaan, vaikka tallenteiden ja asiakirjojen tarkastamisvelvollisuus poistettaisiin. Tarkastamisvelvollisuuden poistaminen merkitsisi sitä, että suojelupoliisilla ei olisi proaktiivista velvollisuutta käydä dataa läpi pelkästään etsiäkseen siitä hävittämisvelvollisuuden piiriin kuuluvat tiedot. Suurista datamääristä johtuen tällaisen velvollisuuden täyttäminen on käytännössä erittäin haastavaa.

Julkisuuslain kohdalla ehdotettu lakimuutos salassapitoajan pidentämisestä 25 vuodesta 40 vuoteen turvaisi ulkoministeriön, TP UTVA:n sekä tasavallan presidentin ja tasavallan presidentin kanslian asiakirjojen välttämättömän salassapidon. 25 vuoden salassapitoaika on liian lyhyt ottaen huomioon, että asiakirjoista voi päätellä Suomea koskevia haavoittuvuuksia. Pidempi salassapitoaika suojaisi siten ulkoministeriön, TP UTVA:n ja tasavallan presidentin sekä tasavallan presidentin kanslian toimintaedellytyksiä. Pidennetty salassapitoaika turvaisi myös Suomen diplomaattien toimintaedellytyksiä Suomen ulkomaanedustustoissa.

Sisäministeriön kohdalla julkisuuslain muutos tarkoittaisi mahdollisuutta salata kansalliseen turvallisuuteen (valtioturvallisuuteen) liittyviä asiakirjoja nykyistä pidemmän aikaa. Suojelupoliisin osalta julkisuuslain muutos tarkoittaisi nykytilan eli valtioneuvoston päätöksellä järjestyn asian saattamista lain tasolle, ja salassapitoaika pidentyisi voimassa olevan valtioneuvoston päätöksen mukaisesta ajasta aikaisemman päätöksen mukaiseen 60 vuoteen. Sotilastiedustelun kohdalla esitys tarkoittaisi kokonaisvaltaisempaa lähestymistapaa salassapitoon yksittäisten päätösten sijasta. Pidempi salassapitoaika suojaisi viranomaisten toimintaedellytyksiä Suomessa ja kansainvälisissä yhteyksissä.

4.2.2.3 Kansallinen turvallisuus

Suojelupoliisin ennakkovaroittaminen ja tiedustelukyvyn turvaaminen antavat mahdollisuuden saada ajoissa tieto Suomeen kohdistuvista vakavista kansallisen turvallisuuden uhista, jotta niihin voidaan varautua ja estää niitä toteutumasta. Tätä tukisi myös Rajavartiolaitoksen mahdollisuus tukea suojelupoliisia.

Kansalliseen turvallisuuteen vaikuttavat kansallisen toimintaympäristön lisäksi Suomen lähiympäristöön ja kansainvälisiin kehityskulkuihin liittyvät tekijät. Turvallisuusympäristön muutoksen myötä kansallista turvallisuutta kohtaan on syntynyt uusia vakavia uhkia. Tärkein suojattava etu on valtion itsemääräämisoikeus. Kansallisen turvallisuuden kannalta keskeisiä ovat sellaiset yhteiskunnan elintärkeät toiminnot, joiden häirintä tai lamauttaminen saattaisi viime kädessä johtaa ihmisten turvallisuuden tai terveyden vakavaan vaarantumiseen. Ehdotetulla sääntelyllä voitaisiin puuttua toimintaan, jolla yritetään vaikuttaa ylimpien valtioelinten ja viranomaisten sekä yhteiskunnan perustoiminnoista huolehtivien tahojen mahdollisuuksiin hoitaa tehtäviään ilman ulkoista häirintää. Erityisesti suojelupoliisin valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun toimivaltuudessa kyse olisi siitä, että kyky torjua erityisesti valtiollisten kyberuhkatoimijoiden kansalliselle turvallisuudelle aiheuttamaa haitallista toimintaa paranisi. Ehdotetut muutokset mahdollistaisivat suojelupoliisille tietojärjestelmien toiminnan ennakoivamman tiedustelun ja uhkien tunnistamisen. Ne mahdollistaisivat sen, että suojelupoliisi pystyisi tunnistetuissa tietojärjestelmissä etsimään hankittavaa tietoa sekä tunnistamaan uusia tietojärjestelmiä, jotka muodostavat uhkan kansalliselle turvallisuudelle.

Ulko- ja turvallisuuspoliittisten vaikutusten arviointi

Uusi toimivaltuus Suomen rajan ulkopuolella olevan tietojärjestelmän toiminnan haittaamiseen edellyttää uudentyyppisiä päätöksentekoprosesseja. Toimenpiteellä voi olla sen luonteen mukaan ulko- ja turvallisuuspoliittisia vaikutuksia.

Jo nykyisellään poliisilain 5 a luvun 58 §:n mukaan siviili- ja sotilastiedustelutoiminta sovitetaan yhteen tasavallan presidentin, valtioneuvoston kanslian, ulkoministeriön, puolustusministeriön ja sisäministeriön sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken. Jos siviilitiedustelutoiminnalla arvioidaan olevan ulko- ja turvallisuuspoliittisia vaikutuksia, asia on valmistelevasti käsiteltävä edellä tarkoitettujen viranomaisten kesken.

Huomattavasti merkittävämmissä tapauksissa ulko- ja turvallisuuspoliittisesti merkittäviä toimenpiteitä voidaan valmistelevasti käsitellä tasavallan presidentin ja ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteisessä kokouksessa. Uudentyyppinen toiminta kuitenkin edellyttänee kokoonpanon tarkastelemista tarkoituksenmukaisella tavalla tai uuden kokoonpanon muodostamista siltä osin kuin on kyse vaikuttamistoiminnasta.

Myös tietolähteen rajanylityksessä avustamisella voi olla vaikutuksia Suomen kansainvälisiin suhteisiin etenkin, jos tietolähde on ollut lähtömaansa yhteiskunnassa korkeassa asemassa.

4.2.2.4 Tietoyhteiskunta ja tietosuoja

Esitys mahdollistaa suojelupoliisille entistä paremmin tiedon hankinnan kybertoimintaympäristössä kansallisen turvallisuuden suojaamiseksi. Kyky hankkia tietoa ja puuttua entistä paremmin valtiollisen toimijan toimintaan on erityisen merkityksellinen. Tämä edistää suoraan tai välillisesti kansalaisille, yrityksille ja viranomaisille tärkeiden viestintäinfrastruktuurien ja viestintäpalveluiden turvallisuutta, toimintavarmuutta sekä luotettavuutta. Useat kriittiset toiminnot, kuten energia, toimivat viestintäinfrastruktuurin ja viestintä- tai digitaalisten palvelujen varassa.

Parantuneella tiedonhankintakyvyllä on vaikutusta verkkojen ja palvelujen tietosuojaan, tietoturvaan sekä yleiseen yhteiskunnalliseen luottamukseen ja kansalliseen turvallisuuteen.

4.2.2.5 Yhdenvertaisuus ja sukupuolten tasa-arvo

Esitetyillä muutoksilla ei arvioida olevan vaikutuksia yhdenvertaisuuden ja sukupuolten tasa-arvon kannalta.

Tiedustelutoimivaltuuksien käyttämisessä on noudatettava poliisilain 1 luvussa säädettyjä perusoikeuksien ja ihmisoikeuksien kunnioittamisen vaatimusta, suhteellisuusperiaatetta, vähimmän haitan periaatetta ja tarkoitussidonnaisuuden periaatetta. Tietoliikennetiedustelusta siviilitiedustelussa annetun lain 1 §:n 3 momentissa säädetään syrjivän tiedustelutoiminnan kiellosta.

4.2.3 Julkisuuslain muutoksen vaikutukset kansainvälisille suhteille ja yhteiskunnalliset vaikutukset sekä kansallinen turvallisuus

Muuttuneessa turvallisuusympäristössä julkisen viranomaistiedon epäasiallisen hyödyntämisen riskit ovat kasvaneet. Ulkopolitiikan ydinalueeseen kuuluvien asiakirjojen julkiseksi tulemiseen liittyy mahdollisuus käyttää niitä väärin sellaisiin tarkoituksiin, jotka ovat omiaan vaikeuttamaan Suomen suhteita ulkovaltoihin, ja vaarantamaan Suomen etuja tai heikentämään ulkoasiainhallinnon sekä tasavallan presidentin ja tasavallan presidentin kanslian toimintaedellytyksiä. Tietojen vaihtamisen edellytyksenä on molemminpuolinen luottamus. Epäilys siitä, että Suomi nykyisen lainsäädäntönsä takia olisi pakotettu luovuttamaan luottamukselliseksi tarkoitettua tietoa julkisuuteen, vaikuttaisi valtioiden ja kansainvälisten järjestöjen halukkuuteen luovuttaa Suomelle tietoa. Tämä puolestaan heikentäisi Suomen edellytyksiä toimia kansainvälisessä yhteistyössä. Salassapitoajan pidentämisellä voidaan siten nähdä olevan myönteisiä vaikutuksia Suomen kansainvälisille suhteille sekä Suomen valtion maineen ja edun kannalta.

Suojelupoliisin ja sotilastiedustelun viranomaistietoon liittyy salassapito-olettama. Riittävän pitkä salassapitoaika on keskeistä kansallisen turvallisuuden (valtioturvallisuuden) ja maanpuolustukseen liittyvien tietojen väärinkäytön estämiseksi. Tietojen oikeudettomalla tai liian varhaisella julkiseksi tulemisella voi olla haitallisia vaikutuksia toimintaan ja kansainväliseen yhteistyöhön ja laajemminkin ulko- ja turvallisuuspoliittista merkitystä.

Esityksellä voidaan kokonaisuutena arvioiden olevan myönteisiä vaikutuksia Suomen kansallisen turvallisuuden suojaamisen kannalta.

5 Muut toteuttamisvaihtoehdot

5.1 Vaihtoehdot ja niiden vaikutukset

Esityksen valmistelussa keskeisenä tavoitteena on ollut sääntelyn ajantasaistaminen ja parantaminen käytännön soveltamisessa muutostarpeista tehtyjen havaintojen perusteella teknologinen kehitys ja turvallisuusympäristön vaikeutuminen huomioon ottaen.

Pääasiallisena vaihtoehtona esitettäville muutoksille on sääntelyn säilyttäminen voimassa olevien lakien mukaisina, mitä ei voida pitää tarkoituksenmukaisena. Nykytilan säilyttämisen myötä voimassa olevassa lainsäädännössä havaitut ongelmakohdat säilyisivät ennallaan, eivätkä mahdollisuudet suojautua kansalliseen turvallisuuteen kohdistuvilta vakavilta uhkilta parantuisi.

Suojelupoliisilla ei olisi mahdollisuutta toteuttaa lakisääteisiä tehtäviänsä siviilitiedusteluviranomaisena mahdollisimman tehokkaasti nykyisessä turvallisuustilanteessa voimassa olevan lainsäädännön rajoitteiden vuoksi. Ehdotettujen muutosten jättäminen tekemättä heikentäisi suojelupoliisin kykyä toimia vallitsevassa turvallisuusympäristössä, jossa muut toimijat jatkuvasti kehittävät omia kyvykkyyksiään. Tämä voisi osaltaan vaarantaa siviilitiedustelun tarkoituksen eli tiedon hankinnan ja tiedon hyödyntämisen kansallisen turvallisuuden suojaamiseksi, tiedon tuottamisen ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten.

Julkisuuslaki

Valmistelun aikana on pohdittu eri vaihtoehtoja. Julkisuuslain 24 §:n 1 momentin 1 ja 2 kohtaan liittyen salassapitoajan osalta valmistelussa oli esillä yhtäältä vaihtoehto pidemmästä salassapitoajasta, eli 50 tai 60 vuotta, ja toisaalta pohdittiin myös nyt ehdotettua 40 vuotta lyhyempää salassapitoaikaa eli 30 vuotta. Valmistelussa parhaaksi vaihtoehdoksi katsottiin 40 vuotta, sillä salassapitoaika on yhtäältä oltava riittävän pitkä, mutta toisaalta julkisuutta ei saa rajoittaa enempää kuin on välttämätöntä.

Toiseksi valmistelussa tunnistettiin vaihtoehto, että salassapitoaikaa olisi mahdollista jatkaa valtioneuvoston päätöksellä julkisuuslain 31 §:n 4 momentin nojalla säädettyjen edellytysten täyttyessä. Valtioneuvosto on tehnyt joitakin päätöksiä salassapitoajan jatkamisesta tiettyjen asiakirjojen osalta. Julkisuuslain muuttamista koskevan lain esitöissä on kuitenkin todettu, että salassapitoajan pidentäminen valtioneuvoston päätöksellä on tarkoitettu poikkeukselliseksi toimenpiteeksi eikä siihen turvautumista voida pitää asianmukaisena silloin, kun kysymys on säännönmukaisesta ja ennakoitavissa olevasta salassapitotarpeesta (HE 20/2005 vp, s. 14). Julkisuuslain 24 §:n 1 momentin 1 kohdan asiakirjojen kohdalla samoin kuin 2 kohdan asiakirjojen kohdalla siltä osin, kun kyse on ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevista asiakirjoista, voidaan katsoa olevan kyse säännönmukaisesta ja ennakoitavissa olevasta salassapitotarpeesta. Näistä syistä yksittäisten valtioneuvoston päätösten tekemistä salassapitoajan pidentämisestä ei voida pitää tarkoituksenmukaisimpana vaihtoehtona. Kokonaisuutena arvioiden myös suojelupoliisia koskeva valtioneuvoston päätös tulisi saattaa lain tasolle. Vastaava tarve salassapitoajan säätämisestä lain tasolla on sisäministeriön ja sotilastiedustelun kohdalla.

Valmistelun aikana tunnistettiin myös, että yksi vaihtoehto olisi muuttaa julkisuuslain 24 §:n 1 momentin 1 kohdan sisältöä. Tätä ei kuitenkaan pidetty tarkoituksenmukaisena, sillä julkisuuslain kokonaisuudistuksesta on oikeusministeriössä vireillä erillinen säädöshanke, jonka yhteydessä tarkastellaan salassapitoperusteita kokonaisuutena (ks. Hankeikkunassa hanke

https://valtioneuvosto.fi/hanke?tunnus=OM083:00/2020. Oikeusministeriö on saanut hankkeen puitteissa lausunnot salassapitoperusteiden muutosehdotuksista. Nyt esitetty pidennys olisi välttämätön ja toimiva ratkaisu sekä nykyisessä että tulevaisuudessa mahdollisesti muutetun 1 kohdan soveltamisessa.

5.2 Ulkomaiden lainsäädäntö ja muut ulkomailla käytetyt keinot

5.2.1 Euroopan ihmisoikeussopimus

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

EIT:n tiedustelutoimintaa koskevasta keskeistä ratkaisukäytäntöä on arvioitu hallituksen esityksessä eduskunnalle siviilitiedustelulainsäädännöksi (HE 202/2017 vp.) ja hallituksen esityksessä eduskunnalle laiksi sotilastiedustelusta (HE 203/2017 vp.). Seuraavassa EIT:n käytäntöä käsitellään keskittyen ennen kaikkea uudempaan EIT:n ratkaisukäytäntöön.

Yksityiselämän suoja (EIS 8 artikla)

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

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

Viranomaisen ei tarvitse tosiasiassa käsitellä tietoja, jotta kyse olisi yksityiselämään puuttumisesta, vaan puuttumiseksi on katsottava jo se, että viranomainen kerää ja tallentaa niitä myöhempää käyttöä varten (Marper v. Yhdistynyt Kuningaskunta). Pelkkä sellaisen lainsäädännön olemassaolokin, joka mahdollistaa viestintäyhteyksien salaisen tarkkailun, puuttuu viestinnän osapuolten ja myös potentiaalisten osapuolten EIS 8 artiklan takaamiin oikeuksiin (Klass v.

Saksa, Liberty ja muut v. Yhdistynyt Kuningaskunta). Valvonnan potentiaalisilla kohteilla on tällöin oltava oikeus EIS 13 artiklan takaamaan tehokkaaseen oikeussuojakeinoon kansallisen viranomaisen edessä. EIS 13 artiklan mukaan jokaisella, jonka yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt.

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

Siitä, että sekä viestinnän sisältö että viestinnän tunnistamistiedot nauttivat EIS 8 artiklan mukaista suojaa, ei seuraa, että viranomaiset eivät niihin voisi puuttua. Yksityiselämään puuttuminen voi olla verrattain laajamittaistakin, kun se tapahtuu EIS 8 artiklan edellyttämissä puitteissa. EIS 8 artikla asettaa kolme ehtoa sille, että artiklan takaamiin oikeuksiin voidaan viranomaistoiminnassa puuttua: 1) puuttumisen on oltava kansallisen lain sallimaa, 2) sen on tapahduttava tiettyjen artiklassa erikseen lueteltujen etujen turvaksi ja 3) puuttumisen on oltava demokraattisessa yhteiskunnassa välttämätön. Yksi yksityiselämän ja siten myös luottamuksellisen viestinnän suojaan puuttumisen mahdollistavista eduista on kansallinen turvallisuus.

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

EIT on ratkaisuissaan toistuvasti korostanut sitä, että yksityiselämän suojaan puuttuvan, salaiset viranomaistoimenpiteet mahdollistavan lain on oltava oikeusvaltioperiaatteiden mukainen, kansalaisten saatavilla sekä laadultaan sellainen, että kansalaiset kykenevät ennakoimaan sen soveltamisen seuraukset omalta osaltaan (mm. Kruslin v. Ranska, Huvig v. Ranska, Lambert v. Ranska).

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

Edellä kuvattuja tapauksia voidaan pitää EIT:n ratkaisukäytännön perustavina tapauksina, joihin vedotaan ja joita kehitetään EIT:n uudemmassa käytännössä. EIT:n uudemmasta

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

Tapauksessa Big Brother Watch ja muut v. Yhdistynyt kuningaskunta EIT tutki Yhdistyneen kuningaskunnan signaalitiedustelujärjestelmää. EIT katsoi, että valtioilla on laaja harkintavalta päättää, millainen tiedustelujärjestelmä on tarpeen kansallisen turvallisuuden suojelemiseksi. Tiedustelujärjestelmä sinänsä ei rikkonut EIS:n artiklaa 8.

Tuomioistuin katsoi kuitenkin, että modernin viestintäteknologian muuttuvan luonteen vuoksi sen tavallinen lähestymistapa kohdennettuihin signaalitiedustelujärjestelmiin oli mukautettava kuvaamaan paremmin sen erityispiirteitä, joihin liittyi sekä riski väärinkäytöksistä että oikeutettu tarve toiminnan salassapidolle.

Erityisesti tällainen järjestelmä oli alistettava päästä päähän -suojatoimille, eli kansallisella tasolla oli tehtävä arviointi kunkin signaalitiedustelun tiedon hankinnan prosessin vaiheen osalta toimenpiteiden tarpeellisuudesta ja suhteellisuudesta. Lisäksi signaalitiedustelujärjestelmän käyttäminen oli alistettava riippumattomalle lupaharkinnalle, jossa on käytävä ilmi operaation kohde ja laajuus. Järjestelmän käytön on myös oltava valvonnan ja riippumattoman jälkikäteisen valvonnan alaisena.

Tuomioistuin määritteli näin ollen useita keskeisiä kriteereitä, jotka oli selkeästi määriteltävä kansallisessa laissa ennen kuin tällaisen järjestelmän voitiin katsoa olevan sopusoinnussa EIS:n vaatimusten kanssa. Soveltaen näitä uusia kriteereitä Yhdistyneen kuningaskunnan signaalitiedustelujärjestelmään, tuomioistuin totesi, että Yhdistyneen kuningaskunnan järjestelmässä oli kolme puutetta. Puutteet koskivat: 1) riippumattoman valtuutuksen puuttumista signaalitiedustelun luville, 2) signaalitiedustelussa käytettävät hakuehdot ja niiden luokat eivät käyneet ilmi lupahakemuksesta ja 3) henkilöä koskevat hakuehtoja ja -luokkia ei tarvinnut ilmoittaa lupahakemuksessa.

EIT totesi, että vaikka Yhdistyneessä Kuningaskunnassa sinänsä oli toiminnalle riippumaton ulkopuolinen valvoja ja oikeudellinen elin, jonka tarkoituksena on tutkia kansalaisten sille osoittamia valituksia, nämä eivät kuitenkaan olleet riittäviä. EIT katsoi, että Yhdistyneen Kuningaskunnan lainsäädäntö ei kokonaisuutena arvioiden kyennyt pitämään kansalaisten yksityisyyteen puuttumista siinä, mikä oli välttämätöntä demokraattisessa yhteiskunnassa. Näin ollen Yhdistyneen kuningaskunnan katsottiin rikkovan EIS:n 8 artiklaa.

Tapauksessa Centrum för Rättvisa v. Ruotsi kantajana oli ruotsalainen säätiö, jonka tehtävänä on suojella yksilöiden perusoikeuksia ja vapauksia. Kantajana oleva säätiö vetosi siihen, että sen viestintää on voitu siepata ja tutkia signaalitiedustelun avulla tai että näin voisi tapahtua tulevaisuudessa. Kantaja vetosi, että sen viestintä tapahtui päivittäin sähköpostitse, puhelimitse

ja faksilla henkilöiden ja yritysten kanssa Ruotsissa ja ulkomailla, usein arkaluonteisissa asioissa.

Suuri jaosto totesi viidentoista äänen enemmistöllä (kaksi vastaan), että oli tapahtunut ihmisoikeussopimuksen 8 artiklan loukkaus. Se totesi erityisesti, että vaikka Ruotsin laajamittaisen signaalitiedustelujärjestelmän keskeiset ominaisuudet täyttivät lain laadulle asetetut vaatimukset, järjestelmässä oli kuitenkin kolme puutetta: 1) ei ollut selvää sääntöä henkilötietoja sisältämättömän aineiston tuhoamisesta, 2) signaalitiedustelulaki tai muu asiaankuuluva lainsäädäntö ei edellyttänyt, että päätöstä tiedustelutiedon välittämisestä ulkomaisille kumppaneille tehdessä olisi otettu huomioon yksilöiden yksityisyydensuoja ja 3) eikä ollut olemassa tehokasta jälkikäteistä valvontaa. Näiden puutteiden vuoksi järjestelmä ei täyttänyt päästä päähän -valvonnan vaatimusta, se ylitti vastaajavaltiolle tässä suhteessa jätetyn harkintavallan eikä kokonaisuudessaan suojannut mielivaltaisuudelta ja väärinkäytösten riskeiltä.

EIT ei ratkaisussaan torju ehdottomasti ns. massavalvonnan (bulk interception regime) käyttöä. EIT katsoo, että sillä torjuttavien uhkien vakavuus, uhkien takana olevien henkilöiden kyky toimia paljastumatta tietoverkoissa ja sähköisen viestinnän reitityksen ennakoimattomuus perustelevat kansallista turvallisuutta vaarantavien uhkien tunnistamiseen tähtäävän massavalvonnan käyttöönoton kuulumista kansallisen harkintamarginaalin alaan. EIT on pitänyt yleisemminkin harkintamarginaalia laajana kansallisen turvallisuuden turvaamisen keinovalikoiman valinnassa (mm. Big Brother Watch kohta 275 ja Centrum för Rättvisa kohta 365). EIT painottaa kuitenkin, että sekä kohdistettujen että massavalvontajärjestelmien sääntelyn tulee vallan väärinkäytön estämiseksi täyttää ainakin edellä mainitut vähimmäisvaatimukset.

EIT toteaa myös tapauksessa Centrum för Rättvisa (kohta 239–245), että puuttuminen EIT 8 artiklan suojaamaan yksityiselämän suojaan on eri tasoista tietoliikenteeseen kohdistuvan tiedustelun eri vaiheissa. EIT jakaa prosessin neljään vaiheeseen: 1) tietoliikenteen hankkimiseen, 2) hakuehtojen tai hakuehtojen luokkien käyttäminen tietoliikenteen valikoimiseen, 3) suodatetun tietoliikenteen analysointi ja 4) tiedon säilyttäminen ja lopputuotteen tekeminen ja sen käyttäminen. Prosessin alussa tietoliikenteen hankkiminen, vaikka kattaakin suuren joukon ihmisiä, ei puutu henkilön yksityisyyden suojaan yhteä mittavasti kuin esimerkiksi vaiheessa kolme, jossa analyytikko tutkii suodatettua viestintää ja siihen liittyviä tietoja yhdistelemällä niitä.

EIT kiinnittää erityistä huomiota myös siihen, että ruotsalaista sääntelyä ja järjestelmää on jatkuvasti arvioitu ja tarvittaessa uudistettu myös yksityisyyden suojan parantamiseksi (kohta 351).

EIT katsoi tapauksessa myös, että Ruotsin laissa säädetty mahdollisuus kerätä tietoliikennettä signaalitiedustelun kehittämiseksi on kansallisen harkintamarginaalin rajoissa (päätöksen kohdat 291–293).

Keskeistä tapauksissa Big Brother Watch ja Centrum för Rättvisa on, että EIT kehitti oikeuskäytäntöään signaalitiedustelulle asetettavista lainsäädännöllisistä edellytyksistä (Big Brother Watch kohdat 343–361 ja Centrum för Rättvisa kohdat 257–278); Weber ja Saravia tapauksesta vakiintuneen lainsäädännölle asetettavan kuuden vaatimuksen sijaan (Weber ja Saravia kohta 95) EIT edellytti kahdeksan vaatimuksen täyttymistä (Big Brother Watch kohta 361 ja Centrum för Rättvisa kohta 275). Signaalitiedustelua koskevassa lainsäädännössä on säädettävä 1) perusteista, joiden perusteella tiedon hankinta voidaan sallia, 2) olosuhteista, joissa tiedonhankinta voi kohdistua henkilön viestintään, 3) luvan myöntämismenettelystä, 4) tiedon valinnassa, tutkimisessa ja käytössä noudatettavista menettelyistä, 5) varotoimista, joita on noudatettava luovutettaessa materiaalia eri osapuolille, 6) toimenpiteen kestosta, tiedon säilyttämisen rajoituksista ja olosuhteista, joissa tieto on poistettava ja tuhottava, 7) menettelyistä ja

yksityiskohtaisista säännöistä, joilla riippumaton viranomainen valvoo edellä mainittujen takeiden noudattamista, ja valvojan valtuudesta puuttua lainvastaiseen toimintaan sekä 8) riippumattomasta jälkikäteisestä valvonnasta ja seuraamuksista.

Tehokkaat oikeusturvakeinot (13 artikla)

EIS 13 artiklan mukaan jokaisella, jonka EIS:n yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino (”effective remedy”) kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt. Artiklan toteutumiseen liittyy olennaisesti ilmoitusvelvollisuus tai viranomaisen toimenpiteiden kohteena olleen henkilön oikeus saada asiansa selvitettäväksi. EIS 13 artiklaan koskevaa EIT:n käytäntöä on käyty laajemmin läpi HE 202/2017:ssä (s.62-64) ja HE 203/2017:ssä (s. 52–56), joten tässä yhteydessä siinä esitettyihin tapauksiin viitataan yleisellä tasolla tarpeen mukaan keskittyen EIT:n uudempaan ratkaisukäytäntöön.

Ihmisoikeussopimuksen 8 artiklan kohdalla EIT on todennut, että oikeussuojakeinojen tulee olla niin tehokkaita, kuin mahdollista ottaen huomioon salaisen viranomaistoiminnasta luonnostaan aiheutuvat rajoitukset (Klass ym. v. Saksan liittotasavalta). Rajoituksista huolimatta oikeusturvajärjestelyt katsottiin riittäviksi 13 artiklan valossa, koska henkilöllä oli oikeus saattaa asiansa lain täytäntöönpanoa valvovan komission käsiteltäväksi ja valtiosääntötuomioistuimeen.

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

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

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

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

Valitus- tai kantelumahdollisuuden käytön edellytyksenä yleensä on, että henkilö saa viranomaiselta tiedon häneen kohdistetusta tiedonhankinnasta sen jälkeen, kun tiedonhankintakeinon käyttö on päättynyt (ks. yllä Zakharov v. Venäjä). Tästä ei kuitenkaan seuraa, että ilmoitus on tehtävä välittömästi tiedonhankinnan päätyttyä. Uhka, josta tiedonhankintamenetelmän avulla on hankittu tietoja, voi jatkua vuosia tai jopa vuosikymmeniä, jolloin ilmoituksen tekemistä on turvallisuusviranomaisten toiminnan suojaamiseksi välttämätöntä lykätä vastaavasti. Oikeussuojakeinon käytön mahdollistamiseksi ilmoitus olisi kuitenkin tehtävä sen jälkeen, kun ilmoittamatta jättämiselle ei enää ole yksilöllistä perustetta (Klass v. Saksa, Zakharov v. Venäjä).

Kuitenkin myös järjestelmä, joka ei lainkaan edellytä kohdehenkilölle ilmoittamista, voi olla sopusoinnussa ihmisoikeussopimuksen kanssa. Tällöin kanteluoikeus on tullut kansallisessa lainsäädännössä säätää niin yleiseksi, että kuka hyvänsä saa kannella pelkästään sen perusteella, että epäilee viranomaisten puuttuneen luottamuksellisen viestintänsä nauttimaan suojaan (Kennedy v. Yhdistynyt Kuningaskunta).

Uudemmassa ratkaisukäytännössään EIT on todennut tapauksessa Centrum för Rättvisa, että tehokkaan oikeusturvakeinon olisi oltava kaikkien niiden käytettävissä, jotka epäilevät joutuneensa salaisten viranomaistoimenpiteiden kohteeksi. EIT on todennut kohdennettujen salaisten viranomaisen toimenpiteiden osalta, että jälkikäteinen ilmoittaminen toimenpiteestä kohteelle tarjoaa riittävän tehokkaan oikeussuojan toimenpiteiden väärinkäyttöä vastaan. Toisaalta EIT on myös todennut, että järjestelmä, jossa kuka tahansa kohteeksi joutumista epäilevä henkilö voi käyttää oikeusturvakeinoa riippumatta ilmoituksesta, voi olla riittävä (Rättvisa kohta 271 sekä siinä viitatut Roman Zakharov v. Venäjä ja Kennedy v. Yhdistynyt Kuningaskunta).

EIT katsoo tapauksessa Centrum för Rättvisa, että oikeussuojakeinot, jotka eivät ole riippuvaisi ilmoituksesta, voivat olla myös tehokkaita tietoliikenteeseen kohdistuvassa tiedustelussa ja olosuhteiden mukaan voivat tarjota parempaa suojaa henkilölle kuin ilmoitukseen sidotut oikeussuojakeinot (tapauksen kohta 272). Etenkin tilanteessa, jossa salaiset viranomaisen toimenpiteet kohdistuvat kyseisen valtion ulkopuolella oleviin kohteisiin ja valtion ulkopuolella oleviin henkilöihin ja vaikka kohteen henkilöllisyys olisi sinänsä tiedossa, toimenpiteestä ilmoittamisella

voi olla vähän tai käytännössä ei lainkaan merkitystä. Etenkin, jos henkilön olinpaikasta ei ole tietoa (tapauksen kohta 272).

EIT painotti useiden itsenäisten tiedustelutoimintaa valvovien elimien olemassaolon merkitystä järjestelmän hyväksyttävyydelle. Oikeusturvamekanismien lukuisuus kompensoi myös sitä, että tiedustelutoimista ei aina ilmoiteta niiden kohteelle. Valvontajärjestelmän osalta tuomiossa Centrum för Rättvisa kiinnitetään huomiota riippumattomuuteen ja valvonnassa esitettyjen huomioiden tosiasialliseen vaikuttavuuteen.

Tilanteessa, jossa ilmoitusvelvollisuutta ei ole, oikeusturvakeinon tehokkuuden kannalta on välttämätöntä, että sitä toteuttaa viranomaisesta riippumaton taho, joka takaa oikeudenmukaisen käsittelyn ja tarjoaa mahdollisuuksien mukaan kontradiktorisen menettelyn. Tällaisen viranomaisen päätökset on perusteltava ja niiden on oltava oikeudellisesti sitovia muun muassa laittoman viestinnän kuuntelun lopettamisen ja laittomasti hankitun ja/tai tallennetun kuunteluaineiston hävittämisen osalta (tapauksen kohta 273 sekä siinä viitatut tapaukset Segerstedt-Wiberg ja muut v. Ruotsi ja Leander v. Ruotsi).

Ruotsalaisessa järjestelmässä valvovalla valtuutetulla on lähtökohtainen läsnäolovelvollisuus tuomioistuinmenettelyssä, pääsy asian kannalta merkityksellisiin asiakirjoihin ja oikeus lausua tuomioistuimessa niiden johdosta. EIT:n mielestä tällainen järjestely kompensoi osittain tuomioistuinmenettelyyn ja tuomioistuimen päätöksiin kohdistuvia julkisuuden rajoituksia (tapauksen kohdat 137–138).

EIT toteaa Centrum för Rättvisa tapausta arvioidessaan, että oikeussuojakeinojen, jotka eivät ole riippuvaisia ilmoituksesta, on oltava toimenpiteen kohteeksi joutuneeksi epäilevien käytettävissä (tapauksen kohta 355). EIT toteaa, että Ruotsin lainsäädäntö antoi henkilöille mahdollisuuden saattaa asiansa tutkittavaksi (tapauksen kohta 356). EIT kuitenkin totesi, että Ruotsin järjestelmässä toimivaltainen valvonnasta vastaava elin (SIUN) myöntää myös luvat tietoliikenteeseen kohdistuvaan tiedonhankintaan. Näin ollen jälkikäteistä valvontaa suorittavaa ja henkilön oikeussuojasta huolehtivaa viranomaista ei voitu pitää erityisen objektiivisena tai sen suorittamaa käsittelyä perusteellisena. Myös kysymys eturistiriidasta nousee esiin, mikä voi houkutella käsiteltävänä olevan asian kohdalla asian ylimalkaiseen käsittelyyn (kohta 359). Tosin SIUN on myös ulkopuolisen valvonnan kohteena, mutta tällaista valvontaa käytännössä ei oltu koskaan suoritettu eikä tällaista lakisääteistä tehtävää oltu varsinaisesti myöskään säädetty (tapauksen kohta 360).

EIT katsoi, että SIUN:n kaksoisrooli heikensi tietoliikenteeseen kohdistuvan tiedonhankinnan jälkikäteistä valvontaa siinä määrin, että se aiheuttaa riskejä asianomaisten henkilöiden perusoikeuksien toteutumiselle (tapauksen kohta 372). Osaltaan tämänkin takia EIT katsoi, että Ruotsin lainsäädäntö ei täyttänyt EIS:n 8 artiklan vaatimuksia (tapauksen kohta 373).

5.2.2 Euroopan unionin oikeus

Jäsenvaltioiden kansallista turvallisuutta suojaamiseksi tapahtuva toiminta ei kuulu Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan mukaan EU:n toimivaltaan. Kansallista turvallisuutta koskeva poikkeus heijastuu useisiin EU:n säädöksiin, kuten tietosuoja-asteukseen ja sähköisen viestinnän tietosuojadirektiiviin.

Unionilla ei ole kansallista turvallisuutta koskevaa toimivaltaa. Kansallinen turvallisuus on myös vakiintuneesti hyväksytty Euroopan unionin tuomioistuimen (EUT) oikeuskäytännössä oikeutetuksi tavoitteeksi rajoittaa perusoikeuksia (esim. tuomio komissio v. Suomi, C-284/05, 45, 47 ja 49 kohta) (esim. PeVL 36/2018 vp.).

Poikkeuksen ei kuitenkaan voida katsoa olevan ehdoton, vaan tiedusteluviranomaisten toiminta saattaa tietyissä tilanteissa kuulua EU-oikeuden soveltamisalaan ja näin ollen kuulua EU:n perusoikeussääntelyn piiriin kansallisten perustuslaillisten säännösten ja kansainvälisten ihmisoikeussopimusten takaamien oikeuksien lisäksi. Kansallista turvallisuutta koskeva poikkeus ei näin ollen ole kaiken kattava poikkeus ja ei itsestään selvästi sulje pois kokonaan unionin oikeuden sovellettavuutta.

Unionin tuomioistuin on sittemmin vahvistanut tämän johtopäätöksen todeten, että kansalliseen turvallisuuteen vetoaminen ei voi oikeuttaa unionin oikeuden kiertämistä, perusoikeuskirjaan perustuva valvonta mukaan lukien. Tuomioistuin on selventänyt periaatetta liittyen jäsenvaltioiden järjestelyihin, joissa yleisesti ja erotuksetta on velvoitettu teleoperaattoreita säilyttämään viestintään liittyviä tietoja ja järjestämään niiden reaaliaikainen saatavuus tiedusteluviranomaisille kansallisen turvallisuuden suojaamiseksi. Tuomioistuin on myös määritellyt kansallisen turvallisuuden suojaamisen valtion elintärkeiden toimintojen ja yhteiskunnan perusetujen suojaamiseksi sekä valtion perusrakenteiden horjuttamiselta ja väestön uhkaamiselta suojaamiseksi (EUT yhdistetyt tapaukset C-511/18, C-512/18 ja C-520/10 kohdat 99 ja 135).

Lisäksi tuomioistuin on täsmentänyt, että yleisen turvallisuuden suojelua ja vakavan rikollisuuden torjuntaa ei voida kohdella samalla tavoin kuin kansallisen turvallisuuden suojaamista. Määrittelemällä kansallisen turvallisuuden suojaamisen tuomioistuin on pyrkinyt sulkemaan pois mahdollisuuden vedota siihen kiertoreittinä muissa tarkoituksissa.

EUT on todennut, että kansalliset turvallisuusnäkökohdat edellyttävät aina, että yksityiset toimijat (kuten palveluntarjoajat) säilyttävät ja asettavat saataville viestintään liittyviä tietoja valtion viranomaisten pyynnöstä ja perustuen lakiin. Näissä tapauksissa on katsottava, että tiedonhankintaa eivät suorita varsinaisesti valtion toimivaltaiset viranomaiset. Koska palveluntarjoajat kuuluvat Euroopan unionin oikeuden soveltamisalaan, tietojen säilyttäminen ja pääsy niihin kansallisen turvallisuuden nojalla kuuluvat näin ollen tältä osin unionin oikeuden soveltamisalaan.

EUT:n oikeuskäytännöllä on ollut kuitenkin merkittävä vaikutus kansallisella tasolla. Esimerkiksi Ranskassa EUT:n tuomio johti niin kutsuttuun Conseil d'État -päätökseen, joka johti tiedustelulain muuttamiseen ranskalaisen valvontaelimen lausuntojen sitovuuden osalta. Saksan perustuslakituomioistuin on todennut vuonna 2020, että tiedustelupalvelujen harjoittama ulkomaisen viestiliikenteeseen kohdistuva tiedustelu loukkaa Saksan perustuslaissa taattuja perusoikeuksia. Yksi syy muutoksille oli se, etteivät toimivaltuudet ja toimivaltaisten viranomaisten rakenne varmistaneet niiden riittävää itsenäistä ja jatkuvaa valvontaa.

Kaiken kaikkiaan jotkin seikat tiedusteluviranomaisten toiminnassa, kuten tietoliikenteeseen kohdistuva tiedonhankinta, ovat unionin oikeuden soveltamisalan ulkopuolella. EUT on myös korostanut, että salassa pidettävän tiedonhankinnan, joka on unionin oikeuden soveltamisalan ulkopuolella, olisi kuitenkin täytettävä EIS:n asettamat vaatimukset.

5.2.3 Euroopan unionin perusoikeuskirja

Euroopan unionin perusoikeuskirjaa ja siihen liittyvää Euroopan unionin tuomioistuimen oikeuskäytäntöä on käsitelty kattavasti hallituksen esityksissä eduskunnalle HE 202 /2017 vp (s. 64-67) ja HE 203/2017 (s. 56-61). Tässä esityksessä keskitytään käsittelemään viimeaikaista EUT:n oikeuskäytäntöä.

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 Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön. EIT:n laajalla ihmisoikeussopimuksen 8 artiklaa koskevalla ratkaisukäytännöllä on näin ollen katsottava olevan relevanssia myös perusoikeuskirjan 7 artiklan tulkinnalle.

Perusoikeuskirjan mukaisten perusoikeuksien kunnioittamisen valvonta ei edellä sanotusta huolimatta kuulu EIT:lle vaan Euroopan unionin tuomioistuimelle (EUT) ja kansallisille tuomioistuimille. Tietoliikennetiedustelun kannalta merkitystä on EUT:n huhtikuussa 2014 antamalla tuomiolla, jolla EUT julisti pätemättömäksi vuonna 2006 säädetyn teletunnistetietojen tallentamista koskevan direktiivin (2006/24/EY). Direktiivi oli asettanut unionin jäsenvaltioille velvoitteen säätää teletunnistamistietojen kattavasta säilyttämisestä vakavien rikosten torjunnan ja tutkinnan tarpeita varten.

EUT on ratkaisun jälkeen lukuisissa tuomioissaan täsmentänyt sitä, millä edellytyksillä tiettyjen tietojen säilyttäminen on mahdollista viranomaistarkoituksia varten. On kuitenkin huomattava, että tapaukset koskevat tilanteita, joissa tiedusteluviranomaisen ulkopuolinen taho on määrätty säilyttämään yleisesti ja erotuksetta tietoja.

Keskeistä nyt käsiteltävänä olevan esityksen kannalta on se, että EUT on tehnyt linjauksia sen suhteen, milloin perusoikeuskirjasta voidaan poiketa kansallisen turvallisuuden, mukaan lukien puolustus, nimissä. Lisäksi ratkaisuista voidaan tulkita yleisen tason linjauksia, miten esimerkiksi teletunnistetietojen suhteesta yksityiselämän suojaan.

Viimeaikaisessa käytännössään (tuomio 30.4.2024, Le Quadrature du net, C-470/21, EU:C:2024:370, kohdat 95-97) EUT on todennut EUT:n oikeuskäytännöstä ilmenevän, että rikosten torjunnan alalla ainoastaan vakavan rikollisuuden torjumista tai yleiseen turvallisuuteen kohdistuvien vakavien uhkien ehkäisemistä koskevilla tavoitteilla voidaan oikeuttaa

perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin puuttuminen, jota merkitsee se, että viranomaisilla on pääsy joukkoon sellaisia liikenne- ja paikkatietoja, jotka ovat omiaan antamaan tietoja sähköisen viestintävälineen käyttäjän harjoittamasta viestinnästä tai tämän käyttämien päätelaitteiden sijainnista ja joista voidaan tehdä täsmällisiä asianomaisten henkilöiden yksityiselämää koskevia päätelmiä, ja muista tietoihin pääsyä koskevan pyynnön oikeasuhtaisuutta koskevista tekijöistä, kuten sen ajanjakson pituudesta, jolta tällaisiin tietoihin pääsyä pyydetään, ei voi seurata, että tällainen tietoihin pääsy voidaan oikeuttaa rikosten ehkäisemistä, tutkintaa, selvittämistä ja syyteharkintaa yleisesti koskevalla tavoitteella (tuomio 2.3.2021, Prokuratuur, C-746/18, EU:C:2021:152, 35 kohta).

Sitä vastoin silloin, kun puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin, jota viranomaisten pääsy sähköisten viestintäpalvelujen tarjoajien säilyttämiin henkilöllisyyttä koskeviin tietoihin merkitsee, ilman, että mainittuja tietoja voidaan yhdistää suoritettua viestintää koskeviin tietoihin, ei ole vakavaa, koska näiden tietojen perusteella ei voida kokonaisuutena tarkasteltuna tehdä täsmällisiä päätelmiä niiden henkilöiden yksityiselämästä, joiden tiedoista on kyse, mainittu pääsy tietoihin voidaan oikeuttaa yleisesti rikosten ehkäisemisen, tutkinnan, selvittämisen ja syyteharkinnan alalla (ks. vastaavasti tuomio 2.10.2018, Ministerio Fiscal, C-207/16, EU:C:2018:788, 54, 57 ja 60 kohta).

EUT myös lisää, että EUT:n vakiintuneessa oikeuskäytännössä on vahvistettu periaate, että kansallinen turvallisuus, sisältäen maanpuolustuksen, on yleisen edun mukainen tavoite ja kansallinen turvallisuus on merkittävämpi peruste kuin rikostorjunta (tuomio 30.4.2024, La Quadrature du net ym., C470/21, kohta 97 ja vastaavasti tuomio 6.10.2020, La Quadrature du Net ym., C 511/18, C 512/18 ja C 520/18, EU:C:2020:791, 166 kohta).

EUT toteaa La Quadrature du net tapauksessa (C-470/21, kohta 103), että siinä tapauksessa, että sähköisten viestintäpalvelujen tarjoajat velvoitetaan käyttämään säilyttämismenetelmiä, IP-osoitteiden yleinen ja erotuksetta tapahtuva säilyttäminen ei merkitse vakavaa puuttumista osoitteiden haltijoiden yksityiselämään, koska näiden tietojen perusteella ei voida tehdä täsmällisiä päätelmiä heidän yksityiselämästään.

Edellä viitatuista tuomioista voidaan tehdä johtopäätös, että oikeushyvien hierarkiassa kansallinen turvallisuus, sisältäen maanpuolustuksen, on korkeampi asema kuin rikosten torjunnalla. Näin ollen se on myös kauempana perusoikeuskirjan soveltamisesta. Lisäksi voidaan todeta, että tallennettavia tietoja ja niiden käsittelyä on arvioitava sen perusteella, miten syvällisiä päätelmiä niiden perusteella voidaan tehdä yksityishenkilön elämästä ja näin ollen tosiasiallisesti puuttuvat henkilön yksityiselämän suojaan. Esimerkiksi pelkkä IP-osoite ei merkitse vakavaa puuttumista osoitteen haltija yksityiselämään, jos IP-osoitetta ei voida yhdistää muihin tietoihin, jolloin henkilön yksityiselämästä voidaan muodostaa tarkempaa tietoa.

5.2.4 Ulkomainen lainsäädäntö

Ruotsi

Säkerhetspolisen (SÄPO) on Ruotsin turvallisuus- ja tiedustelupalvelu (kansallinen turvallisuuspalvelu). Ruotsissa ei ole säädetty kansallisen turvallisuuden suojaamisen tarkoituksessa tapahtuvasta varsinaisesta kotimaan siviilitiedustelusta, vaan maan turvallisuuspoliisi SÄPO:n toimivaltuuksien käyttö tapahtuu valtion turvallisuutta vaarantavien rikosten estämiseksi, paljastamiseksi ja selvittämiseksi. SÄPO:sta säädetään poliisilainsäädännössä (Polislagen

1984:387, Polisförordningen 2014:1104, Förordningen (2022:1719) med instruktion för Säkerhetspolisen).

Ruotsissa tiedustelutoiminnasta säädetään sotilastiedustelusta annetulla yleislailla (Lag om försvarsunderrättelseverksamhet, 2000:130) ja signaalitiedustelusta annetulla yleislailla (Lag om signalspaning i försvarsunderrättelseverksamhet, 2008:717). Puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA) toimii kansallisena signaalitiedusteluviranomaisena. Sotilastiedustelutoimintaa harjoittavat puolustusvoimien tiedustelu- ja turvallisuuspalvelu (Militära underrättelse- och säkerhetstjänsten, MUST), puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA), puolustusvoimien materiaalilaitos (Försvaretsmaterielverk, FMV) sekä Kokonaismaanpuolustuksen tutkimuslaitos (Totalförsvarets forskningsinstitut, FOI).

Ruotsissa signaalitiedustelua puolustustiedustelussa ohjaa signaalitiedustelua koskeva laki (Lag om signalspaning i försvarsunderrättelseverksamhet, 2008:717) ja sitä täydentävä asetus (Förordning om signalspaning i försvarsunderrättelseverksamhet 2008:923). Puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA) toimii kansallisena signaalitiedusteluviranomaisena.

Signaalitiedustelulain mukaan signaalitiedustelulla tarkoitetaan elektronisessa muodossa olevien signaalien hakemista (inhämta signaler i elektronisk form). Määritelmä on tekniikkaneutraali ja kattaa kaikki signaalitiedustelun menetelmät, kuten esimerkiksi kaapeli- ja radiosignaalitiedustelun sekä manuaalisen ja automaattisen tiedonkeräämisen. Signaalia ei saa kerätä, jos vastaanottaja ja lähettäjä ovat Ruotsissa. Kaapelitietoliikennettä saadaan tiedustella vain silloin, kun se ylittää Ruotsin rajan. Kielto ei kuitenkaan koske signaaleja, jotka kulkevat itsenäisesti teknisten järjestelmien välillä silloin, kun signaalit eivät sisällä henkilötietoja tai kun signaalit lähetetään ulkomaiselle sotilashenkilöstölle, ulkomaisille valtionaluksille, valtion ilma-aluksille tai sotilasajoneuvoille tai ne tulevat vastaavilta tahoilta ulkomailta

Ruotsissa on syksyllä 2024 valmistunut loppumietintö (Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (SOU 2024:59)) puolustustiedustelussa harjoitettavaa signaalitiedustelua koskevan lain tarkistamista koskien. Mietinnössä on muun muassa ehdotettu erityistä poikkeusta kieltoon kerätä kotimaista liikennettä, jos tällainen tiedustelu on merkityksellistä Ruotsin turvallisuuteen kohdistuvien ulkoisten uhkien torjumiseksi. Ehdotuksen tavoitteena olisi varmistaa, että sodan oloissa on mahdollista harjoittaa signaalitiedustelua Ruotsissa tapahtuvaa vihamielistä toimintaa vastaan, joka uhkaa Ruotsin suvereniteettia ja alueellista koskemattomuutta, myös ei-sotilaallisista lähteistä käsin. Mietinnössä on lisäksi ehdotettu muutettavaksi signaalitiedustelulain 1 §:ää siten, että signaalien kerääminen olisi mahdollista riippumatta siitä, ovatko signaalit välitettävinä vai tallennettuina. Signaalit voisivat olla tallennettuina esimerkiksi verkkoon liitetyissä laitteistoissa tai ohjelmistoissa.[7]

Ruotsissa on heinäkuussa 2025 lähetetty lausuntokierrokselle esitysluonnos (Fö2024/01478)[8], jossa huomioidaan sekä loppumietinnössä (SOU 2024:59) esitetty että esitetään uusia muutoksia tiedustelulakien päivittämiseksi. Hallitus on antanut lakiluonnokset uudesta ja muutettavista laeista lakineuvostolle (Lagrådet) 5.2.2026 (Lagrådsremiss. Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning). Esitys sisältää seuraavat lakiehdotukset: Förslag till lag om signalspaning i försvarsunderrättelseverksamhet i krig eller

[7] SOU 2024:59; s. 241.

[8] Fö2024:01478 Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning (https://www.regeringen.se/contentassets/20faf90d0b7c40ba82a37dd85db22bf0/utkast-lagradsremiss-signalspaning-i-forsvarsunderrattelseverksamhet---en-modern-och-andamalsenlig-lagstiftning.pdf).

krigsfara, Förslag till lag om ändring i lagen (2008:717) om signalspaning i försvarsunderrättelseverksamhet, Förslag till lag om ändring i lagen (2009:966) om Försvarsunderrättelsedomstol ja 2.4 Förslag till lag om ändring i lagen (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt. Ehdotettu uusi laki ja lakimuutokset on ehdotettu tulemaan voimaan kesäkuussa 2026

Selvitysmies Carl Bildtin johtama hanke antoi kesäkuussa 2025 mietinnön *En reformerad underrättelseverksamhet* (SOU 2025:78) koskien Ruotsin tiedustelupalvelun uudistamista. Selvityksen tehtävänä oli uudistaa tiedustelutoimintaa Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan tueksi sekä muutoin Ruotsin turvallisuuteen kohdistuvien uhkien kartoittamiseksi.

Tietoliikennetiedustelun hakuehdot

Ruotsin signaalitiedustelulain 1 §:n 3 momentin säännöksen mukaan, mikäli toiminnan kannalta on välttämätöntä, voidaan signaaleja hankkia myös signaaliympäristössä, teknisessä kehityksessä ja signaalisuojassa tapahtuvien muutosten seuraamiseksi sekä tiedonhankinnassa käytettävän puolustustiedustelulain mukaisen toimialan tekniikan ja menetelmien kehittämiseksi.

Lain esitöiden (Prop. 2006/07:63) mukaan tällaista tietoa käytetään ainoastaan tiedusteluviranomaisen teknisten kyvykkyyksien kehittämiseksi, jotta tiedustelutehtäviin kyetään vastaamaan entistä paremmin. Teknisten tietojen keräyksestä ja teknisten tietojen käsittelystä ei siten muodostu sellaista tietoa, jota hyödynnettäisiin tiedustelutehtävään vastaamisessa. Lain esitöissä todetaan lisäksi, että tällaista saavutettua teknistä kyvykkyyttä ja sitä koskevaa tietoa on mahdollista jakaa viranomaisten välillä. Jaettava tieto ei kuitenkaan olisi varsinaista tiedustelutietoa, eikä yksityiselämän suojan piiriin kuuluvaa viestintää.

Signaalitiedustelulain 3 §:n mukaan signaalien keräämisen tulee perustua käytettäviin hakuehtoihin. Hakuehtojen määrittämisessä ja niiden käytössä tulee huomioida yksityisyydensuoja. Hakuehtoja, jotka liittyvät suoraan tiettyyn fyysiseen henkilöön, saadaan käyttää vain, jos se on toiminnan kannalta erityisen tärkeää. Hakuehdot voivat kuvata niiden toimijoiden, organisaatioiden, alustojen tai teknisten järjestelmien edustuksia, joihin signaalitiedustelun tulee kohdistua. Hakuehdot mahdollistavat teknisesti sen, että olennainen tieto löydetään ja tunnistetaan. Yksittäinen hakuehto voidaan usein liittää tiettyyn viestintäpalveluun, jota kohde käyttää, esimerkiksi tiettyyn matkapuhelinpalveluun tai sähköpostipalveluun.[9] Lain esitöissä[10] todetaan, että nopeasti muuttuva signaaliympäristö edellyttää, että myös hakuehtoja muokataan ja määritetään uusien tietojen karttuessa.

Puolustustiedustelussa harjoitettavaa signaalitiedustelua koskevan asetuksen 3 §:n mukaan FRA:n tulee ilmoittaa puolustustiedustelun valvonnasta vastaavalle elimelle (Statens inspektion för försvarsunderrättelseverksamheten, SIUN) sellaisten hakuehtojen käyttämisestä, jotka on suoraan yhdistettävissä luonnolliseen henkilöön ja joita käytetään signaalitiedustelutoiminnassa.

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Signaalitiedustelulain 7 § asettaa FRA:lle tietyissä tilanteissa tietojen hävittämisvelvollisuuden. Lain mukaisesti hankittuja tietoja koskevat tallenteet tai muistiinpanot on välittömästi hävitettävä, jos sisältö koskee yksittäistä luonnollista henkilöä eikä sillä katsota olevan merkitystä 1

[9] SOU 2024:59, s. 56.
[10] Prop. 2006/07:63, s. 77–78.

§:ssä tarkoitetun toiminnan kannalta. Niin ikään FRA:lla on velvollisuus hävittää tiedot välittömästi, jos tiedot koskevat rippisalaisuutta, lähdesuojaa tai asianajajan ja asiakkaan välistä kommunikointia rikosoikeudellisessa asiassa.

Puolustustiedustelussa harjoitettavaa signaalitiedustelua koskevaa asetusta (Förordning om signalspaning i försvarsunderrättelseverksamhet 2008:923) on muutettu 1.1.2025 voimaan tulleella asetuksella (SFS 2024:427). Muutosasetuksella on täsmennetty tiettyjen signaalitiedustelulaissa tarkoitettujen tallenteiden hävittämisvelvollisuutta. Tallenteet ja muistiinpanot tulee hävittää siten, ettei niitä saada palautettua.

Henkilötietojen käsittelystä FRA:n toiminnassa annetun lain (Lag (2021:1172) om behandling av personuppgifter vid Försvarets radioanstalt) 2 luvun 19 §:n mukaan henkilötietoja ei saa käsitellä pidempään kuin on tarpeen käsittelyn tarkoitusten kannalta.

Henkilötietojen käsittelystä FRA:n toiminnassa annetun asetuksen (Förordning (2021:1208) om behandling av personuppgifter vid Försvarets radioanstalt) 3 luvun 1 §:n mukaan FRA:lla saa olla henkilötietoja sisältävää automaattisesti käsiteltyä ja käsittelemätöntä raakadataa, jonka merkitystä tiedustelutoiminnalle ei siis ole vielä arvioitu. Tällaiseen raakadataan kuuluvia henkilötietoja ei kuitenkaan saa käsitellä pidempään kuin yhden vuoden ajan siitä, kun tietojen käsittely on aloitettu.

Ilmoitusvelvollisuus

Signaalitiedustelulain 11 a § edellyttää, että luonnolliselle henkilölle tulee ilmoittaa niin pian kuin mahdollista, ja viimeistään kuukausi puolustustiedustelutehtävän päättymisestä, milloin ja missä tarkoituksessa tiedustelu on toteutettu. Lain 11 b §:n mukaan ilmoituksen antamista voidaan kuitenkin lykätä, jos salassapito estää sen antamisen. Jos ilmoitusta ei ole voitu antaa salassapitosyistä vuoden kuluessa tiedustelutehtävän päättymisestä, sitä ei tarvitse antaa. Ilmoitusta ei myöskään tarvitse antaa, jos tiedustelu on koskenut yksinomaan vieraan valtion olosuhteita tai vieraan valtioiden välisiä suhteita.

Ruotsissa esitetään edellä kuvatun ilmoitusvelvollisuuden poistamista. Esityksessä on huomioitu EIT:n kannanotto Centrum för Rättvisa -tapauksessa. Esitysluonnoksessa[11] todetaan, että salassapidon perusteella FRA ei ole koskaan antanut 11 a §:n perusteella ilmoitusta, eikä ole todennäköistä, että ilmoituksia tulevaisuudessakaan annettaisiin. Esitysluonnoksen mukaan ilmoitusvelvollisuudella ei ole käytännön merkitystä oikeusturvan tai yksityisyyden suojan takaajana. Signaalitiedustelulain 10 a §:n mukainen tarkastusvelvollisuus täyttää tätä tarkoitusta.

Norja

Norjan ulkomaan tiedustelupalveluna toimii Etterretningstjenesten (E-tjenesten), jonka tehtävistä ja toimivaltuuksista säädetään laissa tiedustelupalvelusta (Lov om Etterreningstjenesten 2020-06-19 nr. 77). Norjan nykyinen tiedustelupalvelulaki on tullut voimaan 2021. Maan turvallisuuspoliisi on Politiets sikkerhetstjeneste (PST). PST:n toimivaltuuksien käyttö tapahtuu valtion turvallisuutta vaarantavien rikosten estämiseksi, paljastamiseksi ja selvittämiseksi.

[11] Fö2024/01478, Utkast till lagrådsremiss Signalspaning i försvarsunderrättelseverksamhet – en modern och ändamålsenlig lagstiftning, s. 124–126.

E-tjenestenin ja PST:n välisestä yhteistyöstä on säädetty oma asetuksensa (Instruks om samarbejdet mellom Etteretningstjenesten og Politiets sikkerhetstjeneste).

Tietoliikennetiedustelun hakuehdot

Tiedustelupalvelulain 5 luvun 3 §:n mukaan tiedustelupalvelu voi kerätä raakadataa massana (raw data in bulk), kun se on tarpeen asiaankuuluvan ja riittävän tietopohjan saavuttamiseksi. Tällaiseen raakadataan tehtyjen hakujen tulee täyttää kohdennetun tiedonhankinnan perusedellytykset ja hakuprosessi kirjataan valvontaa varten. Raakadataan tehtäviä hakuja, jotka liittyvät Norjassa oleskelevaan henkilöön, saa suorittaa ainoastaan silloin, kun se on ehdottoman välttämätöntä tiedustelupalvelun 3 luvun 1 §:n mukaisten tehtävien hoitamiseksi. Rajoitus ei koske ulkomaalaisia tai kansalaisuudettomia henkilöitä, jotka toimivat vieraan valtion tai valtiollista toimijaa muistuttavan tahon puolesta.

Tiedustelupalvelulain 7 luvun 5 §:n mukaan tiedustelupalvelu voi suorittaa testikeräystä ja testianalyysejä rajat ylittävästä elektronisesta tietoliikenteestä ja verkosta. Pykälän mukaan testikeräystä ja testianalyysejä saa käyttää yksinomaan valinnan, suodatuksen, tallennuksen, haun, uudelleenkäsittelyn, signaaliympäristön ymmärtämisen ja palveluiden sekä dataformaattien tunnistamisen mahdollistamiseksi, sekä muuhun tekniseen tukeen.

Testikeräys suoritetaan suodattamattoman tietoliikenteen poiminnalla yhdestä tai useammasta tietoliikennevirrasta. Yksi poiminta ei saa ylittää 30 sekuntia, eikä poimintoja saa tehdä useammin kuin kerran tunnissa. Poimintoja ei saa säilyttää pidempään kuin on tarpeen, ja ne on poistettava viimeistään 14 päivän kuluttua. Poiminnat on tallennettava lyhytaikaiseen säilöön, joka on pidettävä erillään niistä säilöistä, jotka on varattu tallennetulle metatiedolle ja tallennetulle sisältötiedolle.

Norjan tiedustelupalvelusta annetun lain 7 luvun 7 §:n mukaan tiedustelupalvelu voi kerätä ja tallentaa metadataa massana (metadata in bulk) sähköisestä viestinnästä, joka kulkee Norjan rajan yli. Lain 7 luvun 6 §:ssä säädetään kuitenkin velvollisuudesta pyrkiä ehkäisemään sellaisen metadatan tallentaminen, joka liittyy Norjassa oleskelevien osapuolten väliseen viestintään. Lain 7 §:n mukaan metatiedolla tarkoitetaan tietoja, jotka kuvaavat muuta dataa tai sisältävät lisätietoja dataan liittyen, kuten tietoja, jotka kuvaavat sisällön muotoa, lähettäjää ja vastaanottajaa tai viestinnän kokoa, sijaintia, ajankohtaa ja kestoa. Sisältötietojen tallentamisen ehkäisemiseksi tiedustelupalvelun on ylläpidettävä luetteloa tallennettavissa olevista metatietotyypeistä ja luettelon tulee olla valvontaviranomaisten saatavilla.

Lain 7 luvun 8 §:n mukaan tallennettuihin metatietoihin on mahdollista tehdä hakuehtojen käyttöön perustuvia hakuja tuomioistuimen luvalla. Hakuja tallennettuihin metatietoihin voi tehdä ainoastaan tähän tehtävään koulutetut ja nimetyt henkilöt. Tallennettujen metatietojen päivitystä, teknistä analyysiä ja vianetsintää saa suorittaa lain 5 §:n mukaan ainoastaan sellaiset tekniset asiantuntijat, jotka eivät työskentele tiedusteluanalyysitehtävissä.

Norjan tiedustelupalvelusta annetun lain 7 luvun 9 §:n mukaan tiedustelupalvelu voi lisäksi tuomioistuimen luvalla kerätä ja tallentaa sisältötietoja ja siihen liittyviä metatietoja sellaisesta tietoliikenteestä, joka ylittää Norjan rajan. Sisältötiedon määritelmänä on, että se on tietoa, joka ei ole metatietoa.

Tietoliikennetiedustelulla hankittujen tietojen hävittäminen

Tekniset parametrit ja käsitellyt testianalyysit, joita ei voida yhdistää yksittäisiin henkilöihin, voidaan säilyttää niin kauan kuin se on tarpeen lain 7 luvun 5 §:n mukaisten testianalyysien tavoitteen saavuttamiseksi.

Tiedustelupalvelusta annetun lain 7 luvun 7 §:n mukaan tallennettu metatieto on poistettava viimeistään 18 kuukauden kuluessa.

Ilmoitusvelvollisuus

Norjan tiedustelupalvelulaissa ei säädetä viranomaiselle yleistä velvollisuutta ilmoittaa siitä, että henkilö on ollut tiedustelun kohteena. Tiedustelumenetelmien käyttöä valvoo tiedusteluvalvontavaliokunta (EOS-utvalget). Tiedusteluvalvontavaliokunnalle on mahdollista tehdä valitus, mikäli epäilee olleensa tiedustelun kohteen tai tietojensa tulleen käsitellyksi lainvastaisesti. EOS-valvontalain (Lov om kontroll med etterretnings-, overvåkings- og sikkerhetstjeneste) 8 §:n mukaisesti tiedusteluvalvontavaliokunnalla on kattava pääsy tiedustelupalveluiden tietoihin valvontatehtävässään. Lähtökohtaisesti valituksen johdosta annettavassa lausumassa ei kuitenkaan oteta kantaa siihen, onko henkilö ollut tiedustelun kohteena, sillä kyseessä on salassa pidettävä tieto.

Tanska

Tiedustelutoiminnasta on säädetty turvallisuuspoliisia ja puolustusvoimien tiedustelupalvelua koskevissa laeissa (Lov om Politiets Efterretningstjeneste, nr. 604 af 12. juni 2013; Lov om Forsvarets Efterretningstjeneste, nr. 602 af 12. juni 2013).

Ulkomaantiedustelusta vastaa puolustusvoimien tiedustelupalvelu FE (Forsvarets Efterretningstjeneste), jonka tehtävistä, toimivaltuuksista ja toiminnan valvonnasta säädetään laissa puolustusvoimien tiedustelupalvelusta (Lov om Forsvarets Efterretningstjeneste, jäljempänä FE-laki). FE-lain muutosesitys on ollut lausuntokierroksella helmikuussa 2025.[12] Puolustusministeriö on huhtikuussa 2025 ilmoittanut, että lakiesityksen antaminen siirtyy seuraavalle vuodelle.[13] Muutosesityksen taustalla on Euroopan ihmisoikeustuomioistuimen ratkaisukäytäntö ja FE-lain päivittäminen vastaamaan tuomioistuimen ratkaisukäytäntöä.

Turvallisuuspoliisin, Politiets Efterretningstjeneste (PET, toimivaltuuksien käyttö tapahtuu valtion turvallisuutta vaarantavien rikosten estämiseksi, paljastamiseksi ja selvittämiseksi.

Tietoliikennetiedustelun hakuehdot

Tanskan FE-laissa ei ole erityisiä säännöksiä koskien hakuehtojen määrittämistä ja teknisen analyysin tekemistä signaaliympäristössä tapahtuvien muutosten havaitsemiseksi.

Tietojen hävittäminen

FE-lain 6 §:n 1 momentin mukaan puolustusvoimien tiedustelupalvelun on lähtökohtaisesti poistettava tiedot Tanskassa asuvista luonnollisista tai oikeushenkilöistä, jotka on hankittu 1 §:n 1 momentin mukaisen toiminnan yhteydessä, mikäli viimeisten 15 vuoden aikana ei ole hankittu uutta, samaa asiaa sisällöllisesti koskevaa tietoa, eikä muualla ole toisin säädetty. Pykälän 2 momentin mukaan raakadata tulee poistaa 15 vuoden kuluessa keräysajankohdasta. Tästä

[12] https://hoeringsportalen.dk/Hearing/Details/69633
[13] https://www.ft.dk/samling/20241/almdel/FOU/bilag/127/3012501.pdf

voidaan kuitenkin poiketa, mikäli tehtävien suorittaminen edellyttää sitä olennaisista syistä. FE-lain 6 a §:n mukaan kerätyt tiedot on kuitenkin poistettava riippumatta siitä, onko säilytysaika umpeutunut, mikäli asiat tai asiakirjat eivät enää täytä tietojen käsittelyä koskevia ehtoja. Viranomaisella ei ole velvollisuutta tarkastella tietoja jatkuvasti oma-aloitteisesti sen arvioimiseksi, täyttyvätkö 4 ja 5 §:ssä asetetut edellytykset henkilötietojen käsittelylle edelleen.

Ilmoitusvelvollisuus

FE-laissa ei säädetä viranomaiselle yleistä velvollisuutta ilmoittaa siitä, että henkilö on ollut tiedustelutoiminnan kohteena. Tiedustelupalveluiden toimintaa valvovalle viranomaiselle (Tilsynet med Efterretningstjenesterne, jäljempänä TET) on mahdollista tehdä ilmoitus, mikäli epäilee olleensa tiedustelun kohteena.

Saksa

Saksassa tiedustelutoiminnasta on säädetty tiedusteluviranomaisista säädetyissä laeissa (Gesetz über den Bundesnachrichtendienst, 20. Dezember 1990, BGBl. I S. 2954, 2979; Gesetz über den militärischen Abschirmdienst, 20. Dezember 1990, BGBl. I S. 2954, 2977; Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, 20. Dezember 1990, BGBl. I S. 2954, 2970). Luottamuksellisen viestin sisältöön puuttuvista tiedustelumenetelmistä säädetään erikseen niin sanotussa G 10 -laissa (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, 26. Juni 2001, BGBl. I S. 1254, 2298).

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 Bundesamt für Verfassungsschutz (BfV) ja sotilaallisena turvallisuuspalveluna Militärischer Abschirmsdienst (MAD). MAD:n ensisijaisena tehtävänä on havaita ja torjua sellaisia uhkia, jotka kumpuavat Saksan puolustushallinnon sisältä. Kaikkien edellä mainittujen toimijoiden tehtävistä ja toimivaltuuksista säädetään omissa laeissaan, joskin BND:n ja MAD:n toimintaa koskevat lait toimivaltuuksien osalta laajasti viittaavat BfV:n toimintaa koskevaan lakiin, jossa säädetään liittovaltion turvallisuuspalvelun ja osavaltioiden turvallisuuspalveluiden yhteistyöstä (Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, jäljempänä BfV-laki).

Ulkomaantiedustelupalvelulakia (jäljempänä BND-laki) on uudistettu perustuslakituomioistuimen toukokuussa 2020 antaman päätöksen[14] seurauksena. Uudistettu BND-laki tuli voimaan 1.1.2022. Uudistuksessa huomioitiin erityisesti yksityisyyden suojan sekä lehdistönvapauden toteutuminen ulkomaan tietoliikennetiedustelussa.

Toimivaltuussääntelyn kannalta merkitystä on lisäksi posti- ja telesalaisuuden rajoittamisesta annetulla lailla (Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, jäljempänä G10-laki), joka sisältää kaikkia sellaisia tiedustelumenetelmiä koskevan sääntelyn, joilla turvallisuus- ja tiedustelupalvelujen tiedonhankinta puuttuu luottamuksellisen viestin sisältöön.

Tietoliikennetiedustelun hakuehdot

[14] Bundesverfassungsgericht, 1 BvR 2835/17 (19.5.2020), https://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/EN/2020/05/rs20200519_1bvr283517en.html

BND-lain 19 §:ssä säädetään strategisesta ulkomaan tietoliikennetiedustelusta. Pykälän 8 momentin mukaan rajoittamaton tietoliikennetiedustelu on kielletty, minkä lisäksi tiedustelu saa kohdistua enintään 30 prosenttiin olemassa olevista tietoliikenneverkoista. Pykälän 5 momentin mukaan tietojen kerääminen saadaan toteuttaa ainoastaan hakuehtojen perusteella. Hakuehtojen on oltava muun muassa ennalta määriteltyjä. Pykälän 7 momentin mukaan tiedustelu ei saa kohdistua saksalaisiin, Saksassa oleviin henkilöihin tai kotimaisiin oikeushenkilöihin.

G10-lain 5 § käsittelee perustuslaissa turvatun viestintäsalaisuuden rajoittamista tietoliikennetiedustelussa. Säännöksen mukaan BND saa parlamentaarisen valvontavaliokunnan luvalla suorittaa tietoliikennetiedustelua, jos tämä on välttämätöntä eräiden uhkien havaitsemiseksi ja estämiseksi. Pykälän 2 momentin mukaan hakuehtoja, jotka johtavat yksittäisten teleliikenneyhteyksien kohdennettuun seurantaan tai koskevat yksityiselämän suojan ydinaluetta ei saa käyttää.

Tietojen hävittäminen

BND-lain 27 §:ssä säädetään kerättyjen tietojen arvioinnista ja tarkastusvelvollisuudesta. Kerätyt tiedot tulee tarkistaa viipymättä ja sen jälkeen säännöllisesti, vähintään seitsemän vuoden välein, sen selvittämiseksi, ovatko ne yksinään tai yhdessä jo olemassa olevien tietojen kanssa tarpeellisia 19 §:n 1 momentissa määriteltyihin tarkoituksiin. Mikäli henkilötiedot eivät ole tarpeellisia näihin tarkoituksiin, ne on viipymättä poistettava.

BND-lain 36 §:n mukaan yksityiselämän ydinaluetta koskevat tiedot, jotka tietoliikennetiedustelun yhteydessä mahdollisesti saadaan, on hävitettävä viipymättä ja poistaminen on dokumentoitava. Tällaisten tietojen kerääminen on kiellettyä.

Ilmoitusvelvollisuus

G10-lain 12 §:ssä säädetään ilmoituksista asianomaisille. Toimenpiteen kohteeksi joutuneelle on ilmoitettava toimenpiteen päättymisen jälkeen. Ilmoitusta ei kuitenkaan tehdä, mikäli ilmoitus vaarantaisi toimenpiteen tarkoituksen tai jos on ennakoitavissa merkittävää haittaa liittovaltion tai osavaltion yleiselle edulle. Mikäli ilmoitusta ei ole tehty 12 kuukauden kuluessa toimenpiteen päättymisestä, tulee ilmoituksen tekemättä jättäminen saattaa G10-komission käsiteltäväksi, joka määrää lykkäyksen jatkoajan.

Laissa ei säädetä tiedusteluviranomaiselle yleistä velvollisuutta ilmoittaa henkilölle, mikäli tämä on ollut tiedustelun kohteena. BfV-lain 15 §:ssä säädetään tietojen antamisesta rekisteröidylle. Viranomainen voi rekisteröidyn pyynnöstä antaa tietoja hänen henkilötiedoistaan, mikäli pyyntö on siinä määrin yksilöity, että siinä viitataan johonkin konkreettiseen tapaukseen ja henkilöllä on erityinen intressi saada häntä koskevat tiedot. Pykälän 2 momentin mukaan tietojen antamisesta voidaan pidättäytyä, mikäli tietojen antaminen vaarantaisi esimerkiksi viranomaisen tehtävien hoitamisen.

Alankomaat

Alankomaissa tiedustelutoiminnasta vastaavat yleinen tiedustelu- ja turvallisuuspalvelu Algemene Inlichtingen en Veiligheidsdienst, AIVD) ja sotilaallinen tiedustelu- ja turvallisuuspalvelu (Militaire Inlichtingen- en Veiligheidsdienst, MIVD). Palveluiden toiminnasta säädetään vuoden 2017 laissa tiedustelu- ja turvallisuuspalveluista (Wet op de inlichtingen- en veiligheidsdiensten, 2017, jäljempänä Wiv-laki). Laki korvasi aiemman Wiv-lain vuodelta 2002.

Alankomaissa tiedustelulainsäädännön toimivuutta on arvioitu ja komitea on vuonna 2021 antanut useita suosituksia tiedustelulainsäädännön kehittämiseksi. Heinäkuussa 2024 tuli voimaan väliaikainen laki (Tijdelijke wet onderzoeken AIVD en MIVD naar landen met een offensief cyberprogramma, bulkdatasets en overige specifieke voorzieningen), joka mahdollistaa viranomaisille tehokkaamman toiminnan muuttuneessa turvallisuusympäristössä ja erityisesti valtiollisia kyberuhkia vastaan. Väliaikainen laki on voimassa 1.7.2028 saakka.

Wiv-laista poiketen väliaikainen laki mahdollistaa esimerkiksi yksilöimättömän tietoaineiston (bulk dataset) säilyttämisen Wiv-laissa säädettyä 18 kuukauden määräaikaa pidempään. Wiv-lain 27 artiklan 1 kohdan mukaan yksilöimättömän tietoaineiston tarpeellisuus tulee arvioida mahdollisimman pian ja viimeistään 18 kuukauden kuluessa. Tarpeeton tieto on tämän arvioinnin yhteydessä tuhottava. Väliaikaisen lain 14b ja 14ba artiklojen mukaisesti tarkistamattoman yksilöimättömän tietoaineiston säilyttämisen jatkaminen on mahdollista ministerin päätöksellä. Päätös säilyttämisen jatkamisesta voidaan tehdä vuodeksi kerrallaan, eikä kokonaisenimmäisaikaa ole säädetty. Lain 14 ba artiklan 3 kohdan mukaisesti jatkamispäätöksestä on ilmoitettava tiedustelutoimintaa valvovalle komissiolle (Commissie van Toezicht op de Inlichtingen- en Veiligheidsdiensten CTIVD).

Wiv-lain 25 artiklan 1 kohdan mukaan tiedustelupalveluilla on oikeus kerätä tietoja muun muassa yleisesti saatavilla olevista lähteistä. Tavanomaisiin toimivaltuuksiin kuuluva tiedonhankinta ei edellytä lupaa ministeriltä, eikä hyväksyntää valvontalautakunnalta (Toetsingscommissie Inzet Bevoegdheden, TIB). Ministerin lupaa ei myöskään edellytetä lain 39 artiklan mukaiseen tiedonhankintaan hallintoelimiltä, virkamiehiltä sekä muilta, joiden voidaan katsoa pystyvän toimittamaan tarvittavat tiedot. Valvontalautakunta on riippumaton elin, joka arvioi etukäteen tiedustelutoimivaltuuksien lainmukaisuutta.

Wiv-lain 45 artiklan 1 kohdan nojalla tiedustelupalveluilla on säädettyjen edellytysten täyttyessä oikeus tunkeutua automaattiseen järjestelmään joko käyttämällä teknisiä apuvälineitä, vääriä signaaleja, vääriä avaimia, väärää henkilöllisyyttä tai kolmannen osapuolen automaattisen järjestelmän kautta. Toimivaltuuden käyttäminen on luvanvaraista. Artiklan 5 kohdan mukaan kolmannen osapuolen järjestelmän hyödyntäminen ei kata teknisten laitteiden asentamista.

Ilmoitusvelvollisuus

Wiv-lain 59 artiklan mukaan viranomaisten on arvioitava viiden vuoden kuluttua tiettyjen toimenpiteiden päättymisestä ja sen jälkeen vuosittain, voidaanko toimenpiteestä ilmoittaa sille henkilöille, johon toimipide on kohdistettu. Artiklassa mainitut toimenpiteet kattavat kirjeiden avaamisen, kohdennetun viestinnän seurannan ja asunnossa käymisen. Ilmoitus voidaan kuitenkin jättää tekemättä useilla eri perusteilla, muun muassa toiminnan suojaamiseksi tai mikäli ilmoituksen tekeminen vaarantaisi kansallista turvallisuutta. Tilanteissa, joissa ilmoitusta ei voida tehdä tai sen tekeminen olisi käytännössä mahdotonta, tulee valvontakomissiolle tehdä ilmoitus ja perustella, miksi ilmoitusta ei ole voitu tehdä asianosaiselle.

5.2.4.1 Ulkomainen lainsäädäntö ja julkisuuslain muuttaminen

Yleistä

Euroopan maissa salassapitoa koskevat määräykset sisältyvät yleensä maiden julkisuuslainsäädäntöihin. Salassapitoajan pituudet ja salassapidon päättymisen periaatteet ja käytännöt vaihtelevat maittain. Vertailluissa Euroopan maissa lainsäädäntö mahdollistaa asiakirjojen salassapidon niin pitkään, kuin se on turvattavien etujen kannalta tarpeen.

Suomessa muun muassa ulkoasianhallinnon ja suojelupoliisin asiakirjat tulevat käytännössä aina julkisiksi julkisuuslain 31 §:n 2 momentin mukaisesti 25 vuoden salassapitoajan päätyttyä, ellei salassapitoa jatketa julkisuuslain 31 §:n 4 momentin mukaan valtioneuvoston päätöksellä. Vertailluissa maissa salassapidolle on määrätty yleinen enimmäiskesto, yleensä 30-50 vuotta, jonka jälkeen pidentäminen on mahdollista joko tietyn ajan tai niin kauan kuin tarpeen. Salassapitoajan pidentämisestä päättää yleensä asiakirjat laatinut viranomainen.

Eräissä maissa ulkoasiainhallinnon asiakirjat siirretään 10-30 vuoden kuluttua maan kansallisarkistoon. Salassapitoaikaa koskevia määräyksiä on sisällytetty myös maiden arkistolakeihin. Asiakirjojen ja arkistojen sijainti ministeriössä tai kansallisarkistossa ei vaikuta salassapitoaikaan. Suomessa ulkoministeriö on säilyttänyt arkistonsa arkistolain mukaisesti itsellään. Suomessa tasavallan presidentin arkiston asiakirjat on siirretty kansallisarkistoon tasavallan presidentin toimikauden päättymisen jälkeen tasavallan presidentin kanslian ja kansallisarkiston välillä sovitulla tavalla.

Norjassa julkishallinnon asiakirjojen julkisuudesta säädetään laissa *Lov om rett til innsyn i dokument i offentleg verksamhed, Offentleglova* (2006). Lain 20 §:ssä mainitaan poikkeuksena asiakirjajulkisuuteen salassapito Norjan ulkopolitiikan etujen suojaamiseksi. Lain 21 §:ssä poikkeuksena mainitaan kansallinen turvallisuus tai maanpuolustus.

Lain *Lov om nasjonal sikkerhet, Sikkerhetsloven* (2024) tietoturvallisuutta koskeva luku 5 koskee kansallisen turvallisuusedun kannalta kriittisen tiedon käsittelyä ja suojaamista. Lain 5–3 pykälässä säädetään, että ellei toisin säädetä, salassapito lakkaa olemasta voimassa 30 vuoden kuluttua asiakirjan laatimisesta. Käytännössä tiedon salassapidon tarve tarkistetaan tapauskohtaisesti ennen päätöksen tekemistä salassapidon lakkaamisesta ja salassapitoaikaa on mahdollista jatkaa esimerkiksi 10 vuodella.

Ruotsissa asiakirjojen julkisuutta ja salassapitoa säätelee *Offentlighets- och sekretesslag* (2009). Lain 15 luku käsittelee valtion turvallisuutta ja suhteita muihin valtioihin ja kansainvälisiin järjestöihin. Luvun 1 § *utrikessekretess*, ulkoasiainsalassapito, määrää salassa pidettäviksi asiakirjat, jotka koskevat Ruotsin suhteita toisiin valtioihin tai niiden viranomaisiin ja kansalaisiin sekä kansainvälisiin järjestöihin, jos tietojen paljastuminen haittaisi Ruotsin kansainvälisiä suhteita tai muuten vahingoittaisi maata. Salassapito kestää enintään 40 vuotta. Hallitus voi kuitenkin erityisistä syistä antaa määräyksiä, joiden mukaan salassapito on voimassa pidempään.

Lakiin on myöhemmin lisätty lainkohdat EU- ja Nato-yhteistyössä käsiteltävien asiakirjojen salassapidosta. Naton osalta salassapitoajan enimmäismäärä on viisikymmentä vuotta, jota hallitus voi erityisistä syistä pidentää. Nato-lisäys tuli voimaan 1.1.2026.

Edellä mainitun 15 luvun 2 § (Försvarssekretess) koskee salassapitoa maanpuolustukseen liittyen. Salassapito kestää enintään 40 vuotta, mutta hallitus voi erityisistä syistä antaa määräyksiä pidemmästä salassapitoajasta.

Tanskassa asiakirjojen yleistä saatavuutta säätelevät hallinnon avoimuuslaki *Lov om offentlighed i forvaltningen* (2013) ja arkistolaki *Arkivloven* (2002). Hallinnon avoimuuslain mukaan oikeutta tutustua asiakirjoihin voidaan rajoittaa Tanskan ulkopoliittisten etujen vuoksi. Arkistolain mukaan viranomainen voi asettaa arkistoon siirrettyjen asiakirjojen osalta pidemmän, enintään 60 vuoden salassapitoajan.

Virossa *State Secrets and Classified Information of Foreign States Act* (2007) lain mukaan Viron ulkoasiainhallinnon käsittelemät asiakirjat ovat salassapidettäviä enintään 50 vuotta, jos

niiden tuleminen julkiseksi vahingoittaisi merkittävästi maan ulkosuhteita. Salassapitoa voidaan pidentää aina viidellä vuodella, kuitenkin enintään yhteensä 75 vuoteen. Päätöksen pidentämisestä tekee ministeri

State Secrets and Classified Information of Foreign States Act (2007) lain mukaan maanpuolustukseen liittyvien tietojen salassapitoaika vaihtelee 10 vuodesta 50 vuoteen. Lain mukaan turvallisuusviranomaisten (9 § State secrets related to security authorities) toiminnan osalta salssapitoaika on pääsääntöisesti 50 vuotta ja pisin 75 vuotta.

Latvia. Laki *On Official Secret* (1996) määrää korkeimmille turvallisuusluokille seuraavat yleiset salassapitoajat: Luottamuksellinen viisi vuotta, Salainen kymmenen vuotta ja Erittäin salainen kaksikymmentä vuotta. Ennen salassapidon määräajan päättymistä on viranomaisen tehtävä päätös salassapidon lopettamisesta tai tarvittaessa jatkettava salassapitoa.

Jos ulkopoliittisten tietojen paljastaminen voi vahingoittaa valtion etuja tai yleistä etua tai yksityishenkilöiden oikeuksia ja oikeudellisia etuja, ulkoministeriö voi lain *Diplomatic and Consular Service Law* (1995) perusteella pidentää salassapitoa. Tällä hetkellä ulkopoliittisten salassapidettävien asiakirjojen salassapitoaika Latviassa on 40 vuotta.

Isossa-Britanniassa laki *Freedom of Information Act 2000* määrää salassapidettäväksi asiakirjat, jotka koskevat Ison-Britannian suhteita toisiin valtioihin tai kansainvälisiin järjestöihin, jos niiden julkiseksi tulo vahingoittaisi tai todennäköisesti vahingoittaisi Ison-Britannian etuja. Asiakirjojen salassapito edellyttää aina mahdollisen vahingon arviointia. Kansalliseen turvallisuuteen, kansainvälisiin suhteisiin ja puolustukseen liittyvien salassapidettävien tietojen salassapitoajalle ei ole määritelty loppumisaikaa. Asiakirjojen salassapito jatkuu tarvittavan ajan.

Ranskan Code du Patrimoine -laissa määrätään poikkeukset ja salassapitoajat arkistoissa olevien asiakirjojen yleiseen julkisuuteen (artikla L 213-2). Lain mukaan asiakirjat, joiden julkiseksi tuleminen haittaisi Ranskan suhteita muihin valtioihin ja Ranskan ulkopolitiikan etuja ovat salassa pidettäviä 25 vuotta. Jos vahingon kohteena olisivat perustavanlaatuiset edut, salassapitoaika olisi 50 vuotta

Saksassa Liittovaltion arkistolaki, *Bundesarchivgesetz,* määrää arkistoon siirrettyjen asiakirjojen yleiseksi salassapitoajaksi 30 vuotta. Arkistot siirtäneen viranomaisen suostumuksella voidaan salassapitoaikaa pidentää arkistolain perusteella enintään 30 vuotta. Eräissä tapauksissa salassapitoajan pidentäminen 30 vuotta pidemmäksi on mahdollista *(VSA - Verschlusssachen-Anweisung).*

6 Lausuntopalaute

Sisäministeriö pyysi hallituksen esitysluonnoksesta lausunnot xxx-xxx välisenä aikana. Lausuntopyyntö julkaistiin lausuntopalvelu.fi-sivustolla.

Lausunto saatiin xx taholta/lausunnon antoivat xx. Lausunnot ovat luettavissa hankkeen verkkosivuilla osoitteessa: https://xxx. Lausunnot ja lausuntoyhteenveto ovat luettavissa myös sisäministeriön verkkosivuilla osoitteessa https://intermin.fi/hankkeet hankenumerolla SM040:00/2024.

xxx (lausuntopalaute)

7 Säännöskohtaiset perustelut

7.1 Poliisilaki

5 a luku

2 §. *Tiedustelumenetelmät siviilitiedustelussa***.** Poliisilain 5 a luvun 2 §:ssä säädetään tiedustelumenetelmistä siviilitiedustelussa. Säännökseen lisättäisiin kaksi uutta tiedustelumenetelmää, jotka olisivat valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu ja yksinomaan tietoverkossa toteutettava peitetoiminta.

Uusien toimivaltuuksien vuoksi pykälän *2 momentin* tiedustelumenetelmät luettelevaan listaan lisättäisiin valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu ja yksinomaan tietoverkossa toteutettava peitetoiminta. Muita momentissa mainittuja tiedustelumenetelmiä ovat 5 a luvussa tarkoitetut paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten.

Pykälän *3 momenttia täydennettäisiin* valtiolliseen toimijaan kohdistuvalla tietojärjestelmätiedustelulla ja yksinomaan tietoverkossa toteutettavalla peitetoiminnalla.

4 §. *Tiedustelumenetelmien käytön edellytykset.* Pykälässä säädetään tiedustelumenetelmien käytön yleisestä ja eräistä muista edellytyksistä. Pykälään lisättäisiin valtiollisen toimijan määritelmä uuteen 6 momenttiin. Nykyinen 6 momentti siirtyisi 7 momentiksi.

Valtiollisella toimijalla tarkoitettaisiin vieraan valtion tunnistettua viranomaista tai sellaiseen rinnastuvaa toimijaa sekä tarkoitetun tahon palveluksessa olevaa tai sen määräyksessä ja ohjauksessa toimivaa tahoa. Määritelmässä tarkoitetulla toimijalla ja taholla viitataan uhkatoimijaan, joka toiminnallaan uhkaa kansallista turvallisuutta. Määritelmä on vastaava kuin tietoliikennetiedustelusta siviilitiedustelussa annetun lain 2 §:n 6 kohdan määritelmä. Poliisilain 5 a luvussa ei ole säädöstä määritelmille, mutta luvussa toistuva valtiollinen tai siihen rinnastuva taho on kuitenkin selvyyden vuoksi tarkoituksenmukaista määritellä samalla tavalla kuin tietoliikennetiedustelussa.

6 §. *Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättäminen*. Poliisilain 5 a luvun 6 §:n 1 momentissa säädetään siitä, että tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta siviilitiedustelussa suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Pykälän *1 momenttia* täydennettäisiin säätämällä telekuuntelua ja sen sijasta tapahtuvan tietojen hankkimisen kiirepäätösmenettelystä. Telekuuntelun ja sen sijasta tapahtuvan tietojen hankkimisen kiiretilanteen päätöksentekomenettelystä säädettäisiin samalla tavalla kuin siitä on säädetty tukiasematietojen hankkimiseen, tekniseen kuunteluun ja katseluun, tekniseen seurantaan, tekniseen laitetarkkailuun, paikkatiedusteluun, jäljentämiseen ja tietoliikennetiedustelusta päättämiseen liittyvästä päättämisestä. Pykäläehdotuksen mukaan, jos telekuuntelua tai tietojen hankkimista telekuuntelun sijasta koskeva asia ei sietäisi viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saisi päättää telekuuntelusta tai tietojen hankkimisesta telekuuntelun sijasta siihen asti, kunnes tuomioistuin olisi ratkaissut luvan myöntämistä koskevan vaatimuksen. Asia

olisi saatettava tuomioistuimen ratkaistavaksi heti, kun se olisi mahdollista, ja viimeistään 24 tunnin kuluttua menetelmän käytön aloittamisesta.

Tarve kiirepäätösmenettelyyn telekuuntelussa on jopa suurempi kuin eräissä muissa siviilitiedustelumenetelmissä. Poliisilain 5 a luvun 3 §:n mukaan suojelupoliisin tehtävänä on siviilitiedustelun keinoin hankkia tietoa muun muassa yhteiskunnan elintärkeisiin toimintoihin kohdistuvista vakavista uhkista ja ulkomaisesta tiedustelutoiminnasta. Telekuuntelu on yksi niistä keskeisistä menetelmistä, joilla voidaan hankkia tiedustelutietoa Suomeen kohdistuvasta kyberympäristössä tapahtuvasta vakoilusta ja muusta Suomea vaarantavasta valtiollisesta kybertoiminnasta. Suomeen kohdistuvassa kybervakoilussa hyödynnetään toistensa kanssa kommunikoivien laitteiden ketjuja, jotka muuttuvat hyvinkin nopeasti. Ketjutuksessa tapahtuvien nopeiden muutosten takia, tuomioistuimelta saattaa olla mahdotonta saada lupaa telekuunteluun sen aikaikkunan puitteissa, jolloin telekuuntelu pitäisi voida toteuttaa. Suojelupoliisin päällystöön kuuluvan poliisimiehen tulisi näissä tapauksissa voida tehdä telekuuntelua koskeva kiirepäätös, jonka lainmukaisuus jälkikäteen saatettaisiin tuomioistuimen arvioitavaksi.

14 §. *Teknisestä laitetarkkailusta siviilitiedustelussa päättäminen.* Pykälän 3 momentissa säädetään siitä, mitä teknistä laitetarkkailua koskevassa vaatimuksessa ja tuomioistuimen päätöksessä on mainittava. Poliisilain 5 a luvun 14 §:n 3 momentin 2 kohtaa ehdotetaan muutettavaksi siten, että tekninen laitetarkkailu voitaisiin kohdistaa teknisen laitteen ja ohjelmiston lisäksi myös teknistä laitetta tai ohjelmistoa käyttävään henkilöön. Voimassa olevan lainkohdan mukaan vaatimuksessa ja päätöksessä on mainittava toimenpiteen kohteena oleva tekninen laite tai ohjelmisto. Kyse olisi vastaavan kaltaisesta ratkaisusta kuin mitä säädetään poliisilain 5 a luvun 6 §:ssä telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättämisestä ja 7 §:ssä televalvonnasta siviilitiedustelussa päättämisestä. Sekä telekuuntelu että televalvonta voidaan kohdistaa joko henkilöön, teleosoitteeseen tai telepäätelaitteeseen.

Kun teknisen laitetarkkailun lupa kohdistuisi henkilöön, lupa käsittäisi luvan kohteena olevan henkilön hallussa olevan tai hänen oletettavasti muuten käyttämän laitteen tai ohjelmiston. Teknisen laitetarkkailun lupa ei olisi laite- tai ohjelmistokohtainen, vaan lupa käsittäisi kaikki luvan kohteena olevan henkilön hallussa olevat ja käyttämät laitteet ja ohjelmistot. Luvan hakijan tulisi pystyä osoittamaan perusteet sille, että tietty laite tai ohjelmisto on luvan kohteena olevan henkilön käyttämä tai että henkilö oletettavasti muuten käyttää näitä.

Laitteen yksilöinti reaalimaailmassa on haastavaa. Tiedustelun lähtötilanteessa voi esimerkiksi olla tiedossa kansallisen turvallisuuden uhkaan liittyvä yksilöity henkilö, mutta ei yksilöityjä laitteita. Kohdehenkilöllä havaitaan olevan käytössään laitteita, esimerkiksi tietokoneita, älykelloja tai massamuisteja, mutta niiden teknisen laitetarkkailun edellyttämät yksilöivät tiedot eivät ole tiedossa. Laitteista saatavan yksilöintitiedon hankkiminen edellyttäisi laitteen haltuun saamista, mikä ei käytännössä ole mahdollista. Laitteiden yksilöinti olisi ehdotetun pykälämuutoksen jälkeen mahdollista myös kohdehenkilön kautta. Tuomioistuimen siviilitiedustelun kohteeksi hyväksymän yksittäisen teknisen laitteen takaa paljastuu säännönmukaisesti kymmeniä tai jopa satoja muita laitteita, jolloin tiedonhankinnan eteneminen parantuisi, koska se voisi perustua myös teknistä laitetta tai ohjelmistoa käyttävään henkilöön eikä lukuisiin, toistuvasti eri laitteisiin tai ohjelmistoihin haettaviin tuomioistuimen lupiin kohdehenkilön vaihtaessa laitteita.

14 a §. *Valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelu.* Pykälä olisi uusi. Pykälässä säädettäisiin tietojärjestelmätiedustelun toimivaltuudesta, jonka avulla saataisiin hankkia tietoteknisin menetelmin tietoa valtiollisen toimijan tai siihen rinnastuvan tahon kansallista turvallisuutta vakavasti uhkaavaan toimintaan käyttämän tietojärjestelmän toiminnasta, sen

sisältämistä tiedoista, tietojärjestelmän osien välillä liikkuvista viesteistä sekä tietojärjestelmään saapuvista tai siitä lähtevistä viesteistä. Tiedustelu mahdollistettaisiin laite- ja järjestelmäketjuihin.

Ehdotettu toimivaltuus mahdollistaisi tiedustelun kohdistamisen esimerkiksi seuraavasti määriteltyihin tietojärjestelmiin tai niiden osiin:

- kyberuhkatoimijan rakentama ja käyttämä tietoverkkoinfrastruktuuri siihen kuuluvine palvelimineen, kaapattuine laitteineen ja tietoliikenneyhteyksineen;
- tietty käyttäjätili Internetin tiedostonjakopalvelussa;
- tietyn henkilöryhmän tai organisaation yksityiskäytössä oleva viestintäpalvelu;
- päätelaite niine tietoineen, jotka se on eri sovellusten kautta tallentanut Internetin pilvipalveluun;
- palveluntarjoajan virtualisoituna ylläpitämä tietty palvelin ja sen tietosisältö, mutta ei muut samassa fyysisessä palvelimessa sijaitsevat tietosisällöt, jotka ovat muiden toimijoiden hallinnassa;
- abstraktit tietovarannot kuten tietyt virtuaalivaluuttatransaktiot.

Pykälän 1 momentin mukaan valtiolliseen toimijaan kohdistuvalla tietojärjestelmätiedustelulla tarkoitettaisiin tiedonhankintaa valtiollisen tai siihen rinnastuvan tahon käyttämien tietojenkäsittelylaitteiden, tiedonsiirtolaitteiden ja tietoja käsittelevien ohjelmistojen muodostaman yhteen toimivan kokonaisuuden siitä osasta, joka toteuttaa tai edesauttaa siviilitiedustelun kohteena olevaa toimintaa tai joka tallentaa tai välittää siviilitiedustelun kohteena olevaan toimintaan liittyviä tietoja.

Ehdotetun 2 momentin mukaan valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua saisi käyttää vain siinä laajuudessa kuin se on välttämätöntä tiedon hankkimiseksi poliisilain 5 a luvun 3 §:ssä tarkoitetusta toiminnasta. Mainitun luvun 3 §:ssä säädetään siviilitiedustelun kohteista.

Valtiollinen toimija tai siihen rinnastuva taho määriteltäisiin poliisilain 5 a luvun 4 §:ssä vastaavasti kuin laissa tietoliikennetiedustelusta siviilitiedustelussa.

Tietojärjestelmällä tarkoitettaisiin tietojenkäsittelylaitteista, tiedonsiirtolaitteista, tietoa käsittelevistä ohjelmista ja tietojen käsittelysäännöistä muodostuvaa kokonaisuutta. Tietojärjestelmä voi muodostua useiden eri laitteiden ja ohjelmistojen tai näiden osien muodostamasta maantieteellisesti ja loogisesti hajautetusta kokonaisuudesta. Tietojärjestelmä voi kattaa osia, esimerkiksi laitteita tai ohjelmia, jotka kuuluvat samanaikaisesti johonkin toiseen tietojärjestelmään. Tietojärjestelmätiedustelu kohdistuisi toistensa kanssa tietyssä kansallista turvallisuutta uhkaavassa tarkoituksessa kommunikoivien laitteiden ja virtuaalisten järjestelmien muodostamaan loogiseen kokonaisuuteen, jolloin lupaa ei edellytettäisi vaadittavan erikseen jokaiseen sellaiseen tietoa käsittelevään tai siirtävään laitteeseen, ohjelmistoon tai tietojenkäsittelysäännöstöön, joka kuuluu kokonaisuuteen.

Tietojärjestelmätiedustelu sisältäisi teknisesti telekuuntelua ja televalvontaa vastaavat menetelmät, joilla saataisiin hankkia tietoa kulussa olevasta viestistä. Tämä mahdollistaisi tietojärjestelmien sisäisen liikenteen tarkastelun. Tällaista sisäistä liikennettä ovat esimerkiksi tekninen viestinvaihto käyttöliittymän ja sen taustalla toimivan tiedontallennusalustan välillä sekä viestiliikenne tietojärjestelmän eri käyttäjien välillä. Tietojärjestelmän osien välisen teknisen kontrolliliikenteen tarkkailu mahdollistaisi myös kokonaiskuvan luomisen tietojärjestelmän sisäisestä toiminnasta, sen sisältämistä tiedoista ja täten sen muodostamasta uhkasta.

Tiedon hankkiminen tietojärjestelmään saapuvasta tai siitä lähtevästä viestistä puolestaan mahdollistaisi tiedustelun tietojärjestelmän toimintaan suhteessa sen kyberympäristöön, eli esimerkiksi siihen, miten tietojärjestelmä toteuttaa uhkatoimijan käskyjä tai millaisen uhkan se muutoin muodostaa.

Moniosaisissa tietojärjestelmissä sen osien välillä kulkeva tietoliikenne saattaa olla väliaikaisesti tallennettuna järjestelmän eri laitteisiin tai sitä voidaan synkronisoida eri laitteiden välillä. Rajanveto tallennetun tiedon, josta tieto hankittaisiin nykyisellään teknisellä laitetarkkailulla – ja kulussa olevan viestiliikenteen – josta tieto hankittaisiin telekuuntelulla – välillä on käytännössä usein häilyvä, jolloin telekuuntelun mukaisen sääntelyn soveltaminen on hankalaa. Tietojärjestelmät saattavat myös muodostaa sisäisiä tietoliikenneverkkoja, joiden ei voida ajatella olevan liitettyjä yleiseen viestintäverkkoon. Tällöin telekuuntelumenetelmän käyttö ei tule kysymykseen, vaan kyse on eri tiedustelumenetelmien välisen nykyisen rajanvedon näkökulmasta teknisestä kuuntelusta.

Tietojärjestelmätiedustelun kohdistaminen poikkeaisi siis nykyisen teknisen laitetarkkailun kohdistamisesta siinä, että kohdelaitteiden, -ohjelmien ja -käsittelysääntöjen muodostama kokonaisuus määritellään ensisijaisesti niiden kansalliseen turvallisuuteen kohdistuvaan uhkaan liittyvän toiminnallisuuksien perusteella eikä niiden fyysisen sijainnin, verkko-osoitteen tai muun sellaisen yksilöivän ominaisuuden, jolla ei tosiasiassa ole yksi-yhteen vastaavuutta uhkatoimintaan.

Jonkin tietojärjestelmän komponentin, esimerkiksi laitteen tai tietoverkkoyhteyden, osallistuminen tietojärjestelmätiedustelun kohteena olevan tietojärjestelmän toteuttamiseen ei tarkoittaisi sitä, että suojelupoliisilla olisi oikeus hankkia tietoa kaikesta sen sisältämästä tai siirtämistä tiedoista, vaan oikeus hankkia tietoa koskisi vain sitä osaa tallennetusta tai siirrettävästä tiedosta, joka tosiasiallisesti toteuttaa kohteena olevan tietojärjestelmän toimintaa. Menetelmän kohteena olevan tietojärjestelmän rajauksessa olisi kiinnitettävä huomiota siihen, miten kyseessä oleva valtiollinen toimija kykenee hallinnoimaan tai tietojenkäsittelysäännöillä ohjaamaan tietojärjestelmää taikka muilla toimin vaikuttamaan tietojärjestelmän sisältämään tai välittämään tietoon. Lähtökohtaisesti valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu kohdistuu sellaisiin tietojärjestelmiin, joiden käyttäjät ovat valtiollisia toimijoita tai siihen rinnastuvia tahoja tai joita hallinnoi tai joiden toimintaa muutoin ohjaa valtiollinen toimija tai siihen rinnastuva taho.

Esimerkiksi tietojärjestelmätiedustelun kohdistaminen tietyn valtiollisen organisaation sähköpostijärjestelmään tarkoittaisi, että organisaation sähköpostien sisällöstä, sähköpostiliikenteestä sekä teknisistä toteutustavoista voisi hankkia tietoa kaikilta niiltä laitteilta ja tietoverkoista, jotka toteuttavat organisaation sähköpostien välitystä ja tallentamista. Siinä tapauksessa, että nämä laitteet tai tietoverkot toteuttavat myös muiden henkilöiden tai organisaatioiden sähköpostiliikenteen välitystä tai tallentamista, eli osallistuvat muiden organisaatioiden sähköpostijärjestelmien toteuttamiseen, ei oikeutta hankkia tietoa olisi koko laitteen sisällöstä tai tietoverkon liikenteestä vaan ainoastaan niistä osista, joka toteuttavat tiedonhankinnan kohteena olevan organisaation sähköpostijärjestelmää.

Toisena esimerkkinä valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun tarkoittamasta tietojärjestelmästä voisi olla kaupallisen kolmannen osapuolen tarjoama pikaviestinalustan suljettu keskusteluryhmä, jota valtiollinen toimija käyttää viestinnässään. Tällöin menetelmän kohteena olisi tietojärjestelmä, johon kuuluu pikaviestimen toimintaa toteuttavat ohjelmistot ja laitteistot siltä osin kuin niille on säilöttynä tietoa keskusteluryhmän toiminnasta ja sen viestinnän sisällöstä.

Tietojärjestelmätiedustelua koskevassa vaatimuksessa ja päätöksessä olisi tehtävä muiden seikkojen ohella selkoa toimenpiteen kohteena olevan tietojärjestelmän rajauksesta perustuen kuvaukseen tietojärjestelmän toiminnasta, sen tietojenkäsittelysäännöistä, siihen kuuluvien laitteiden tai ohjelmien tunnisteista tai niiden roolista osana tietojärjestelmää, sen käyttämistä teleosoitteista, sen käyttäjien teleosoitteista tai muista käyttäjätiedoista tai jostakin näiden yhdistelmistä siten, että tiedon hankinta voidaan kuvauksen perusteella teknisesti rajata. Kuvauksesta tietojärjestelmän toiminnasta tulisi ilmetä, millä tavalla valtiollisen toimijan oletetaan käyttävän kohteena olevaa tietojärjestelmää kansallista turvallisuutta uhkaavaan toimintaan. Päätöksenteosta ehdotetaan säädettäväksi 14 b §:ssä.

Tietojärjestelmätiedustelua ei lisättäisi tiedustelumenetelmän käytöstä ilmoittamista koskevaan poliisilain 5 a luvun 47§:ään, koska sen kohteena on valtiollinen toimija tai siihen rinnastuva taho.

Ehdotetut muutokset mahdollistaisivat suojelupoliisille tietojärjestelmien toiminnan ennakoivamman tiedustelun ja uhkien tunnistamisen. Ne mahdollistaisivat sen, että suojelupoliisi pystyisi tunnistetuissa tietojärjestelmissä etsimään hankittavaa tietoa sekä tunnistamaan uusia tietojärjestelmiä, jotka muodostavat uhkan kansalliselle turvallisuudelle.

14 b §. *Valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta päättäminen*. Pykälä olisi uusi.

Pykälässä säädettäisiin valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta päättämisestä. Tietojärjestelmätiedustelun kohteena oleva tietojärjestelmä tulisi sitä koskevassa päätöksessä rajata sellaiseksi kokonaisuudeksi, joka toteuttaa joitakin tiettyjä toiminnallisuuksia tai joka muutoin voidaan määrittää omaksi tietojärjestelmän osaksi perustuen tietojärjestelmän käyttäjään tai tietojärjestelmän osan perustellusti oletettuun tietosisältöön. Edellä mainittujen toiminnallisuuksien, käyttäjien tai tietosisältöjen tulisi liittyä kansallista turvallisuutta vakavasti uhkaavaan toimintaan.

Pykälän 1 momentin mukaan tuomioistuin päättäisi valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta siviilitiedustelussa tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Vaatimuksen käsittelystä tuomioistuimessa säädetään poliisilain 5 a luvun 35 §:ssä. Päätöksentekotaso vastaisi siviilitiedustelun telekuuntelun tasoa.

Tietojärjestelmätiedustelusta ulkomailla päättäisi sotilastiedustelulain 63 §:ää mukaillen sekä poliisilain 5 a luvun 39 §:n mukaisesti suojelupoliisin päällikkö. Tietojärjestelmätiedustelusta kotimaassa päättäisi tuomioistuin. Tuomioistuimen myöntämän luvan tulisi koskea tietojärjestelmää, jolloin yksittäisen teleosoitteen, tiedonkäsittelylaitteen, tiedonsiirtolaitteen tai tietoa käsittelevän ohjelman ja tietojen käsittelysäännön kuulumisesta kohteena olevaan tietojärjestelmään päättäisi tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Päällystöön kuuluvan poliisimiehen päätösten tulisi olla perusteltuja ja niihin tulisi kohdistaa laillisuusvalvontaa.

Pykälän 2 momentin mukaan lupa valtiolliseen toimijaan kohdistuvaan tietojärjestelmätiedusteluun voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Kuuden kuukauden lupa-aika on perusteltu siviilitiedustelun luonteen ja tiedustelumenetelmien käytön perusteen vuoksi ja yhtä pitkä enimmäislupa-aika on tyypillinen tiedustelumenetelmien kohdalla. Tiedustelu on pitkäkestoista tiedonhankintaa kohdevaltion Suomen etuja vahingoittavasta toiminnasta ja siihen liittyvistä seikoista. 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 3 momentissa säädettäisiin vaatimukseen ja päätökseen sisällytettävistä tiedoista. Momentin 1 kohdan mukaan vaatimukseen ja päätökseen tulisi sisällyttää 5 a luvun 3 §:ssä tarkoitettu toiminta, joka vakavasti uhkaa kansallista turvallisuutta. Vähintään yhden 3 §:ssä tarkoitetuista kohdista tulisi olla mainittuna tiedustelumenetelmän käytön perusteena.

Momentin 2 kohdassa säädettäisiin edellytyksestä sisällyttää vaatimukseen ja päätökseen toimenpiteen kohteena oleva valtiollinen tai siihen rinnastuva taho ja kuvaus sen käyttämästä tietojärjestelmästä.

Momentin 3 kohdan mukaan vaatimukseen ja päätökseen tulee sisällyttää tosiseikat, joihin valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun 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 valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella.

Momentin 5 kohdan mukaan vaatimuksessa ja päätöksessä olisi mainittava valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Momentin 6 kohdan mukaan vaatimukseen tai päätökseen tulisi sisällyttää mahdolliset valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun rajoitukset ja ehdot. Tuomioistuin voisi asettaa päätöksessään toimivaltuudelle rajoituksia ja käyttöehtoja. Jos tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, ne olisi kirjattava siihen.

16 §. *Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa***.** Poliisilain 5 a luvun 16 §:n *1 momenttia* ehdotetaan muutettavaksi siten, että momenttiin lisättäisiin valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelu, johon voimassa olevassa pykälässä lueteltujen tiedustelumenetelmien lisäksi liittyy tarve laitteen, menetelmän tai ohjelmiston asentamiseen ja poisottamiseen sen käytön toteuttamiseksi. Lisäksi ensimmäistä virkettä muutettaisiin siten, että laite, menetelmä tai ohjelmisto voitaisiin sijoittaa mihin tahansa esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan tai tietojärjestelmään, jos käytetty tiedustelumenetelmän toteuttaminen sitä edellyttää. Voimassa olevan momentin sanamuodon mukaan laitteen, menetelmän tai ohjelmiston voisi sijoittaa vain toimenpiteen kohteena olevaan esineeseen, aineeseen tai omaisuuteen. Nykyisissä tietoverkkoympäristöissä on hyvin tyypillistä, että kohteena oleva laite tai ohjelmisto ei ole tietoverkossa saavutettavissa suoraan, vaan se liikennöi muiden laitteiden ja ohjelmistojen kautta. Nämä muut laitteet ja ohjelmistot ovat toiminnoiltaan esimerkiksi tietoliikennettä välittäviä (reitittimiä, välityspalvelimia, yms.) tai

tietoturvaa parantavia (palomuureja, tunnistautumispalveluita, yms.). Jos kohteena oleva laite, ohjelmisto tai tietojärjestelmä ei ole savutettavissa suoraan esimerkiksi fyysisen saavutettavuuden avulla, ei myöskään nykysääntelyn asentamistoimivaltuutta voida hyödyntää. Hyödyntämisvaikeus ilmenee yhtä lailla kohdistettaessa tiedonhankintaa kyberuhkatoimijoiden tarkoituksella peittelytarkoituksessa ketjuttamiin laitteisiin ja ohjelmistoihin kuin silloinkin, kun tiedonhankintaa kohdistetaan sellaisiin valtiollisiin organisaatioihin, joilla on edistyneet tekniset kyvyt suojata omia tietojärjestelmiään.

Pykälään lisättäisiin *2 momentti*, jonka mukaan suojelupoliisin pyynnöstä viranomaisen ulkopuolisella henkilöllä olisi oikeus suojelupoliisin päällystöön kuuluvan poliisimiehen ohjeiden mukaisesti ja valvonnassa toteuttaa tiedustelumenetelmän käytön edellyttämä yksittäinen asennus- tai poistamistoimenpide. Kyse ei olisi avustamisvelvollisuudesta, ja pyynnön vastaanottajalla olisi oikeus kieltäytyä. Pyynnön esittäjä ei saisi käyttää taivuttelua tai muuta johdattelua, jotta vastaus olisi halutunlainen. Tarkoituksenmukaista olisi, että suojelupoliisi tuo esiin suostumusperusteisuuden, mutta johtopäätösten tekeminen keinon käytöstä olisi jätettävä asianomaiselle henkilölle. Avustajalle olisi myös tuotava ilmi hänelle mahdollisesti aiheutuvat seuraamukset, kuten mahdollisuus työpaikan menettämiseen. Myönteisen vastauksen olisi oltava vapaaehtoisesti annettu ennen toimenpiteeseen ryhtymistä ja niin, että pyynnön vastaanottaja on ymmärtänyt sen merkityksen Lisäys kuitenkin mahdollistaisi yksityisen henkilön avustaa suojelupoliisia tiedustelumenetelmän käytön edellyttämän asennustoimenpiteen toteuttamisessa. Käytännössä suojelupoliisin pyyntö kohdistuisi sellaiseen henkilöön, jolla on luonnollinen pääsy siihen esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan tai tietojärjestelmään, johon laite, menetelmä tai ohjelmisto on tarpeen sijoittaa. Kyse olisi esimerkiksi sellaisen tietojärjestelmän käyttäjästä, johon teknisen laitetarkkailun toteuttamisen mahdollistava ohjelmisto on tarve asentaa. Selvää kuitenkin on, että suojelupoliisin olisi lähtökohtaisesti tehtävä 1 momentissa tarkoitetut toimenpiteet itsenäisesti ja ainoastaan välttämättömissä tapauksissa voisi tukeutua ulkopuolisen tahon apuun. Ulkopuolisen henkilön oikeus koskee ainoastaan tiedustelumenetelmän käyttämiseksi tarvittavia asennus- ja poistamistoimenpiteitä, eikä varsinaista tiedustelumenetelmän käyttöä.

Avustamisoikeudesta säätäminen on tarpeen erityisesti, kun kyse olisi laitteen, menetelmän tai ohjelmiston sijoittamisesta sellaisiin teknisesti hyvin suojattuihin tietojärjestelmiin, joita hyödynnetään kansallista turvallisuutta vakavasti uhkaavaan toimintaan tai jotka sisältävät sellaista uhkaa koskevaa tärkeää tietoa. Tällaisten tietojärjestelmien suojauksen kiertäminen tai purkaminen ulkopuolelta tapahtuvien toimenpiteiden avulla voi olla erittäin vaikeaa tai mahdotonta. Tietojärjestelmien ja tilojen tekninen valvonta ja turvallisuusmekanismit parantuvat koko ajan, etenkin erilaisten uhkatoimijoiden piirissä. Tällaisia uhkatoimijoita ovat paitsi valtiolliset tahot myös ei-valtiolliset uhkatoimijat. Jälkimmäisten mahdollisuus teknisin suojauksin piilottaa kansalliselle turvallisuudessa vaaraa aiheuttavaa toimintaansa parantuu jatkuvasti, sillä kaupallisten tai muutoin yleisölle saataville saatettujen kommunikointivälineiden ja tiedontallennusalustojen suojauskeinojen käyttäminen vaatii yhä vähenevässä määrin erikoisosaamista käyttäjiltään. Esimerkiksi salausmenetelmät ovat yleistyneet niin, että jokaisella Internet-käyttäjällä on ilman teknistä osaamista käytössään sellaiset salausmenetelmät, jotka vielä 30 vuotta sitten olivat ainoastaan kaikkein suurimpien valtiollisten toimijoiden käytettävissä.

Fyysisessä ympäristöissä tilojen valvontaan käytettävät tekniset ratkaisut ovat vastaavasti teknologialtaan kehittyneet nopeaa vauhtia ja toisaalta tulleet enenevässä määrin myös ei-valtiollisten ja yksittäisten kevyestikin resursoitujen toimijoiden saataville. Ehdotetulla muutoksella parannettaisiin suojelupoliisin mahdollisuutta kohdistaa tiedonhankintaa myös teknisesti hyvin suojattuihin kohteisiin sekä kohteisiin, joihin ei voida tehdä tiedonhankinnan edellytyksenä olevaa asennusta yleisten tietoverkkojen kautta. Tällaisissa kohteissa luonnollisen pääsyn omaava henkilö saattaa olla ainoa linkki, jonka kautta tietoa on teknisesti hankittavissa. Luonnollisen

pääsyn omaava henkilö ei välttämättä pysty toimimaan tietolähteenä, sillä pääsystä huolimatta hänellä ei välttämättä ole itsellään tietoa siitä asiasta, josta suojelupoliisi haluaisi hankkia tietoa.

Selvää on, että toimenpiteen olisi perustuttava viranomaisen asianmukaisesti tekemään tiedustelumenetelmän käyttöpäätökseen. Säännöksen nojalla suojelupoliisi ei voisi pyytää henkilöä asentelemaan summittaisesti pykälässä tarkoitettuja laitteita, menetelmiä tai ohjelmistoja oletuksella, että ne voisivat joskus tulla käytettäviksi.

Pykälään lisättäisiin *3 momentti*, jonka mukaan suojelupoliisilla olisi oikeus menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja tiedonsiirtämiseksi tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmää, jos se olisi välttämätöntä tiedustelumenetelmän käyttämiseksi. Suojelupoliisi ei saisi aiheuttaa vähäistä suurempaa haittaa tai vahinkoa käytettävälle laitteelle tai tietojärjestelmälle.

Säännöksen mukainen toiminta edellyttäisi välttämättömyyttä. Tässä tapauksessa kyse olisi sen arvioimisesta, voisiko suojelupoliisi päästä haluamaansa tavoitteeseen omin toimin käyttämättä ulkopuolisia laitteita tai tietojärjestelmiä. Mikäli omat toimet olisivat mahdottomia tai vaatisivat poikkeuksellisen paljon resursseja, täyttyisi säännöksessä tarkoitettu välttämättömyys.

Säännöksessä viitattu tilapäisyys tarkoittaisi sitä, että menetelmän tai ohjelmiston asentamisessa ja poisottamisessa ja tiedon siirtämisessä ei voitaisi käyttää vakituisesti samoja laitteita ja tietojärjestelmiä. Tarkoituksen mukaista myös operatiivisesta näkökulmasta on, että mahdollisuuksien mukaan menetelmä tai ohjelmisto ujutetaan kohteeseen useita eri reittejä samanaikaisesti käyttäen.

Säännöksen mukaisesti toiminnassa ei saisi aiheuttaa vähäistä suurempaa haittaa käytettävälle laitteelle tai tietojärjestelmälle. Säännöksen tarkoittamassa toiminnassa on kyse ennen kaikkea tietoliikenteen välittämisestä menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja toisaalta tiedonsiirtämisestä kohde laitteesta tai järjestelmästä tiedustelulle. Näin ollen tarpeellisessa vähäisessä haitassa olisi kyse lähinnä hetkellisestä tietoliikenneliittymän käytön lisääntymisestä ja tätä kautta liittymän haltijan käyttämien sähköisten palveluiden mahdollisesta hetkellisestä hidastumisesta. Ulkopuolisen tietojärjestelmän käyttö voisi näkyä järjestelmän käytön tilapäisenä hetkellisenä kasvuna.

Mikäli vastoin edellä kuvattua, säännöksen toiminnasta aiheutuisi tarpeetonta haittaa, olisi suojelupoliisi velvollinen korvaamaan vahingon ja haitan. Toiminnan luonteen takia henkilö tai yhteisö, jonka laitetta tai tietojärjestelmää käytetään, ei saa tietoa suojelupoliisin toiminnasta. Toisaalta lähtökohtaisesti henkilön tai yhteisön ei pitäisi tällaista edes havaita. Jos henkilö tai yhteisö epäilisi, että laitetta tai tietojärjestelmää olisi käytetty säännöksessä tarkoitetulla tavalla ja taholle olisi aiheutunut vähäistä suurempaa haittaa suojelupoliisin toiminnasta, voisi henkilö tai yhteisö tehdä tiedusteluvalvontavaltuutetulle tutkimispyynnön.

Edellä kuvatussa toiminnassa ei voida hankkia välittävänä olevasta laitteesta tai tietojärjestelmästä taikka näiden tuottamasta tiedosta tietoa. Tällöin olisi kyse tiedonhankinnasta, mitä käsiteltävänä oleva säännös ei kata. Toimiessaan edellä tarkoitetulla tavalla, suojelupoliisi syyllistyisi rikolliseen toimintaan, jos tarvittavia tiedustelumenetelmän käyttöä koskevia lupia ei ole.

17 §. *Peitetoimintaa siviilitiedustelussa koskeva suunnitelma***.** Poliisilain 5 a luvun 17 §:ää ehdotetaan muutettavaksi siten, että pykälästä poistettaisiin peitetoimintaa koskevan erillisen esityksen vaatimus. Pykälän otsikkoa muutettaisiin ja pykälä jäisi koskemaan peitetoimintaa koskevaa suunnitelmaa ja olisi vastaava kuin voimassa olevan lain 17 §:n 2 momentti. Sen 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. Suojelupoliisin tarvitsemasta peitetoiminnasta päättää suojelupoliisin päällikkö. Mikäli päällikkö ei olisi yhtä mieltä vastuuvirkamiehen laatimasta peitetoimintapäätöksen sisällöstä, päätös joko laadittaisiin uudelleen taikka peitetoimintapäätöstä ei lainkaan tehtäisi.

Peitetoimintapäätöksestä erillisen peitetoimintaesityksen laatimiselle ei suojelupoliisin toiminnassa ole todettu olevan perusteltua syytä. Kahden eri asiakirjan laatimista koskevan vaatimuksen taustalla näyttäisi olevan se, että pakkokeinolain 10 luvun ja poliisilain 5 luvun mukaisessa ns. avoimen poliisin peitetoiminnassa esityksen laatimisvastuu ja peitetoimintaa koskeva päätöksenteko on eriytetty eri poliisiyksiköille. Avoimessa poliisissa peitetoiminnasta päättää keskusrikospoliisin päällikkö paikallisen poliisilaitoksen esityksestä ja peitetoiminnan toteuttaa keskusrikospoliisi.

Peitetoiminnasta olisi laadittaisiin suojelupoliisissa ainoastaan yksi asiakirja eli suunnitelma, josta ilmenisi päätöksentekijän ohella myös peitetoiminnan käyttöä esittäneen ja sen toteuttamisesta vastaavan virkamiehen tiedot. Peitetoimintaa koskeva päätöksenteko on suojelupoliisin sisäistä toimintaa.

18 §. *Peitetoiminnasta siviilitiedustelussa päättäminen.* Poliisilain 5 a luvun 18 §:n 1 momentti muutettaisiin sisällöllisesti muotoon, jonka mukaan suojelupoliisin päällikkö päättää peitetoiminnasta siviilitiedustelussa. Momentista erotettaisiin yksinomaan tietoverkossa tapahtuvan peitetoiminnan päätöksenteko omaksi 18 b pykäläkseen. Reaalimaailman ja yksinomaan tietoverkoissa tapahtuvan peitetoiminnan erotteleminen omiksi pykälikseen on säädösteknisesti perusteltua. Näin ollen peitetoiminnasta siviilitiedustelussa päättämistä koskeva 18 §:n 1 momentti muutettaisiin siten, että momentin yksinomaan tietoverkossa toteutettavaa peitetoimintaan koskeva päätöksentekosäädös siirrettäisiin uuteen yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskevan päätöksentekopykälään 18 b §.

Pykälän *2 ja 3 momentit* säilyisivät ennallaan.

Pykälän *4 momentti* muutettaisiin viimeisen, peitetoiminnan lopettamista koskevan virkkeen osalta. Momentista poistettaisiin peitetoiminnan lopettamista koskevan kirjallisen päätöksen vaatimus. Ehdotetun momentin sisällöksi jäisi, että päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava.

Peitetoimintaa koskevan sääntelyn esitöissä (HE 202/2017 vp, HE 222/2010 vp, HE 224/2010 vp) tai oikeuskirjallisuudessa ei perustella erillisen lopettamispäätöksen tarpeellisuutta. Hallituksen esityksestä HE 224/2010 vp kuitenkin ilmenee, että lopettamista koskeva säännös on siirretty poliisilakiin tuolloin voimassa olleesta poliisin tiedonhankinnan järjestämisestä ja valvonnasta annetusta sisäministeriön asetuksesta (174/2008). Säännöksen taustalla lienee se, että peitetoiminnalle ei ollut vuoden 1995 poliisilaissa (493/1995) säädetty, eikä edellä mainitussa asetuksessa määrätty voimassaoloaikaa eikä enimmäiskestoa, mistä syystä nimenomaista kirjallista lopettamispäätöstä koskevalle velvoitteelle oli paikkansa. Poliisilain nykyisen 5 a luvun mukaan peitetoimintaa koskevassa päätöksessä kuitenkin on mainittava päätöksen voimassaoloaika, joka voi kerrallaan olla enintään kuusi kuukautta. Lisäksi menetelmän käyttö on lopetettava jo ennen päätöksen voimassaoloajan päättymistä, jos menetelmän tarkoitus on saavutettu tai sen käytön edellytykset eivät enää täyty. Siviilitiedustelusta annetun valtioneuvoston asetuksen (719/2019) 12 §:n mukaan peitetoimintaa koskevalle pöytäkirjalle on kirjattava perustelut, mikäli tiedustelumenetelmän käyttö lopetetaan ennen päätöksen määräajan päättymistä. Edellä sanotun johdosta on perusteltua, että kirjallisen lopettamispäätöksen tekemiseen velvoittava lainkohta, jolle ei ole vastinetta muita tiedustelumenetelmiä koskevassa sääntelyssä, kumotaan.

18 a §. *Yksinomaan tietoverkossa toteutettava peitetoiminta***.** Uudessa 18 a §:ssä säädettäisiin yksinomaan tietoverkossa toteutettavan peitetoiminnan määritelmästä. Yksinomaan tietoverkossa toteutettavalla peitetoiminnalla siviilitiedustelussa tarkoitettaisiin poliisilain 5 a luvun 3 §:ssä tarkoitettua toimintaa koskevaa tietoverkossa tapahtuvaa suunnitelmallista tiedonhankintaa käyttämällä soluttautumista, jossa tiedonhankinnan edellyttämän luottamuksen hankkimiseksi tai tiedonhankinnan paljastumisen estämiseksi käytettäisiin vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka valmistettaisiin tai käytettäisiin vääriä asiakirjoja. Määritelmä noudattaa soveltuvin osin reaalimaailman peitetoiminnan määritelmää.

Ehdotetun pykälän 2 momentin mukaan yksinomaan tietoverkossa tehtävän peitetoiminnan toteuttamisesta olisi laadittava kirjallinen suunnitelma, jonka tulisi sisältää päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa olisi olosuhteiden muuttuessa tarvittaessa tarkistettava.

18 b §. *Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen***.** Uudessa poliisilain 5 a luvun 18 b §:ssä säädettäisiin yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättämisestä.

Poliisilain 5 luvun 28 §:n 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. Poliisilain 5 a luvun 18 §:ssä säädetään peitetoiminnasta päättämisestä siviilitiedustelussa. Pykälän 3 momentin 5 kohdan mukaan peitetoimintapäätöksessä on mainittava tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä. Poliisilain 5 a luvun 9 §:n 4 momentin mukaan henkilöryhmällä tarkoitetaan vähintään kolmen hengen muodostamaa tietyn ajan koossa pysyvää ja rakenteeltaan jäsentynyttä yhteenliittymää, joka toimii yhteistuumin tai yhteisen tavoitteen saavuttamiseksi. Siinä missä perinteisen peitetoiminnan kohdehenkilö tai kohteena oleva ryhmä on yleensä jokseenkin selkeästi rajattavissa, olisi yksinomaan tietoverkossa tapahtuvalle peitetoiminnalle leimallista se, että siihen liittyviä henkilöitä voi olla erittäin runsaasti, että verkossa toimitaan nimimerkkien turvin, ja että yksittäisten henkilöiden liityntä tiedonhankinnan kohteena olevaan toimintaan ei ole yksiselitteinen tai selvä.

Tietoverkoissa tapahtuvasta peitetoiminnasta ehdotetaan säädettäväksi tietolähteen ohjattua käyttöä vastaavalla tavalla siten, että tiedustelumenetelmän käyttöä koskevassa päätöksenteossa ei olisi velvoitetta yksilöidä kohdehenkilöä taikka henkilöryhmää (vrt. poliisilain 5a luvun 24 §). Sen sijaan olisi yksilöitävä poliisilain 5a luvun 3 §:n mukainen siviilitiedustelun kohteena oleva toiminta (esimerkiksi ulkomainen tiedustelutoiminta), kohdistamisen perustelut, tiedonhankinnan tavoite ja toteuttamissuunnitelma. Muutos mahdollistaisi suojelupoliisin peitetoiminnan kohdistaminen laajemmin kansallista turvallisuutta uhkaavaan toimintaan tai ilmiöön ilman ehdotonta henkilöyhteyttä. Henkilöperusteinen toiminta voisi edelleen olla ensisijainen toimintatapa, jos henkilö tai henkilöryhmä olisi tunnistettavissa. Muutos ei myöskään tarkoittaisi sitä, etteikö peitetoiminnan tosiasialliseksi kohteeksi joutuvia henkilöitä kirjattaisi peitetoiminnan jatkamista koskevilla päätöksille taikka peitetoiminnan käytöstä laadittavalle pöytäkirjalle ottaen huomioon, että peitetoiminnasta on ilmoitettava kohteelle, jos sen takia käynnistetään esitutkinta.

Ehdotetun pykälän *1 momentin* mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi yksinomaan tietoverkossa toteutettavasta peitetoiminnasta. Säännös vastaisi

päätöksentekotasoltaan, mitä yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättämisestä on säädetty 5 luvun 32 §:n 1 momentissa.

Pykälän *2 momentin* mukaan yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Säännös vastaisi poliisilain 5 luvun 32 §:n 2 momenttia.

Pykälän *3 momentin* mukaan päätös peitetoiminnasta olisi tehtävä kirjallisesti. Päätöksessä olisi mainittava: 1) toimenpiteen esittäjä; 2) peitetoiminnan toteuttamisesta vastaava poliisimies; 3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä; 4) 3 §:ssä tarkoitettu toiminta; 5) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat; 6) peitetoiminnan tavoite ja toteuttamissuunnitelma; 7) päätöksen voimassaoloaika ja 8) peitetoiminnan mahdolliset rajoitukset ja ehdot.

Säännös vastaisi 5 luvun 32 §:n 3 momenttia, lukuun ottamatta vaatimusta kohteena olevan henkilön yksilöimisestä. Yksinomaan tietoverkossa tapahtuvan peitetoiminnan kohdalla vaatimus ei ole tarkoituksenmukainen. Siinä missä perinteisen peitetoiminnan kohdehenkilö tai kohteena oleva ryhmä on yleensä jokseenkin selkeästi rajattavissa, on yksinomaan tietoverkossa tapahtuvalle peitetoiminnalle leimallista se, että siihen liittyviä henkilöitä voi olla erittäin runsaasti, että verkossa toimitaan nimimerkkien turvin, ja että yksittäisten henkilöiden liityntä tiedonhankinnan kohteena olevaan toimintaan ei ole yksiselitteinen tai selvä. Henkilöitä voi ilmaantua esimerkiksi keskusteluun nopeassa tahdissa ja toisaalta he voivat poistua keskustelusta yhtä nopeasti. Tiedustelutehtävässä olisi kuitenkin pystyttävä rajaamaan kohteena olevaa toimintaa mahdollisimman tarkasti eikä peitetoiminta tietoverkossa voisi olla täysin kohdentumatonta.

Pykälän 4 momentin mukaan päätöstä olisi olosuhteiden muuttuessa tarvittaessa tarkistettava.

25 §. *Tietolähteen turvaaminen siviilitiedustelussa*. Pykälän 5 momenttia muutettaisiin. Momentissa säädetään muun muassa tietolähteen turvaamiseksi annettavista vääristä asiakirjoista. Tältä osin nykytila pysyisi vastaavanlaisena. Uuden ehdotuksen nojalla suojelupoliisi voisi avustaa maahantulon järjestämisessä rikoslain 17 luvun 8 §:n estämättä, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi.

Nyt käsiteltävässä ehdotuksessa säännökseen ehdotetaan lisättäväksi mahdollisuus avustaa tietolähde muulla tavalla Suomen rajan yli. Kyse ei olisi kaikissa tapauksissa normaalista rajayli-tyspaikan kautta tapahtuvasta maahantulosta, vaan tietolähteen saapumisesta Suomeen tarvittaessa vaivihkaisesti.

Rikoslain 17 luvun 8 §:ssä säädetään laittoman maahantulon järjestämisestä. Esimerkiksi pykälän 1 momentin 2 kohdan mukaan laittoman maahantulon järjestämisestä on tuomittava henkilö, joka tuo tai yrittää tuoda Suomeen tai Suomen kautta muuhun maahan ulkomaalaisen, jonka maahantulo asiakirja on väärä, väärennetty, myönnetty toiselle henkilölle taikka saatu viranomaiselta asiakirjan myöntämisen kannalta merkityksellisen totuudenvastaisen tai harhaanjohtavan tiedon avulla, lahjomalla virnaomainen tai virkamiehen väkivaltaisella vastustamisella. Viittaus rikoslain pykälään selkeyttäisi myös sääntelyä säännöksessä jo nykyisin säädettyjen väärien asiakirjojen ja tietojen käytön osalta. Ehdotettu viittaus poistaisi selkeästi rikosoikeudellisen vastuun säännöksen tarkoittamissa tilanteissa.

Soveltamisen voidaan arvioida olevan poikkeuksellista. Mahdollisuus myös poikkeavan maahantulon järjestämiseen voidaan katsoa parantavan tietolähteen luottamusta siviilitiedusteluun sekä suomalaiseen yhteiskuntaan. Käytännössä myös tietolähteen on oltava erittäin luotettava

ja pitkäaikainen sekä hänen toimittamiensa tietojen on oltava merkityksellisiä, jotta säännöksen soveltaminen tulisi kyseeseen.

Säännöksen soveltamisen edellytyksenä on välttämättömyys. Välttämättömyys edellyttäisi sitä, että tietolähteen turvaamista ei voida käytännössä suorittaa muilla keinoin tai se vaatisi huomattavia resursseja. Lisäksi tietolähteen hengen ja terveyden suojaamisen tarve on voitava arvioida todelliseksi.

Tietolähde voisi hakea Suomesta turvapaikkaa, jolloin hän kävisi läpi normaalin turvapaikanhakijaa koskevan prosessin. Suomea voitaisiin myös käyttää kauttakulkumaana kolmanteen maahan.

27 §. *Paikkatiedustelusta siviilitiedustelussa päättäminen*. Pykälän 3 momenttia ehdotetaan muutettavaksi.

Voimassa olevan pykälän 1 momentin mukaan tuomioistuin päättää paikkatiedustelusta siviilitiedustelussa, jos se kohdistuu muuhun kotirauhan suojaamaan paikkaan kuin pysyväisluonteiseen asumiseen käytettävään paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy on rajoitettu tai estetty paikkatiedustelun toimittamisajankohtana, tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Pykälän 2 momentti koskee kiiretilanteita. Pykälän 3 momentin mukaan suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.

Pykälän *3 momenttia* ehdotetaan muutettavaksi edellä 5 a luvun 27 §:ää koskevassa nykytilan kuvauksessa todetun johdosta siten, että suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättäisi muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta sekä kulkuneuvoon kohdistuvasta paikkatiedustelusta. Kulkuneuvo on paikka, johon ei ole yleistä pääsyä paikkatiedustelun ajankohtana, mutta jonka ei ole perusteltua saada normaalitilanteessa vastaavanlaista suojaa kuin esimerkiksi lukittu toimisto. Toisaalta ajoneuvo ja lukittu toimisto eivät välttämättä aina ole toisiinsa verrattavissa olevia tiloja. Kulkuneuvoon kohdistuvasta paikkatiedustelusta säädettäisiin täten omana paikkatiedustelun alalajina ja siitä päättäväksi tahoksi olisi perusteltua osoittaa suojelupoliisin päällystöön kuuluva poliisimies. Tällöin päätöstä kulkuneuvoon kohdistuvasta paikkatiedustelusta ei tehtäisi tuomioistuimessa.

Säännöksen soveltamisessa on kuitenkin otettava huomioon tilanteet, joissa kulkuneuvoa käytetään pysyväisluonteiseen asumiseen.

27 a §. *Näytteenotto paikkatiedustelussa*. Säännös olisi uusi. Pykälää ehdotetaan edellä nykytilakuvauksessa otsikon ”paikkatiedustelua koskevan sääntelyn täydentäminen näytteenottoa ja esineen/omaisuuden/asiakirjan tilapäistä haltuunottoa koskevalla sääntelyllä ” alla todetun johdosta. Pykälän mukaan suojelupoliisilla olisi oikeus paikkatiedustelussa ottaa aineesta, omaisuudesta tai esineestä näyte, jos se olisi tarpeen siviilitiedustelutehtävän suorittamiseksi.

Siviilitiedustelun kohteista säädetään poliisilain 5 a luvun 3 §:ssä eli niin sanotussa uhkaluettelossa. Kohteita ovat muun muassa terrorismi ja ulkomainen tiedustelutoiminta. Paikkatiedustelun yhteydessä voi löytyä esimerkiksi aineita, joita voidaan käyttää räjähteiden valmistukseen tai kemikaaleja. Aineita ei yleensä ole mahdollista tunnistaa tai niiden vaarallisuutta arvioida pelkästään visuaalisesti paikan päällä. Ulkomaisen tiedustelutoimijan kohdalla voi löytyä

esimerkiksi asiakirjoja, joiden osalta on oletettavissa, että niihin sisältyy kemiallisen käsittelyn avulla näkymättömäksi tehtyä kirjoitusta.

Omaisuus tai erä siitä voitaisiin ottaa haltuun laboratorio-olosuhteissa suoritettavan analysoinnin mahdollistamiseksi ja aineen tunnistamiseksi. Esimerkiksi räjähteen lähtöaineeksi tai toksiiniksi epäillystä aineesta voitaisiin monessa tapauksessa ottaa niin pieni näyte, ettei omaisuuden väheneminen ole silmin havaittavissa. Vaikka aine, esine tai omaisuus olisi tarpeen ottaa haltuun kokonaisuudessaan, olisi se ainakin osassa tapauksista ilmeisesti mahdollista vaihtaa ulkoisesti sitä muistuttavaan mutta vaarattomaan aineeseen, esineeseen tai omaisuuteen, jolloin uhkan aiheuttava taho ei ainakaan välittömästi havaitsisi haltuunottoa.

28 a §. *Aineen, omaisuuden tai esineen tilapäinen haltuunotto.* Säännös olisi uusi. Pykälää ehdotetaan edellä nykytilakuvauksessa otsikon ”*paikkatiedustelua koskevan sääntelyn täydentäminen näytteenottoa ja esineen/omaisuuden/asiakirjan tilapäistä haltuunottoa koskevalla sääntelyllä* ” alla todetun johdosta.

Pykälän mukaan jos 27 a §:ssä tarkoitettu näytteenotto tai 28 §:ssä tarkoitettu jäljentäminen sitä välttämättä edellyttäisi, suojelupoliisilla olisi oikeus ottaa aine, omaisuus tai esine tilapäisesti haltuun. Aine, omaisuus tai esine olisi palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua.

Tiedustelutoiminnan luonteen vuoksi toimivaltuuden käytössä tarkoitettu haltuunotto olisi tilapäistä. Jotta suojelupoliisin toiminta pysyisi salassa, olisi haltuunoton oltava mahdollisimman lyhytkestoista ja haltuun otettava aine, esine tai omaisuus olisi palautettava mahdollisimman pian alkuperäiselle paikalleen.

Poliisilain 5 a luvun 28 §:ssä säädetään jäljentämisestä siviilitiedustelussa. Sen mukaan suojelupoliisilla on oikeus siviilitiedustelussa jäljentää asiakirja tai esine.

Sekä 27 a §:n että 28 §:n tapauksissa omaisuus tai erä siitä saataisiin ottaa haltuun laboratorio-olosuhteissa suoritettavan analysoinnin mahdollistamiseksi ja aineen tunnistamiseksi**.** Paikka tiedustelun yhteydessä voi löytyä sellaisia aineita, joita mahdollisesti voidaan käyttää räjähteiden valmistukseen tai myrkyllisiä kemikaaleja. Löydettyä ainetta ei kuitenkaan voida yleensä tunnistaa tai sen vaarallisuutta arvioida pelkästään ulkoisten tunnusmerkkien perusteella. Esimerkiksi räjähteen lähtöaineeksi tai toksiiniksi epäillystä aineesta voitaisiin monessa tapauksessa ottaa niin pieni näyte, ettei omaisuuden väheneminen ole silmin havaittavissa. Vaikka aine, esine tai omaisuus olisi tarpeen ottaa haltuun kokonaisuudessaan, olisi se ainakin osassa tapauksista ilmeisesti mahdollista vaihtaa ulkoisesti sitä muistuttavaan mutta vaarattomaan aineeseen, esineeseen tai omaisuuteen, jolloin uhkan aiheuttava taho ei ainakaan välittömästi havaitsisi haltuunottoa. Tilapäisen haltuunoton ei voida katsoa lisäävän käynnissä olevan siviilitiedustelun paljastumisen riskiä.

Jos pykälän toimivaltuudella hankittu tieto esimerkiksi räjähteessä käytettävästä aineesta varmistuisi, tieto voitaisiin luovuttaa niin kutsutun palomuurisääntelyn mukaisesti rikostorjuntaviranomaiselle.

Ehdotetun pykälän 2 momentin mukaan, jollei omaisuutta, esinettä tai ainetta voida vaaratta palauttaa, suojelupoliisin päällystöön kuuluva poliisimies voisi määrätä omaisuuden, esineen tai aineen hävitettäväksi. Hävittämisestä olisi tehtävä merkintä paikkatiedustelusta laadittavaan pöytäkirjaan tai tehtävä vastaava merkintä muuhun asiakirjaan. Poliisilain 5 a luvun 48 §:ssä säädetään, että tiedustelumenetelmän käytöstä on sen lopettamisen jälkeen laadittava ilman

aiheetonta viivytystä pöytäkirja. Paikkatiedustelua koskevasta pöytäkirjasta säädetään tarkemmin siviilitiedustelusta annetun valtioneuvoston asetuksen 19 §:ssä.

39 §. *Tiedustelumenetelmän käytöstä päättäminen eräissä tilanteissa.* Pykälän *1 momenttia* muutettaisiin, koska sääntelyyn on tiedusteluoperaatioiden päätöksenteon osalta liittynyt edellä nykytilan kuvauksessa todettua epäselvyyttä. Voimassa olevan 1 momentin mukaan muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja tiedustelumenetelmän käytöstä päättää suojelupoliisin päällikkö. Ehdotuksen mukaan muualla kuin Suomessa toteutettavasta siviilitiedustelusta päättäisi suojelupoliisin päällikkö, ja tiedustelutoimintaan liittyvästä yksittäisen tiedustelumenetelmän käytöstä saisi päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Ehdotetun muutoksen myötä suojelupoliisin päällikkö tekisi päätöksen ulkomailla tapahtuvasta siviilitiedustelusta (tiedusteluoperaatiosta) ja siinä käytettävistä tiedustelumenetelmistä kuten nykyisinkin, ja päätöksen mukaista tiedustelumenetelmän käyttöä koskevan yksittäisen päätöksen voisi tehdä myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Viimeksi mainittu virkamies on lähempänä käytännön toimintaa. Muutos selkeyttäisi oikeustilaa ja virkamiehen oikeusturva parantuisi.

Ulkomailla tapahtuvaan tiedusteluun liittyvien ulkopoliittisten herkkyyksien takia päätöksenteossa olisi otettava huomioon tiedustelun painopisteet ja sitä kautta tulleet mahdolliset suuntaviivat.

Pykälän *3 momenttiin* lisättäisiin viittaus tietolähdetoimintaa koskevan poliisilain 5 luvun 40 §:n 3 momenttiin. Lisäyksen myötä ulkomailla tapahtuvassa tietolähdetoiminnassa ei tarvitsisi soveltaa kieltoa hankkia tietoja viranomaistoimivaltuuksilla. Kyse olisi yksittäistapauksista.

Voimassa olevien säännösten takia epäselvyyttä on aiheuttanut se, onko kiellossa käyttää viranomaistoimivaltuuksia kyse suomalaisen viranomaisten vai kohdevaltion viranomaisten toimivaltuuksista. Joissain valtioissa viranomaisten toimivaltuudet saattavat olla erittäin laajoja, minkä takia voi jäädä epäselväksi se, käyttääkö tietolähde viranomaistoimivaltuuksia vai ei.

Uuden viittauksen myötä poikkeamisessa olisi kuitenkin oltava kyse välttämättömyydestä kansallisen turvallisuuden suojaamiseksi.

39 a §. *Tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi.* Pykälä olisi uusi. Sen mukaan suojelupoliisilla olisi oikeus estää tietoteknisin menetelmin Suomen ulkopuolella olevan tietojärjestelmän käyttö tai haitata tai muokata sen toimintaa, jos tietojärjestelmällä tai sen kautta voitaisiin aiheuttaa kansalliselle turvallisuudelle vakavaa vaaraa. Toimenpiteen käytön olisi oltava välttämätöntä vakavan vaaran torjumiseksi, eikä sillä saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin olisi välttämätöntä tehtävän suorittamiseksi.

Säännöksen käyttöala olisi sidottu siviilitiedustelutoimintaan, joten pelkästään estäviin toimenpiteisiin ryhtyminen ei olisi säännöksen nojalla mahdollista. Säännöksen käyttäminen edellyttäisi käytännössä sitä, että kyse on ollut ensisijaisesti tiedonhankinnasta. Käytännössä tilanne voisi tulla kyseeseen esimerkiksi, jos tiedustelun kohteena olisi tietojärjestelmä, jota sittemmin käytettäisiin säännöksessä kuvattuun vakavasti vaarantavaan toimintaan tai sen mahdollistamiseen. Toimivaltuutta voitaisiin käyttää myös, jos olisi viitteitä Suomen kansallista turvallisuutta vakavasti vaarantavasta toiminnasta, jonka nojalla käynnistettäisiin tiedusteluoperaatio, jonka

myötä vakavaa vaaraa aiheuttavaan tietojärjestelmään voitaisiin kohdistaa säännöksessä tarkoitettuja toimenpiteitä.

Säännöksessä tarkoitetulla estämisellä tarkoitettaisiin tietoteknisiä toimenpiteitä, joilla järjestelmän toiminta estettäisiin kokonaan tai osittain. Tämä voi edellyttää järjestelmän käyttämiseksi tarpeellisten tietojen muokkaamista tavalla, jonka takia järjestelmän käyttö tarkoitettuun tarkoitukseen ei ole käytännössä mahdollista. Käytön haittaamisella viitattaisiin toimenpiteisiin, joilla esimerkiksi järjestelmän tai ohjelmiston tietoja taikka niiden sisältämiä tietoja muokataan tavalla, joka kohdistaa vakavasti vaarantavan toimenpiteen esimerkiksi käyttäjään itseensä. Haittaamisella tarkoitettaisiin myös sitä, että järjestelmästä poistetaan tietoja, kuten sinne Suomen kriittisestä infrastruktuurista kyberverkkotiedustelulla hankittuja tietoja.

Vaikuttamismahdollisuuden tarve voisi ilmetä esimerkiksi kyberuhkatoimijan infrastruktuuria vastaan. Infrastruktuuria ja sitä hyödyntäen toteutettavaa kyberhyökkäystä tai sen valmistelua tulisi voida häiritä tai aktiivisesti estää, jos havaitaan sen muodostavan uhkan kansalliselle turvallisuudelle. Vaikuttamistoimella voitaisiin myös haitata sellaisten tietojärjestelmien toimintaa, joita käytetään tukemaan perinteisempiä fyysisen maailman uhkia tai ns. hybridiuhkia. Tällaisia tietojärjestelmiä voisivat olla esimerkiksi uhkatoimijan käyttämät viestintäjärjestelmät, logistiikkajärjestelmät tai sosiaalisessa mediassa tapahtuvaan järjestelmälliseen valtiolliseen vaikuttamistoimintaan tarkoitetut tietotekniset ratkaisut.

Päätöksenteosta säädettäisiin uudessa 39 b §:ssä.

Koska säännöksessä tarkoitetut toimenpiteet voivat tietyissä tilanteissa sisältää merkittäviäkin ulko- ja turvallisuuspoliittisia vaikutuksia, olisi toimenpiteitä käsiteltävä matalahkolla kynnyksellä poliisilain 5 a luvun 58 §:ssä tarkoitetussa menettelyssä. Toimenpiteet saattavat myös edellyttää tasavallan presidentin ja ulko- ja turvallisuuspoliittisen ministerivaliokunnan yhteistä kokousta tai sitä vastaava mahdollinen uusi ulko- ja turvallisuuspolitiikkaa käsittelevä kokoonpano, joka käsittelisi valmistelevasti toimenpiteen suorittamista.

Toimivaltuutta saisi käyttää ainoastaan Suomen kansalliselle turvallisuuden mahdollisesti vakavaa vaaraa aiheuttavan tietojärjestelmän käytön estämiseen ja haittaamiseen. Vaikka toiminta vaikuttaa sen kohteena olevan laitteen tai tietojärjestelmän toimintaan, ei siinä olisi kyse sotilaalliseen tai aseelliseen voimankäyttöön rinnastuvasta vaikutuksiltaan vertautuvasta toiminnasta, vaan sitä vähäisemmästä, oman suojautumisen välttämättä edellyttämästä vastapuolen laittoman toimintaan kohdistuvasta vastatoimesta ja laillisen tilan palauttamisesta.

39 b §. *Tietojärjestelmän käytön estämisestä tai sen toiminnan haittaamisesta vakavan vaaran torjumiseksi päättäminen.* Pykälä olisi uusi ja siinä säädettäisiin edellä 39 a §:n toimivaltuuden käyttämistä koskevasta päätöksenteosta.

Ulko- ja turvallisuuspoliittisesti herkällä alueella olisi toimenpidettä koskevassa päätöksenteossa aina huomioitava ulko- ja turvallisuuspoliittisten näkökantojen lisäksi kansallinen lainsäädäntö ja kansainvälinen oikeus. Edellä tarkoitetut näkökannat olisi valmisteltava toimenpiteen luonteesta riippuen poikkihallinnollisesti. Tämä tarkoittaisi käsittelyä tiedustelun koordinaatioryhmässä ja tarvittaessa asia olisi vietävä valmistelevaan käsittelyyn TP-UTVA:an tai sitä vastaavaan perustettavaan ryhmään.

Ehdotetun 39 a §:n toimivaltuuden käytöstä päätettäessä olisi aina huomioitava toimenpiteen oikeasuhtaisuus sisältäen eettisen arvioinnin ja vaikutukset kohteelle. Tässä olisi otettava huomioon myös kansainvälinen humanitaarinen oikeus. Keskeinen osa toimenpiteen vaikutusten arvioinnissa on myös operaatioturvallisuudella. Jos toimenpidettä ei voi suorittaa operaatiotur-

vallisesti, toimenpide jää tekemättä. Päätöksenteossa olisi myös aina huomioitava toimenpiteen vaatimat resurssit ja suhteuttaa niitä realistisesti odotettavissa oleviin hyötyihin.

Ehdotetun pykälän *1 momentin* mukaan suojelupoliisin päällikkö päättäisi tietojärjestelmän käytön estämisestä tai haittaamisesta. Päätös olisi tehtävä kirjallisesti.

Pykälän *2 momentissa* olisi tarkemmin säädetty päätöksen sisältövaatimuksista Momentin mukaan päätöksessä olisi mainittava: 1) toimenpiteen kohteena oleva tietojärjestelmä; 2) toimenpiteen perusteena olevaa vakavaa vaaraa ja toimenpiteen käytön edellytyksiä koskevat tosiseikat; 3) toimenpiteen tavoite ja toteuttamissuunnitelma; 4) toimenpiteen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies ja 5) mahdolliset toimenpiteen rajoitukset ja ehdot.

Edellä *2 momentin 1 kohdan* tietojärjestelmällä tarkoitetaan tietojenkäsittelylaitteiden, tiedonsiirtolaitteiden ja tietoja käsittelevien ohjelmistojen muodostamaa yhteen toimi-van kokonaisuutta. *Kohdan 2* mukaisen vakavan vaaran kuvauksessa olisi kiinnitettävä huomiota vaaran konkreettisuuteen, eli minkälaista vaaraa tietojärjestelmän käytöllä voitaisiin aiheuttaa Suomelle. Vaara konkretisoituu useimmin tietoverkkojen kautta tapahtuvana vaikuttamisena esimerkiksi Suomen kriittisen infrastruktuurin tietojärjestelmiin. Vaara voi myös konkretisoitua fyysisessä maailmassa, mutta tällöin arviointi ei voi perustua täysin hypoteettisiin kehityskulkuihin. Fyysisen maailman vaaran voidaan olettaa olevan hitaammin kehittyvä ja sen toteuttaminen hitaampaa. Näin ollen tietoverkoissa toteutuvaan vaaraan verrattuna fyysisen maailman vaaralta edellytetään enemmän konkretiaa ja tietoa, että vaaraa voi aiheutua Suomelle. *Kohdan 3* tavoitteella tarkoitettaisiin odotettua lopputulosta ja mitä siitä voidaan olettaa seuraavan. Lisäksi toteuttamissuunnitelmassa olisi tehtävä selkoa siitä, miten toimenpide käytännössä toteutetaan. Mitä käytännön toimenpiteitä tehdään, että haluttu lopputulos saadaan aikaiseksi. *Momentin 4 kohdan* mukaan päätöksessä olisi mainittava toimenpiteen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies. Momentin *5 kohdan* mukaan päätöksessä voitaisiin asettaa erityisiä rajoituksia ja ehtoja. Etenkin ulko- ja turvallisuuspoliittisesti herkissä tilanteissa rajoituksia ja ehtoja voisi tulla esimerkiksi poliisilain 5 a luvun 58 §:ssä tarkoitetussa menettelyssä tai mahdollisessa tasavallan presidentin ja ulko- ja turvallisuuspoliittisen ministerivaliokunnan yhteisessä kokouksessa tai sitä vastaavalta mahdolliselta uudelta kokoonpanolta.

41 §. *Kuuntelu- ja katselukiellot siviilitiedustelussa.* Poliisilain 5 a luvun 41 §:ssä säädetään kuuntelu- ja katselukielloista siviilitiedustelussa. Pykälän 1 ja 2 momenttiin lisättäisiin tässä esityksessä säädettäväksi ehdotettu uusi valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun toimivaltuus. Kiellot koskisivat myös tätä uutta valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua samalla tavalla kuin ne koskevat telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua ja teknistä laitetarkkailua.

41 a §. *Telekuuntelun, televalvonnan, teknisen kuuntelun, teknisen laitetarkkailun ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun keskeyttäminen*. Pykälä olisi uusi. Pykälässä säädettäisiin telekuuntelun, televalvonnan, teknisen kuuntelun, teknisen laitetarkkailun ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun keskeyttämisestä.

Poliisilain 5 luvun 56 §:ssä säädetään telekuuntelun, televalvonnan, teknisen kuuntelun ja teknisen laitetarkkailun keskeyttämisestä, mutta näitä salaisia tiedonhankintakeinoja vastaavien tiedustelumenetelmien keskeyttämisestä ei ole säädetty siviilitiedustelumenetelmiä koskevassa 5 a luvussa. Keskeyttämisestä ehdotetaan säädettäväksi myös uuden valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun toimivaltuuden osalta.

Pykälän ensimmäisen momentin mukaan, jos kävisi ilmi, että telekuuntelu tai televalvonta kohdistuisi muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskelisi kuunneltavassa tilassa tai muussa paikassa, tiedonhankintakeinon käyttö olisi tältä osin keskeytettävä niin pian kuin mahdollista sekä kuuntelulla saadut tallenteet ja sillä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

Pykälän toisen momentin mukaisesti velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskisi myös teknistä laitetarkkailua, jos kävisi ilmi, että tarkkailu kohdistuisi sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta kuin laitetarkkailusta säädetään 5 a luvussa, taikka että toimenpiteen kohteena oleva henkilö ei käytä tarkkailun kohteena olevaa laitetta. Edelleen, pykälän toisen momentin mukaan jos kävisi ilmi, että valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu kohdistuisi sellaiseen tietojenkäsittelylaitteeseen, tiedonsiirtolaitteeseen tai tietoja käsittelevään ohjelmistoon, joka ei kuuluisi luvan kohteena olevaan tietojärjestelmään, olisi valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu tältä osin keskeytettävä niin pian kuin mahdollista ja sillä saadut tallenteet ja tiedot sekä saatuja tietoja koskevat muistiinpanot olisi heti hävitettävä.

46 §. *Kiiretilanteessa saadun tiedon hävittäminen.* Poliisilain 5 a luvun 46 §:n 1 momentissa säädetään tuomioistuimen kumoaman suojelupoliisin virkamiehen tekemän kiirepäätöksen vaikutuksista. Momentin mukaan, jos suojelupoliisin päällystöön kuuluva poliisimies on kiireellisessä tilanteessa päättänyt tiedustelumenetelmän käytön aloittamisesta, mutta tuomioistuin katsoo, ettei edellytyksiä toimenpiteelle ollut, tiedustelumenetelmän käyttö on lopetettava sekä sillä saatu aineisto ja sillä saatuja tietoja koskevat muistiinpanot on heti hävitettävä. Näin saatuja tietoja saadaan kuitenkin käyttää luvun 44 §:n (ns. palomuuripykälä) mukaisesti sellaisesta jo tehdystä tai vielä estettävissä olevasta rikoksesta ilmoittamiseksi, josta säädetty ankarin rangaistus on vähintään kuusi vuotta vankeutta. Tietoja saisi käyttää myös 44 a §:n 2 momentissa tarkoitetuissa tilanteissa. Momentin mukaan tiedustelumenetelmän käytön avulla saatua tietoa saa aina luovuttaa salassapitosäännösten estämättä syyttömyyttä tukevaksi selvitykseksi sekä hengelle, terveydelle tai vapaudelle aiheutuvan merkittävän vaaran taikka huomattavan ympäristö-, omaisuus- tai varallisuusvahingon estämiseksi.

Tässä esityksessä ehdotetaan muutettavaksi poliisilain 5 a luvun 6 §:ää siten, että säädettäisiin telekuuntelun ja sen sijasta tapahtuvan tietojen hankkimisen kiiretilanteen päätöksentekomenettelystä. Muutoksen myötä kiiretilanteessa saadun tiedon hävittämisestä tulee säätää vastaavalla tavalla kuin muidenkin kiirepäätösten vaikutuksista. Pykälään tehdään tätä koskevat viittaukset ja tekniset lisäykset.

47 §. *Tiedustelumenetelmän käytöstä ilmoittaminen.* Poliisilain 5 a luvun 47 §:ssä säädetään tiedustelumenetelmän käytöstä ilmoittamisesta. Pykälän 3 momentin mukaan, jos tiedonhankinnan kohteen henkilöllisyys ei ole tiedossa pykälän 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden selvittyä.

Pykälän *3 momenttia* ehdotetaan muutettavaksi siten, että henkilöllisyyttä koskevan tiedon lisäksi oleskelupaikka mainittaisiin edellytykseksi ilmoituksen tekemiselle. Henkilöllisyyden tietäminen ei yksinään riitä kirjallisen ilmoituksen tekemiseen, vaan tiedossa olisi oltava oleskelupaikka tai muu osoite, jonne ilmoitus voidaan toimittaa. Tällöin, jos tiedonhankinnan kohteen henkilöllisyys ja oleskelupaikka ei olisi tiedossa pykälän 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä olisi ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden ja oleskelupaikan selvittyä.

51 §. *Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan velvollisuus avustaa siviilitiedustelussa.* Pykälässä säädettäisiin viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan velvollisuudesta avustaa siviilitiedustelussa. Pykälän nykyisenä otsikkona on ” teleyrityksen velvollisuus avustaa siviilitiedustelussa”. Uutena otsikkona olisi ” viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan velvollisuus avustaa siviilitiedustelussa”, mikä ilmentäisi sitä muuttuneita olosuhteita.

Ehdotuksen mukaan jatkossa viitattaisiin teleyrityksen sijaan sähköisen viestinnän palveluista annetun lain 3 §:n 36 kohdassa tarkoitettuun viestinnän välittäjään. Lainkohdan mukaan viestinnän välittäjällä tarkoitetaan teleyritystä, yhteisötilaajaa ja myös sellaista muuta tahoa, joka välittää sähköistä viestintää muutoin kuin henkilökohtaisiin tai niihin verrattaviin tavanomaisiin yksityisiin tarkoituksiin. Lisäksi avustamisvelvollisuus koskisi tietoyhteiskunnan palvelun tarjoajia. Tietoyhteiskunnan palvelu on määritelty sähköisen viestinnän palveluista annetun lain 3 §:n 29 kohdan mukaan sähköisenä etäpalveluna vastaanottajan henkilökohtaisesta pyynnöstä tavallisesti korvausta vastaan toimitettavaa palvelua.

Pykälän *1 momentissa* mainittaisiin myös uusi tiedustelumenetelmä, valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu. Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan olisi avustettava suojelupoliisia vastaavasti kuin esimerkiksi telekuuntelussa. Ehdotetun 1 momentin mukaan viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan olisi ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun ja televalvonnan ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun edellyttämät kytkennät sekä annettava suojelupoliisin käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskisi myös niitä tilanteita, joissa telekuuntelu, televalvonta tai televerkkoon kohdistuva valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu toteutetaan suojelupoliisin toimesta teknisellä laitteella. Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan olisi lisäksi annettava suojelupoliisin päällystöön kuuluvan poliisimiehen käyttöön hallussaan olevat teknisen seurannan toimeenpanoa varten tarpeelliset tiedot.

Pykälän *2 momentin* mukaan suojelupoliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä olisi oikeus telekuuntelua ja televerkkoon kohdistuvaa valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän tai tietoyhteiskunnan palvelun tarjoajan hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättäisi suojelupoliisin päällystöön kuuluva poliisimies.

52 §. *Korvaus viestinnän välittäjälle ja tietoyhteiskunnan palvelun tarjoajalle siviilitiedustelussa avustamisesta ja tietojen antamisesta.* Pykälän otsikko ehdotetaan muutettavaksi pykälän sisältöä vastaavaksi. Pykälän nykyinen otsikko kuuluu ”korvaus teleyritykselle siviilitiedustelussa avustamisesta ja tietojen antamisesta” ja se muutettaisiin kuulumaan ”korvaus viestinnän välittäjälle ja tietoyhteiskunnan palvelun tarjoajalle siviilitiedustelussa avustamisesta ja tietojen antamisesta”.

Pykälään tehtäisiin vastaavat 51 §:ään ehdotetuista muutoksista johtuvat muutokset korvauksen saajiin. Poliisilain 5 a luvun 51 §:ssä säädettäisiin viestinnän välittäjille ja tietoyhteiskunnan palvelun tarjoajille velvollisuus avustaa siviilitiedustelussa. Poliisilain 5 a luvun 52 §:ää tarkistettaisiin niin, että vastaavasti laajennettaisiin korvaukseen oikeutettujen joukkoa.

Ehdotetun pykälän *1 momentin* mukaan viestinnän välittäjällä ja tietoyhteiskunnan palvelun tarjoajalla olisi oikeus saada valtion varoista korvaus 51 §:ssä tarkoitetusta viranomaisten

avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksesta säädetään sähköisen viestinnän palveluista annetun lain 299 §:ssä. Korvauksen maksamisesta päättäisi suojelupoliisi. Voimassa olevan 52 §:n mukaan teleyrityksen oikeuteen saada korvausta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista sovelletaan, mitä poliisilain 5 luvun 62 §:ssä säädetään. Luvun 62 §:n mukaan teleyrityksellä on oikeus saada valtion varoista korvaus tässä luvussa tarkoitetusta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksesta säädetään sähköisen viestinnän palveluista annetun lain 299 §:ssä. Korvauksen maksamisesta päättää toimenpiteen suorittaneen poliisiviranomaisen yksikkö.

Pykälän *2 momentti* olisi uusi. Momentissa olisi informatiivinen viittaus hallintolakiin ja oikeudenkäynnistä hallintoasioissa annettuun lakiin oikaisuvaatimuksen ja valitusoikeuden osalta.

Pykälän *3 momentti* olisi uusi. Momentissa säädettäisiin Liikenne- ja viestintäviraston oikeudesta tulla kuulluksi, mikäli korvausasiaa käsitellään hallinto-oikeudessa.

55 §. *Yhteistyö muiden viranomaisten, yritysten ja yhteisöjen kanssa***.** Pykälän *3 momenttia* muutettaisiin niin, että **s**uojelupoliisi voisi siviilitiedustelutehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille salassapitosäännösten estämättä muita kuin henkilötietoja koskevia tietoja, jos tietojen luovuttaminen olisi tarpeen kansallisen turvallisuuden suojaamiseksi. Tietojen luovuttamista ei olisi enää sidottu välttämättömyyteen vaan tarpeellisuuteen kansallisen turvallisuuden suojaamiseksi. Tämä tarkoittaisi sitä, että tietojen luovutuksella voitaisiin parantaa Suomen kansallista turvallisuutta, ja tiedonluovutuksella olisi oltava liityntä näihin etuihin.

55 a §. *Yhteistoiminta Rajavartiolaitoksen kanssa.* Pykälä olisi uusi. Pykälässä säädettäisiin Rajavartiolaitoksen mahdollisuudesta avustaa suojelupoliisia siviilitiedustelutehtävän suorittamisessa osallistumalla tiedustelumenetelmien käyttöön. Suojelupoliisin ja Rajavartiolaitoksen väliseen yhteistoimintaan sovelletaan lähtökohtaisesti poliisilain 5 a luvun 55 §:ää, mutta käytännön toiminnassa, erityisesti tiedustelumenetelmien käyttöön liittyvissä yksittäistapauksissa, on kuitenkin havaittu olevan Rajavartiolaitoksen tuelle laajempia tarpeita. Kyse olisi siis lyhytaikaisesta, yksittäisten tiedustelutehtävään liittyvien tehtävien tai toimenpiteiden suorittamisesta ja ne tapahtuisivat aina suojelupoliisin pyynnöstä. Pyyntö voisi olla tietyissä tilanteissa ennalta tehty tai se voisi tapahtua nopeampaa reagointia vaativissa tilanteissa viranomaisten välisten päivystysjärjestelyjen kautta.

Suojelupoliisin toimenpiteiden on aina oltava puolustettavia suhteessa tiedonhankinnan merkittävyyteen. Myös Rajavartiolaitokselle tehtävää yksittäistä toimenpidettä koskevaa pyyntöä olisi siten aina arvioitava sillä tavoiteltavaan päämäärään nähden. Tiedonhankintatoimenpiteiden mitoittamiseen vaikuttaisi esimerkiksi se, kuinka oleellinen merkitys tietyllä yksittäisellä toimenpiteellä on uhkaan liittyvien tietojen hankinnan kannalta eikä toimenpiteellä saisi puuttua kenenkään oikeuksiin enempää kuin on välttämätöntä tiedustelun käytön tarkoituksen saavuttamiseksi.

Pykälän 1 *momentissa* säädettäisiin, että lain poliisilain 5 a luvun 55 §:n lisäksi Rajavartiolaitos voisi avustaa pykälässä lueteltujen tiedustelumenetelmien käytössä. Tiedustelumenetelmään liittyvällä yksittäisellä toimenpiteellä tarkoitettaisiin esimerkiksi menetelmän käyttöön liittyvää teknistä asennustoimenpidettä taikka henkilöön tai henkilöryhmään tilapäisesti kohdistuvaa tarkkailua. Luettelo olisi tyhjentävä ja koskisi ensisijaisesti vain niitä tiedustelumenetelmiä, joista päätöksen voi lain mukaan tehdä tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Tällaisia tiedustelumenetelmiä olisivat tarkkailu ja suunnitelmallinen tarkkailu, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen

laitetarkkailu, teleosoitteen tai telepäätelaiteen yksilöintitietojen hankkiminen, laitteen sekä menetelmän tai ohjelmiston asentaminen ja poisottaminen sekä paikkatiedustelu ja jäljentäminen. Rajavartiolaitos voisi kuitenkin avustaa teknisessä kuuntelussa, katselussa ja seurannassa, teknisessä laitetarkkailussa sekä paikkatiedustelussa ja jäljentämisessä myös silloin, kun tiedustelumenetelmän käyttöön liittyvän luvan on antanut tuomioistuin. Kyseeseen tulisi siis joukko tiedustelumenetelmiä, joiden käyttö sekä siihen liittyvät yksittäiset toimenpiteet vastaisivat toteutukseltaan lähinnä Rajavartiolaitoksen omissa tehtävissään käyttämiä salaisia tiedonhankintakeinoja ja joissa sillä jo olisi vastaavaa käytännön kokemusta yksittäisen tehtävän tai toimenpiteen suorittamisesta. Suojelupoliisin olisi kuitenkin velvollisuus järjestää tehtäviä tai toimenpiteitä suorittavalle Rajavartiolaitoksen henkilöstölle tiedustelumenetelmiin liittyvien erityispiirteiden koulutusta. Suojelupoliisi vastaisi niin ikään tiedustelumenetelmää koskevasta päätöksestä tai luvasta, sekä 47 §:n mukaisesta ilmoitusvelvollisuudesta.

Pykälän 1 momentissa säädettäisiin lisäksi, että Rajavartiolaitoksen olisi suojelupoliisin pyynnöstä ilman aiheetonta viivytystä keskeytettävä tässä momentissa tarkoitettu toimenpide, eli käytännössä heti, kun se olisi mahdollista esimerkiksi vaarantamatta menetelmän käytön tarkoitusta. Keskeytystä koskeva pyyntö voisi tulla kyseeseen esimerkiksi tilanteessa, jossa tuomioistuin toteaisi, ettei suojelupoliisin tiedustelumenetelmää koskevalle kiirepäätökselle olisi ollut lupaan oikeuttavia perusteita. Pyyntö keskeytyksestä voitaisiin tehdä myös Rajavartiolaitoksen ilmoituksen perusteella, mikäli Rajavartiolaitos arvioisi, ettei sillä kyseisellä hetkellä olisi, esimerkiksi omista lakisääteisistä tehtävistään johtuen, mahdollisuuksia pyydetyn toimenpiteen suorittamiseen tai suojelupoliisi toteaisi, että sillä olisi itsellä mahdollisuus toteuttaa pyydetty toimenpide.

Ehdotettavan *2 momentin* mukaan Rajavartiolaitos voisi tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä suorittaa Rajavartiolaitokselle säädetyn tehtävän yhteydessä rajavartiolain (578/2005) 28 §:ssä tarkoitettuja toimenpiteitä, jotka olisivat välttämättömiä siviilitiedustelutehtävän kannalta. Toimenpiteitä voisi momentin perusteella toteuttaa suojelupoliisin tiedustelutehtävän edellyttämässä laajuudessa ja niille asetettaisiin välttämättömyysedellytys.

Rajavartiolain 28 §:ssä säädetään rajavalvontaa koskevista toimivaltuuksista. Pykälän 1 momentin mukaan rajavartiomiehellä on Schengenin rajasäännöstössä tarkoitetun rajavalvonnan suorittamiseksi oikeus ilman rikosepäilyä suorittaa momentin 1–11 kohdissa lueteltuja toimenpiteitä Schengenin rajasäännöstön edellyttämässä laajuudessa. Schengenin rajasäännöstön johdanto-osan 6 kohdan mukaan rajavalvonnan olisi autettava torjumaan laitonta maahanmuuttoa ja ihmiskauppaa ja ehkäisemään jäsenvaltioiden sisäiseen turvallisuuteen, yleiseen järjestykseen, kansanterveyteen ja kansainvälisiin suhteisiin kohdistuvat uhkat.

Rajavalvonnassa rajatarkastus voi vähimmäistarkastuksena yksinkertaisimmillaan olla henkilöllisyyden ja matkustusasiakirjojen tarkastamista sekä muiden maahantuloedellytysten täyttymisen varmistamista esimerkiksi kyselemällä matkan tarkoituksesta sekä sen varmistamista, että henkilöllä on riittävät varat ilmoitetun oleskelunsa ajalle. Siviilitiedustelutehtävän edellyttämällä laajuudella tarkoitettaisiin rajavartiolain 28 §:ssä säädettyjen toimenpiteiden, kuten esimerkiksi perusteellisemman tarkastuksen, toteuttamista laajemmin kuin esimerkiksi rajavalvonnassa olisi yksittäistapauksessa muuten tarpeen. Momentti ei rajoittaisi Rajavartiolaitoksen osallistumista ainoastaan rajavalvonnan yhteydessä toteutettaviin tehtäviin. Tarkoituksenmukaista olisi, että Rajavartiolaitos voisi suojelupoliisin pyynnöstä toteuttaa 28 §:ssä tarkoitettuja toimenpiteitä myös muiden tehtäviensä yhteydessä esimerkiksi silloin, kun se suorittaa vesiliikenteen valvontaa tai alustarkastuksia. Toimenpiteissä voisi esimerkiksi olla kyse henkilön hallussa olevien asiakirjojen, tämän mukana olevien tavaroiden tai hänen käyttämänsä

kulkuneuvon tarkastaminen tai siihen kohdistettava etsintä, tai henkilön matkustusasiakirjojen jäljentäminen esimerkiksi valokuvaamalla.

Toteutettavien toimenpiteiden tulisi aina olla välttämättömiä suojelupoliisin tiedustelutehtävän kannalta. Välttämättömyyttä arvioitaessa tulisi ottaa huomioon, olisiko pyydetty toimenpide välttämätön tiedustelutehtävän kannalta ja olisiko välttämätöntä, että sen suorittaisi Rajavartiolaitos. Välttämättömyys voisi tarkoittaa esimerkiksi sitä, ettei suojelupoliisin pyytämää toimenpidettä olisi mahdollista toteuttaa muussa yhteydessä tai, ettei suojelupoliisi voisi esimerkiksi asian kiireellisyyden vuoksi lähtökohtaisesti toteuttaa sitä itse. Rajavartiolaitos voisi lisäksi aina kieltäytyä pyydetyn toimenpiteen toteuttamisesta, mikäli se arvioisi, ettei sillä olisi sen toteuttamiseen tarvittavia edellytyksiä tai se voisi vaarantaa Rajavartiolaitoksen omien lakisääteisten tehtävien suorittamista. Rajavartiolaitoksen yhteistoiminnan suojelupoliisin kanssa tulisi alueellisesti kohdentua rajavartiolain 4 §:n mukaisesti.

Pykälän *2 momentissa* säädettäisiin lisäksi, että toimenpiteen kohteena oleva henkilö olisi velvollinen olemaan läsnä toimenpiteitä suoritettaessa enintään 12 tuntia kerrallaan ja toimenpiteen suorittamisesta päättäisi rajanylityspaikan esimies tai vähintään luutnantin arvoinen rajavartiomies. Koska momentissa viitattaisiin rajavartiolain 28 §:ssä tarkoitettuihin toimenpiteisiin, joiden toteuttamiseksi Rajavartiolaitokselle on säädetty 12 tunnin aika, olisi tarkoituksenmukaista säätää läsnäolovelvollisuus saman mittaiseksi. Toimenpiteistä voisi päättää rajanylityspaikan esimiehenä toimiva rajavartiomies sekä vähintään luutnantin arvoinen rajavartiomies, joilla katsotaan olevan koulutuksen ja kokemuksensa puolesta riittävä tietotaito päätöksen tekemiseen.

Ehdotettu pykälän *3 momentti* sisältäisi oikeuden 2 momentissa säädetyissä tilanteissa käyttää vääriä, harhauttavia tai peiteltyjä tietoja 2 momentissa tarkoitettujen toimenpiteiden suorittamiseksi silloin, kun se olisi välttämätöntä toimenpiteen paljastumisen estämiseksi. Suojelupoliisin tiedustelutehtävän suorittaminen ja tiedonhankinta sekä siinä käytettävät keinot ja menetelmät olisi kyettävä tarvittaessa suojaamaan niiden paljastumisen estämiseksi myös silloin kun Rajavartiolaitos oman tehtävänsä yhteydessä suorittaisi yksittäisiä toimenpiteitä. Väärien, harhauttavien tai peiteltyjen tietojen käyttämisen tarkoituksena olisi siis tarve olla paljastamatta tiedonhankinnan kohteelle, että rajavalvonnassa käytettävää toimivaltuutta vastaavaa toimivaltuutta käytetäänkin kokonaan tai osittain tiedustelutarkoituksessa. Rajavartiolaitos ei silloin olisi velvollinen esimerkiksi ilmoittamaan toimenpiteen kohteelle rajatarkastuksen laajuuteen vaikuttavaa tosiasiallista syytä. Päätöksen suojaamisesta voisi tehdä rajanylityspaikan esimiehenä toimiva rajavartiomies sekä vähintään luutnantin arvoinen rajavartiomies, joilla katsotaan olevan koulutuksen ja kokemuksensa puolesta riittävä tietotaito päätöksen tekemiseen.

Pykälän 4 momentin mukaan Rajavartiolaitoksen olisi luovutettava tässä pykälässä tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat käsittelemättöminä suojelupoliisille, sekä hävitettävä toimenpiteen suorittamisessa syntyneet tallenteet ja asiakirjat, jollei tietojen käsittely olisi tarpeen Rajavartiolaitokselle säädettyjen muiden tehtävien suorittamiseksi.

Koska Rajavartiolaitos voisi suorittaa tässä pykälässä tarkoitettuja tehtäviä Rajavartiolaitokselle säädetyn tehtävän yhteydessä olisi tarpeen säätää, että hävitysvelvollisuus ei koskisi sellaisia tallenteita ja asiakirjoja, joita Rajavartiolaitos tarvitsisi oman tehtävänsä suorittamiseksi, vaikka ne voisivat kuulua myös suojelupoliisille luovutettaviin tallenteisiin ja asiakirjoihin. Kumpikin viranomainen olisi silloin vastuussa tietojen säilyttämisestä ja niiden hävittämisestä oman sääntelynsä mukaisesti.

Rajavartiolaitoksella olisi kuitenkin aina oikeus kirjata omaan rekisteriinsä perustiedot tässä pykälässä tarkoitetun toimenpiteen ajankohdasta ja paikasta sekä suoritetusta toimenpiteestä tai tiedon sen suorittamatta jättämisestä.

57 §. *Kansainvälinen yhteistyö.* Poliisilain 5 a luvun 57 §:ää koskevassa ehdotuksessa muutettaisiin *kolmannessa momentissa* esiintyvä termi *vieraan valtion toimivaltainen viranomainen* muotoon *ulkomainen toimivaltainen viranomainen*. Nykyisessä turvallisuuspoliittisessa keskustelussa termi vieras valtio on vakiintunut tarkoittamaan Suomen kansallista turvallisuutta uhkaavaa valtiota. Pykälässä tarkoitettu yhteistyö tapahtuu kuitenkin Suomelle ei-vihamielisen valtion toimivaltaisen viranomaisen kanssa. Asiantilan selventämiseksi vieraan valtion termi tulisi muuttaa termiksi ulkomainen, joka on edellistä neutraalimpi ilmaus.

Pykälän 3 momenttia muutettaisiin. Pykälän 3 *momentin* mukaan vieraan valtion toimivaltaisella virkamiehellä on oikeus suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa käyttää niitä tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ssä. Säännöksestä poistettaisiin viittaus tiettyjen tiedustelumenetelmien käyttöön. Sääntelyn alkuperäisenä tarkoituksena on ollut, että vieraan valtion viranomainen voisi käyttää mainittuja tiedustelumenetelmiä, koska ne merkitsevät vain vähäistä puuttumista perusoikeuksiin, eikä yhdelläkään niistä kajottaisi luottamuksellisen viestin salaisuuden suojaan. Suojelupoliisin ohjauksessa ja valvonnassa toimiva vieraan valtion eli ulkomainen virkamies toimii suojelupoliisin tiedonhankintaoperaatiossa avustavassa roolissa. Ulkomaisella virkamiehellä voi olla sellaista osaamista tai muita ominaisuuksia, joita suomalaisella virkamiehellä ei ole ja jota tarvitaan operaation onnistuneeksi toteuttamiseksi. Kansainvälisen yhteistyön käytännössä on kuitenkin havaittu, että ulkomaisen toimivaltaisen viranomaisen avustamismahdollisuutta tarvitaan myös muissa kuin voimassa olevassa laissa lueteltujen tiedustelumenetelmien käytössä. Yhteistyössä toteutettavien tiedustelumenetelmien luettelo korvattaisiin yleisemmällä ilmauksella, joka mahdollistaisi kaikkien tiedustelumenetelmien käytön yhteisissä tiedusteluoperaatioissa.

7.2 Laki tietoliikennetiedustelusta siviilitiedustelussa

4 §. *Tietoliikennetiedustelun käytön edellytykset.* Pykälässä säädetään tietoliikennetiedustelun käytön edellytyksistä, ja pykälän 2 momenttia tarkistettaisiin. Pykälän 1 momentin mukaan tietoliikennetiedustelun käytön yleisenä edellytyksenä on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta, eikä tietoja ole hankittavissa muulla tiedustelumenetelmällä. Pykälän 2 momentin mukaan, jos tietoliikennetiedustelun hakuehtojen käyttö koskee ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, tietoliikennetiedustelun käytön tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Pykälän *2 momenttia* muutettaisiin niin, että tietoliikennetiedustelun käytön matalampaa edellytyskynnystä voitaisiin soveltaa tilanteissa, joissa tietoliikennetiedustelun tarkoituksena on kerätä valtiollisen toimijan tai siihen rinnastuvan toimijan tietoliikennettä, eli toisin sanoen, kun tiedonhankinnan kohteena on vieras valtiollinen toimija. Momentista poistettaisiin maininta hakuehdoista. Voimassa olevan pykälän toisen momentin sanamuoto ”*Jos tietoliikennetiedustelun hakuehtojen käyttö koskee ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä*” muutettaisiin kuuluvaksi : ”*Jos tietoliikennetiedustelun kohteena on valtiollinen toimija tai siihen rinnastuva toimija”.*

Luvan toimivaltuuden käyttöön myöntää tuomioistuin. Merkitystä tuomioistuimen edellytysharkinnassa ei olisi sillä, voiko siinä tietoliikenteessä, johon hakuehtoja vertaillaan, kulkea muutakin kuin valtiollista tietoliikennettä, vaan ainoastaan sillä, koskeeko tuomioistuimen lupa valtiollisen toimijan tai siihen rinnastuvan tahon ja sen tietoliikenteen tietoliikennetiedustelua.

Valtiollisen toimijan ja muiden toimijoiden tietoliikenteen sekoittuneisuuden viestintäverkossa ei ratkaisisi tapaukseen sovellettavaa edellytyskynnystä, vaan edellytyskynnyksen tulisi

määräytyä sen perusteella, kyetäänkö tietoliikennetiedustelun hakuehtoperusteisen vertailun avulla suodattamaan automaattisen ja manuaalisen jatkokäsittelyn kohteeksi pelkästään valtiollisen tahon liikenne. Se laajempi tietoliikennevirta, johon hakuehtoja verrataan, mutta joka ei ohjaudu jatkokäsittelyyn, ei missään vaiheessa päädy tiedusteluviranomaisten haltuun.

Asetelmaa voitaneen joiltain osin verrata yleisessä viestintäverkossa toteutettavaan perinteiseen telekuunteluun. Telekuuntelun tavanomaisena kohdistamisperusteena, toisin sanoen siinä käytettävänä ”hakuehtona”, on tietyn henkilön käyttämän telepäätelaitteen yksilöivä tieto. Siinä viestintäverkon osassa, josta kyseisen telepäätelaitteen viestiliikenne erotetaan, kulkee myös lukuisten muiden telepäätelaitteiden viestiliikennettä. Telekuuntelulla katsottaneen tästä huolimatta puututtavan ainoastaan sen tahon viestintäsalaisuuteen, jonka puhelinliikenne käytössä olevan kohdentamisperusteen avulla ohjataan syrjään kuunneltavaksi, ei sen sijaan kyseisen viestintäverkon muiden käyttäjien yksityisyyden suojaan.

5 §. *Tietoliikennetiedustelun kohdistaminen.* Pykälää muutettaisiin niin, että sen sisällöksi jäisi voimassa olevan pykälän 1 momentti edellä nykytilan kuvauksessa esitetyillä perusteilla ja muutettuna ottaen huomioon ehdotetut 10 a ja 10 c §:t.

Voimassa olevan lain 5 §:n 1 momentin mukaan tietoliikennetiedustelu kohdistetaan tietoliikenteen automatisoidun erottelun avulla. Automatisoitu erottelu perustuu 7 tai 9 §:n mukaisessa menettelyssä hyväksyttyjen hakuehtojen käyttöön. _Tämän osalta säännös säilyisi muuttumattomana.

Pykälän 2 momentin mukaan 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.

Pykälän 3 momentin mukaan hakuehtona ei saa käyttää Suomessa olevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

Kumottavaksi ehdotetussa *2 momentissa* säädetty sisällöllisen hakuehdon käytön kielto haittaa merkittävästi tietoliikennetiedustelun tehokkuutta, ja se johtaa tilanteisiin, joissa tiedusteluviranomaisten haltuun tarpeettomasti päätyy sellaista tiedustelun kohteena olevan uhkan kannalta epäolennaista sivullista viestintää, joka nauttii luottamuksellisen viestin salaisuuden suojaa.

Viestien semanttiseen sisältöön kohdistuvat hakuehdot ovat monessa tapauksessa mahdollista muotoilla sellaisiksi, että ne erottelevat vähemmän ja kohdennetummin tietoliikennettä tietoliikennetiedustelun automaattisen ja manuaalisen käsittelyn piiriin kuin nykyisin nimenomaisesti sallitut, esimerkiksi ip-osoitealueita, autonomisten järjestelmien numeroita ja domain-nimiä koskevat hakuehdot. Salauksen yleistymisestä huolimatta viestin sisällön käyttäminen hakuehtona mahdollistaa keräyksen tarkentamisen. Tällöin tiedusteluviranomaisille ei edes väliaikaisesti päätyisi niin useasti sellaisia viestejä, jotka eivät ole tiedustelutiedon hankinnan kannalta relevantteja.

Siviilitiedustelulainsäädännön esitöissäkin todetusti tietoliikennetiedustelusta säätäneiden eurooppalaisten vertailuvaltioiden lainsäädännöissä ei ole asetettu rajoituksia tai esteitä käyttää sisällöllisiä hakuehtoja, vaan ”sisällöllisten hakuehtojen käytölle asetetut rajoitukset ovat

omintakeinen suomalainen ratkaisu". Kyseinen ratkaisu toimii tällä hetkellä nimenomaisten tarkoitusperiensä vastaisesti.

Pykälän *3 momentissa* säädetty kielto käyttää telepäätelaitteen tai teleosoitteen yksilöiviä tietoja tietoliikennetiedustelun hakuehtona ehdotetaan myös kumottavaksi.

Lain 4 § koskee tietoliikennetiedustelun käytön edellytyksistä. Pykälän 1 momenttia täydennettiin lakiehdotuksen eduskuntakäsittelyn aikana niin, että tietoliikennetiedustelun käyttö edellyttää muun ohella myös, että hankittavat tiedot eivät ole hankittavissa muulla tiedustelumenetelmällä. Koska kyseisen ns. viimesijaisuusedellytyksen soveltaminen jo sellaisenaan ratkaisee kysymyksen tietoliikennetiedustelun ja teletiedustelumenetelmien (ynnä kaikkien muidenkin tiedustelumenetelmien) välisestä suhteesta, on lain 5 §:n 3 momentissa säädetty erillinen kielto käyttää hakuehtona Suomessa olevan telepäätelaitteen tai teleosoitteen yksilöivää tietoa tarpeeton.

Lisäksi on tilanteita, joissa teletiedustelumenetelmien kuten telekuuntelun käyttäminen on mahdotonta, mutta telepäätelaitteen tai teleosoitteen yksilöivää tietoa olisi mahdollista käyttää tietoliikennetiedustelun hakuehtona sikäli kuin tämä olisi sallittua. Esimerkiksi sähköpostiosoite on oikeudelliselta luonteeltaan tietoliikennetiedustelulain 5 §:n 3 momentissa mainittu teleosoite. Telekuuntelua ei ole mahdollista kohdentaa ja toteuttaa pelkästään sähköpostiosoitetta koskevan tiedon avulla, mutta tietoliikennetiedustelussa sähköpostiosoitetta koskevan tiedon käyttö hakuehtona olisi mahdollista. Lain 5 §:n 3 momentin nimenomainen kielto käyttää Suomessa olevan henkilön hallussa olevaa teleosoitetta hakuehtona estää tämän.

Edellä käsiteltyä lain 4 §:n 1 momentin ns. viimesijaisuusedellytystä ei sovelleta sellaiseen tietoliikennetiedusteluun, joka kohdistuu yksinomaan valtiollisiin toimijoihin. Lain 4 §:n 2 momentin (jota edellä ehdotetaan muutettavaksi) mukaan, jos tietoliikennetiedustelun hakuehtojen käyttö koskee ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, tietoliikennetiedustelun käytön tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Tällaisessa tietoliikennetiedustelussa se seikka, että telekuuntelua olisi mahdollista (joskin kohtuuttoman hankalaa) käyttää, ei sulje pois tietoliikennetiedustelun käytön mahdollisuutta. Lain 5 §:n 3 momentissa säädetty kielto kuitenkin estää tietoliikennetiedustelun käytön.

Lain esitöissä 5 §:n 3 momentissa säädettyä kieltoa perustellaan tarpeella minimoida vaikutus sivullisten tietoliikenteeseen. Perustelu ei ole käypä, koska käytettäessä telepäätelaitteen tai teleosoitteen yksilöivää tietoa tietoliikennetiedustelun hakuehtona, hakuehto ei voine erotella jatkokäsittelyyn sivullista tietoliikennettä. Telepäätelaitteen tai teleosoitteen yksilöivä tieto lienee tarkin ajateltavissa oleva hakuehto.

7 §. *Tietoliikennetiedustelua koskeva tuomioistuimen lupa*. Pykälän *3 momenttia* muutettaisiin. Lupa tietoliikennetiedusteluun voitaisiin myöntää edelleen voimassa olevan lain mukaisesti kuudeksi kuukaudeksi kerrallaan. Säännösehdotuksen mukaan lupa voisi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voisi olla kuutta kuukautta pidempi.

Käytännössä tämä voi tarkoittaa esimerkiksi tilannetta, jossa käytettäisiin valtiollisen toimijan tietoliikenteen tiedustelussa ehdotetun 10 a §:n 3 momentin ja 10 c §:n 4 momentin perusteella tallennettuja tietoja.

10 §. *Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa.* Pykälää ehdotetaan muutettavaksi niin, että sen *1 momentissa* säädettäisiin siitä, että puolustusvoimien tiedustelulaitos toteuttaisi tietoliikennetiedustelun teknisesti suojelupoliisin

puolesta keräämällä tämän lain 7, 9, 10 b ja 10 d §:ssä tarkoitettujen lupien tai päätösten mukaiset tiedot tietoliikenteessä. Lain 7 §:ssä säädetään tietoliikennetiedustelua koskevasta tuomioistuimen luvasta ja 9 §:ssä päätöksenteosta kiireellisessä tilanteessa. Ehdotettu 10 b § koskisi teknisten tietojen käsittelystä päättämistä viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi, ja ehdotettu 10 d § hakuehtojen määrittämisestä päättämistä.

Voimassa olevan tietoliikennetiedustelusta siviilitiedustelussa annetun lain 10 §:n 1 momentin mukaan tietoliikennetiedustelun teknisenä toteuttajana toimii Puolustusvoimien tiedustelulaitos. 3 momentin mukaan suojelupoliisi toimittaa 7 tai 9 §:ssä tarkoitetun päätöksen Puolustusvoimien tiedustelulaitokselle, joka suorittaa 5 §:n mukaiset toimenpiteet suojelupoliisin puolesta. Puolustusvoimien tiedustelulaitos toimittaa toimeksiannon toteuttamisella erottelemansa tietoliikenteen suojelupoliisille.

Pykälän *4 momentin* sisältö säilyisi ehdotetussa pykälässä ennallaan. Sen mukaan suojelupoliisin muuhun yhteistyöhön sotilastiedusteluviranomaisen kanssa sovelletaan poliisilain 5 a luvun 54 §:ää.

10 a §. *Teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi*. Pykälä olisi uusi. Pykälässä säädettäisiin teknisten tietojen käsittelystä viestintäverkon osan tunnistamisen lisäksi teknisten tietojen käsittelystä tietoliikenteen reitittymisen ja muutosten seuraamiseksi.

Ehdotetun *1 momentin* mukaan suojelupoliisi voisi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 66 §:ssä tarkoitettujen teknisten tietojen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaisi tämän lain 10 b §:ssä tarkoitetun tuomioistuimen luvan mukaisen teknisten tietojen keräämisen ja luovuttaisi kyseiset tiedot suojelupoliisille.

Voimassa olevan tietoliikennetiedustelusta siviilitiedustelussa annetun lain 10 §:n 2 momentin mukaan suojelupoliisi voi antaa puolustusvoimien tiedustelulaitokselle toimeksiannon sotilastiedustelulain 66 §:ssä tarkoitettuun teknisten tietojen käsittelyyn. Sotilastiedustelulain mainittua pykälää (66 §) ehdotetaan muutettavaksi HE……./2026:ssa. Sotilastiedustelulain 66 §:ssä säädettäisiin voimassa olevan lain teknisten tietojen käsittelyn lisäksi teknisten tietojen käsittelystä tietoliikenteen reitittymisen ja muutosten seuraamiseksi.

Edelleen voimassa olevan lain 10 §:n 2 momentin mukaan puolustusvoimien tiedustelulaitos hakee suojelupoliisin puolesta sotilastiedustelulain 67 §:n mukaisen luvan teknisten tietojen käsittelyyn sekä toimittaa mainitun lain 66 §:n 2 momentissa tarkoitetun tilastollisen analyysin tuloksen suojelupoliisille sen jälkeen, kun se on saanut luvan teknisten tietojen käsittelyyn ja toteuttanut luvan mukaiset toimenpiteet. Sotilastiedustelulain mainittua pykälää (67 §) ehdotetaan muutettavaksi HE……./2026:ssa.

Ehdotetun *2 momentin* mukaan suojelupoliisilla olisi oikeus tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä tilastollista analyysia varten tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan ja tietoliikenteen reitittymisen ja muutosten seuraamiseksi.

Ehdotetun *3 momentin* mukaan suojelupoliisi voisi tallentaa puolustusvoimien tiedustelulaitoksen luovuttamat tekniset tiedot enintään 18 kuukauden ajaksi, minkä jälkeen ne olisi viimeistään hävitettävä. Tallennettuja tietoja voitaisiin käyttää tämän pykälän 1 momentissa säädettyyn tarkoitukseen.

Ehdotetun *4 momentin* mukaan suojelupoliisilla ja puolustusvoimien tiedustelulaitoksella olisi oikeus pyynnöstä tai oma-aloitteisesti luovuttaa tilastollisen analyysin tuloksia toisilleen siviili- ja sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi poliisilain 5 a luvun 54 §:ssä ja sotilastiedustelulain 17 §:ssä tarkoitetulla tavalla.

10 b §. *Teknisten tietojen käsittelystä päättäminen viestintäverkon osan sekä tietoliikenteen reitittymien ja muutosten tunnistamiseksi.* Pykälä olisi uusi ja se liittyisi edellä 10 a §:ssä säädettyyn. Pykälän otsikossa viitattaisiin 10 a §:n mukaisesti viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamisesta päättämiseen.

Pykäläehdotuksen *1 momentin* mukaan tuomioistuin päättäisi teknisten tietojen käsittelystä viestintäverkon osan tunnistamiseksi tai tietoliikenteen reitittymisen ja muutosten tunnistamiseksi tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Pykäläehdotuksen *2 momentin* mukaan lupa voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan. Ehdotettu kuuden kuukauden määräaika olisi perusteltu ottaen huomioon sen, että toimivaltuuden käytöllä ei hankita muuta kuin tietoliikenteen teknistä tietoa. Määräaika olisi myös yhteneväinen varsinaisen tietoliikennetiedustelun määräaikojen kanssa. Luvan voimassaoloaika alkaisi kulua luvan antopäivästä lähtien. Säännöksen mukaan lupa voisi koskea myös todettua luvan antopäivää edeltävää aikaa, joka voisi olla kuutta kuukautta pidempi.

Pykäläehdotetun *3 momentin* mukaan vaatimuksessa ja päätöksessä olisi mainittava momentin 1 kohdan mukaan maantieteellinen alue tai verkkoalue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan, taikka kohde, jonka tietoliikenteen reitittymistä tai muutosta seurataan. Kohteella tarkoitettaisiin tiedustelun kohteena olevaa toimijaa, jonka tietoliikenteen reitittymisestä tai muutoksista olisi hankittava tietoa.

Momentin toisen kohdan mukaan olisi mainittava viestintäverkon osat, joista tietoa haetaan ja kolmannen kohdan mukaan käsittelyä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt suojelupoliisin päällystöön kuuluva poliisimies. Se on olennaista, että tähän tehtävään on määrätty tiedustelumenetelmien käyttöön erityisesti perehtynyt virkamies eli suojelupoliisin päällystöön kuuluva poliisimies. Momentin 4 kohdan mukaan olisi mainittava suunnitelma käsittelyn toteuttamisesta. Suunnitelman laatimista olisi sovellettava myös momentin 1 kohtaan, eli tietoliikenteen reitittymisen ja muutosten seurantaan. Näin ollen suunnitelmassa olisi tehtävä selkoa siitä, miten seuranta tullaan tarkemmin ottaen toteuttamaan.

10 c §. *Tietoliikennetiedustelu hakuehtojen määrittämiseksi*. Pykäläehdotuksen *1 momentin* mukaan suojelupoliisi voisi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 67 a §:n 1 momentissa tarkoitetun tietoliikenteen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaisi 10 d §:ssä tarkoitetun tuomioistuimen luvan mukaisen tietoliikenteen keräämisen ja luovuttaisi sen suojelupoliisille.

Sotilastiedustelulakiin on ehdotettu uutta 67 a §:ää (HE /2026), jonka 1 momentin mukaan” Puolustusvoimien tiedustelulaitos voi tietoliikennetiedustelun tarkemmaksi kohdentamiseksi kerätä ja tallentaa satunnaista tietoliikennettä Suomen rajan ylittävän viestintäverkon osasta ja käsitellä sitä, jos se on välttämätöntä kohdetta kuvaavien uusien hakuehtojen määrittämiseksi. Kerättävän ja tallennettavan tietoliikenteen määrä ei saa ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista”.

Ehdotettu 10 c § tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin olisi uusi ja siinä viitattaisiin sotilastiedustelulakiin ehdotettuun uuteen 67 a §:ään, jossa säädettäisiin tietoliikennetiedustelusta hakuehtojen määrittämiseksi. Mainitussa 67 a §:ssä säädettäisiin mahdollisimman kohdennetussa tietoliikennetiedustelussa tarpeellisten uusien hakuehtojen määrittämisestä. Sotilastiedustelulakia koskevan hallituksen esityksen 1. lakiesityksen 67 a §:n yksityiskohtaisissa perusteluissa todetaan, että ”termillä määrittäminen viitattaisiin siihen, että sinänsä tiedustelun kohteet pysyvät voimassa olevan lain mukaisesti samana, mutta esimerkiksi kohteiden viestintäverkossa käyttämä teknologia ja viestinnän keinot saattavat muuttua. Etenkin vallitsevassa turvallisuuspoliittisessa tilanteessa teknologian kehityssykli on nopeutunut ja uutta teknologiaa ja uusia menetelmiä pyritään ottamaan käyttöön aiempaa nopeampaan tahtiin. Siviilitiedustelun kohteena olevat toimijat muuttavat alituiseen toimintaansa ja kehittävät uusia toimintatapoja. Uuden toimivaltuuden tarkoituksena on riittävän erottelukykyisten hakuehtojen määrittäminen. Nykytilassa kaikissa tilanteissa uusien hakuehtojen määrittäminen tapahtuu käytännössä varsinaisen tietoliikennetiedustelun yhteydessä, mutta kohteena olevan toimijan vaihtaessa viestintään käytettävää menetelmää, voi tiedon saaminen kohteesta lakata yllättäen. Toimivaltuuden käyttö olisi sidottu välttämättömyyteen. Välttämättömyyden määritelmän mukaisesti uusien hakuehtojen määrittämisen olisi toisin sanoen oltava käytännössä mahdotonta muilla keinoin, sen olisi vaadittava oleellisesti enemmän voimavaroja tai muiden keinojen käyttö viivyttäisi tiedonhankintaa kohtuuttomasti. Esimerkiksi tilanteessa, jossa kohteena olevan toimijan tietoliikenteestä ei enää yllättäen saada hankittua tietoa käytetyillä hakuehdoilla tietäen kuitenkin kohteen viestivän vakituiseen, voidaan olettaa kohteen ottaneen käyttöön uuden viestinnän keinon, jonka takia käytössä olisi oltava uuteen viestinnän keinoon kohdistuvia hakuehtoja. Tilanteessa tieto toki voitaisiin hankkia muilla tiedustelumenetelmillä, mutta esimerkiksi tiedustelumenetelmien käyttöä ulkomailla ei voida pitää realistisena vaihtoehtona jo pelkästään virkamiesten hengen ja terveyden suojaamisen, saati tiedusteluoperaatioon käytettävien resurssien ja ajan kannalta. ”

Pykäläehdotuksen *2 momentin* mukaan suojelupoliisilla olisi oikeus tallentaa luovutettua tietoliikennettä ja käsitellä sitä, jos se olisi välttämätöntä kohdetta kuvaavien hakuehtojen määrittämiseksi. Hakuehtojen määrittämisessä ei saisi käsitellä viestin merkityssisällössä olevia tietoja. Hakuehtojen määrittämisessä voitaisiin käyttää ehdotetun 10 a §:ssä tarkoitettuja teknisiä tietoja. Säännöksellä suojattaisiin viestin merkityksellistä sisältöä eikä sen selvittäminen ole toimivaltuuden tarkoituksena. Lisäksi säännöksen toimivaltuudella ei voitaisi selvittää tietyn henkilön toimintaa.

Pykäläehdotuksen 3 *momentin* mukaan suojelupoliisi voisi tallentaa puolustusvoimien tiedustelulaitoksen luovuttaman tietoliikenteen enintään 12 kuukauden ajaksi, minkä jälkeen se olisi viimeistään hävitettävä. Säilytettävien tietojen rajaus ei koskisi määritettyjä hakuehtoja, vaan määritettyjä hakuehtoja voitaisiin käyttää niin pitkään kuin ne toimivat tarkoitetulla tavalla.

10 d §. *Hakuehtojen määrittämisestä päättäminen.* Pykälä olisi uusi. Pykäläehdotuksen *1 momentin* mukaan tuomioistuin päättäisi hakuehtojen määrittämisestä tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Pykäläehdotuksen *2 momentin* mukaan lupa voitaisiin antaa luvan antopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa voisi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi. Käytännössä tämä tarkoittaisi tilannetta, jossa käytettäisiin hakuehtojen määrittämisessä ehdotetun 10 a §:n 2 momentissa tarkoitettuja tallennettuja teknisiä tietoja tai 10 c §:n 4 momentissa tarkoitettuja tietoja.

Pykälän *3 momentissa* olisi säädetty vaatimuksessa ja päätöksessä mainittavat seikat. Momentin *1 kohdan* mukaan vaatimuksessa ja päätöksessä olisi mainittava siviilitiedustelun kohde, jota varten hakuehtoja määritettäisiin.

Momentin 2 *kohdan* mukaan vaatimuksessa ja päätöksessä olisi mainittava kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritettäisiin ja perustelut sille; Jotta sähköinen viestintä ohjautuisi haluttuun määränpäähän tarkoitetulla tavalla, vaatii tietoliikenne säännöstöjä, eli protokollia. Protokollat muun muassa pilkkovat tiedoston tiettyyn muotoon ja salaavat tietoliikenteen tietyllä tavalla. Tämä näkyy tietoliikennevirrassa tiettynä säännönmukaisuutena tai ominaispiirteenä. Säännönmukaisuuksia ja ominaispiirteitä voidaan tunnistaa esimerkiksi protokollapinossa käytettävän yksittäisen protokollan toiminnan ominaispiirteestä, mutta varsinaista hakuehtoa ei voida kohdistaa tämän perusteella.

Tiedossa voisi olla esimerkiksi vieraan valtion uhkatoimijan käyttämiä verkko-osoitteita tai fyysisiä sijainteja, mutta kommunikointimenetelmän tarkemmat tiedot ovat toistaiseksi tuntemattomia, jolloin tarkkoja hakuehtoja ei voida määrittää. Uusia uhkatoimijaan rajautuvia hakuehtoja voitaisiin määrittää keräämällä tietoliikennettä, ja etsien em. sijainneista tulevasta tietoliikenteestä uhkatoimijaan viittaavia kommunikointitekniikoita.

Ominaispiirrettä vastaavan tietoliikenteen löytäminen edellyttää usein manuaalista työtä, jotta säännönmukaisuutta tai ominaispiirrettä vastaava tietoliikenne löydetään. Tietoliikenteen tavuvirrasta hakuehtojen määrittäminen ei edellytä tietoliikenteen purkamista muotoon, josta ilman merkittävää tietoteknistä osaamista oleva henkilö voisi selvittää viestin sisällön.

Momentin 3 *kohdan* mukaan vaatimuksessa ja päätöksessä olisi mainittava viestintäverkon osat, joista tietoa haettaisiin. Näitä olisivat viestintäverkon osat, kuten kaapeleiden kuidut, joihin tietoliikennetiedustelua hakuehtojen määrittämiseksi kohdennettaisiin.

Momentin 4 *kohdan* mukaan vaatimuksessa ja päätöksessä olisi mainittava suunnitelma hakuehtojen määrittämisestä. Suunnitelmassa olisi tehtävä tarkemmin selkoa esimerkiksi siitä, että miten hakuehtojen määrittäminen toteutettaisiin ja minkälaisin keinoin. Suunnitelmassa olisi myös kuvattava sitä, miten tarkempaan käsittelyyn päätyisi mahdollisimman vähän viestinnän merkityksellistä sisältöä ja miten yksityisyyden suojasta huolehditaan mahdollisimman pitkälle.

Momentin 5 *kohdan* mukaan vaatimuksessa ja päätöksessä olisi mainittava luvan voimassaoloaika kellonajan tarkkuudella ja *7 kohdan* mukaan olisi mainittava hakuehtojen määrittämistä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

Momentin 7 *kohdan* mukaan tuomioistuin voisi asettaa päätöksessään tietoliikennetiedustelulle rajoituksia ja ehtoja. Jos tällaisia rajoituksia ja ehtoja olisi tiedossa jo vaatimusta laadittaessa, niin ne olisi syytä kirjata jo vaatimukseen. Rajoituksia ja ehtoja voitaisiin asettaa esimerkiksi sille, kuinka hakuehtoja saadaan muodostaa niiden hakuehtojen luokkien puitteissa, joihin tuomioistuin myöntää luvan.

13 §. *Tallenteiden ja asiakirjojen tarkastaminen***.** Pykälää ehdotetaan kumottavaksi edellä tietoliikennetiedustelusta siviilitiedustelussa annetun lain 13 §:ää koskevassa nykytilan kuvauksessa todetun johdosta. Tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa säädetyt hävittämisvelvollisuudet jäisivät kuitenkin yhä voimaan, vaikka tallenteiden ja asiakirjojen tarkastamisvelvollisuus poistettaisiin. Jos suojelupoliisi havaitsee hallussaan olevasta aineistosta hävittämisvelvollisuuden alaista tietoa, tulisi sen hävittää se viipymättä.

20 §. *Tietoliikennetiedustelun käytöstä ilmoittaminen*. Pykälää ehdotetaan muutettavaksi edellä tietoliikennetiedustelusta siviilitiedustelussa annetun lain 20 §:ää koskevassa nykytilan kuvauksessa todetun johdosta.

Pykäläehdotuksen *1 momentin* mukaan tietoliikennetiedustelusta ei olisi velvollisuutta ilmoittaa.

Pykäläehdotuksen 2 *momentin* mukaan, jos tietoliikennetiedustelussa kuitenkin on selvitetty sellainen tieto, josta olisi velvollisuus tai oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla, ilmoitettaisiin tietoliikennetiedustelusta 12 §:ssä tarkoitetulle taholle noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei olisi, jos todistamiskiellon tai todistamatta jättämisoikeuden alainen tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

Lain 12 §:ssä säädetään tiedustelukiellosta ja sen mukaan 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.

Tietoliikennetiedustelun ilmoitusvelvollisuuden supistaminen ei rajoita jokaisen mahdollisuutta saattaa tutkittavaksi kysymystä siitä, onko häneen kohdistunut tietoliikennetiedustelua ja onko tiedonhankinta ollut lainmukaista.

Tiedustelutoiminnan valvonnasta annetun lain 12 §:n mukaan tiedustelutoiminnan kohteena ollut tai henkilö, joka epäilee, että häneen on kohdistettu tiedustelua, voi pyytää tiedusteluvalvontavaltuutettua tutkimaan häneen kohdistuneen tiedustelumenetelmän lainmukaisuuden. Lisäksi saman lain 11 §:n mukaan jokainen, joka katsoo, että tiedustelutoiminnassa on rikottu hänen oikeuksiaan tai menetelty muutoin lainvastaisesti, voi kannella tiedusteluvalvontavaltuutetun valvontavaltaan kuuluvassa asiassa.

7.3 Rajavartiolaki

3 §. *Rajavartiolaitoksen tehtävät.* Pykälän 3 momenttiin lisättäisiin säännös Rajavartiolaitoksen osallistumisesta siviilitiedusteluun. Rajavartiolaitoksen osallistumisesta siviilitiedusteluun säädettäisiin tarkemmin ehdotettavassa 25 b §:ssä ja toimivaltuuksista poliisilain 5 a lukuun ehdotetussa 55 a §:ssä.

25 b §. *Rajavartiolaitoksen osallistuminen siviilitiedusteluun.* Pykälä olisi uusi. Pykälässä säädettäisiin Rajavartiolaitoksen osallistumisesta siviilitiedusteluun.

Pykälän 1 momentissa säädettäisiin, että Rajavartiolaitos osallistuisi pyynnöstä siviilitiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä suojelupoliisin tiedustelutehtävien tukemiseksi. Tehtävä olisi Rajavartiolaitokselle uusi.

Poliisin hallinnosta annetun lain 10 §:n 1 momentin nojalla 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. Poliisilain 5 a luvussa säädetään suojelupoliisin suorittamasta tiedonhankinnasta ja tiedon hyödyntämisestä

kansallisen turvallisuuden suojaamiseksi, ylimmän valtiojohdon päätöksenteon tukemiseksi ja muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten (siviilitiedustelu). Siviilitiedustelun kohteista säädetään luvun 3 §:ssä.

Poliisilain 5 a luvun 58 §:ssä säädetään tiedustelutoiminnan yhteensovittamisesta. Siviili- ja sotilastiedustelutoiminta sovitetaan yhteen tasavallan presidentin, valtioneuvoston kanslian, ulkoministeriön, puolustusministeriön ja sisäministeriön sekä tarvittaessa muiden ministeriöiden ja viranomaisten kesken. Jos siviilitiedustelutoiminnalla arvioidaan olevan ulko- ja turvallisuuspoliittisia vaikutuksia, asia on valmistelevasti käsiteltävä edellä mainittujen viranomaisten kesken.

Sisäministeriö asettaa siviilitiedustelutoimintaa koskevat painopisteet. Ulko- ja turvallisuuspoliittisen ministerivaliokunnan ja tasavallan presidentin yhteinen kokous käsittelee valmistelevasti sekä siviili- että sotilastiedustelun painopisteet. Ulko- ja turvallisuuspolitiikkaa käsittelevän ministerivaliokunnan ja tasavallan presidentin yhteiselle kokoukselle saatetaan tiedoksi siviilitiedustelun painopisteet.

Rajavartiolaitos osallistuisi siviilitiedusteluun tukemalla suojelupoliisia tämän pyynnöstä tiedustelutehtävään liittyvän yksittäisen toimenpiteen suorittamisessa.

Sääntelyllä ei olisi tarkoitus muuttaa nykyisten tiedusteluviranomaisten asemaa, eikä Rajavartiolaitos olisi tehtävässään siviilitiedusteluviranomainen. Kyse olisi lyhytaikaisesta, yksittäisten tiedustelutehtävään liittyvien tehtävien tai toimenpiteiden suorittamisesta ja ne tapahtuisivat aina suojelupoliisin pyynnöstä. Pyyntö voisi olla tietyissä tilanteissa ennalta tehty tai se voisi tapahtua nopeampaa reagointia vaativissa tilanteissa viranomaisten välisten päivystysjärjestelyjen kautta.

Pykälän 2 momentti sisältäisi informatiivisen viittauksen siitä, että Rajavartiolaitoksen toimivaltuuksista siviilitiedusteluun osallistumisessa säädettäisiin poliisilaissa.

7.4 Laki henkilötietojen käsittelystä Rajavartiolaitoksessa

32 §. *Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle.* Pykälään lisättäisiin uusi 3 momentti, jossa säädettäisiin radioteknisen valvonnan tietojen luovuttamisesta salassapitosäännösten estämättä suojelupoliisille laissa säädettyjä tehtäviä varten. Kyse olisi henkilötiedoista ja muista tiedoista, joita Rajavartiolaitos käsittelee lain 15 b §:n mukaisesti radioteknisen valvonnan suorittamiseksi rajavartiolain 29 a–29 c §:ssä säädetyin edellytyksin. Radioteknisellä valvonnalla tarkoitetaan rajavartiolain 29 a §:n 1 momentin mukaan muulla teknisellä laitteella kuin tutkalla tapahtuvaa radiotaajuisten sähkömagneettisten aaltojen ja radiolaitteiden havaitsemista, tunnistamista, paikantamista, yksilöintiä ja seurantaa sähkömagneettisten aaltojen ominaisuuksien avulla. Rajavartiolain 29 b §:ssä säädetään sähköisen viestinnän tietojen käsittelystä radioteknisessä valvonnassa ja 29 c §:ssä radioteknisen valvonnan tietojen käsittelystä ja hävittämisestä.

7.5 Rikoslaki

7 §. *Valtionrajarikos.* Pykälän 2 momentin mukaan valtionrajanrikoksesta ei tuomittaisi ulkomaalaista, joka on tehnyt valtionrajarikoksen poliisilain 5 a luvun 25 §:n 5 momentin perusteella. Kyse on tilanteista, joissa Suomea avustanut henkilö joutuu hengen ja terveyden vaaraan lähtömaassaan ja henkilön hengen ja terveyden suojaamiseksi on välttämätöntä saada kyseinen henkilö pois lähtömaastaan. Tilanteissa kohtuussyistä ja selvyyden vuoksi olisi aihetta säätää erikseen valtionrajarikosta koskevasta syytevapaudesta.

Poistamalla edellä viitatuilta osin teon rangaistavuus, henkilö ei syyllistyisi suojelupoliisin hänelle poliisilain 5 a luvun 25 §:n 5 momentin perusteella antamien väärien asiakirjojen käytöllä rikoslain 17 luvun 7 §:ssä tarkoitettuun tekoon. Toisaalta henkilö voitaisiin joutua järjestämään asian sensitiivisyyden vuoksi Suomen rajan yli muuten kuin virallisen rajaylityspaikan kautta.

Tilanteissa henkilö saattaa jäädä Suomeen, mikä edellyttäisi normaaleja maahanmuuttoprosesseja tai turvapaikanhakua, mutta tilanteissa Suomi saattaisi olla myös vain kauttakulkumaa, josta henkilö siirretään kolmanteen valtioon.

7.6 Laki viranomaisten toiminnan julkisuudesta

31 §. *Viranomaisen asiakirjan salassapidon lakkaaminen*. Julkisuuslain 31 §:n 2 momenttiin lisättäisiin sääntely siitä, että julkisuuslain 24 §:n 1 momentin 1 kohdassa salassa pidettäväksi säädetyn asiakirjan ja 2 kohdassa tarkoitetun ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevan asiakirjan salassapitoaika olisi 40 vuotta. Sisäministeriön ja suojelupoliisin 9 kohdassa sekä sotilastiedustelun 10 kohdassa salassa pidettäväksi säädetyn asiakirjan salassapitoaika olisi 60 vuotta.

Julkisuuslain 31 §:n 1 momentin mukaan viranomaisen asiakirjaa ei saa pitää salassa, kun salassapidolle laissa säädetty tai lain nojalla määrätty aika on kulunut tai kun asiakirjan salassa pidettäväksi määrännyt viranomainen on peruuttanut salassapitoa koskevan määräyksen.

Pykälän 2 momentin nykyisen sanamuodon mukaan viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty tai lain nojalla määrätty. Yksityiselämän suojaamiseksi 24 §:n 1 momentin 24–32 kohdassa salassa pidettäväksi säädetyn asiakirjan tai niitä vastaavan muussa laissa salassa pidettäväksi säädetyn tai muun lain nojalla salassa pidettäväksi määrätyn asiakirjan salassapitoaika on 50 vuotta sen henkilön kuolemasta, jota asiakirja koskee tai, jollei tästä ole tietoa, 100 vuotta. Momenttiin lisättäisiin erityiset säännökset eräiden salassa pidettävien tietojen pidemmästä salassapitoajasta kuten edellä on todettu.

Julkisuuslain 24 §:n 1 momentin 1 kohdan mukaan salassa pidettäviä asiakirjoja ovat valtioneuvoston ulkopoliittisia asioita käsittelevän valiokunnan asiakirjat, jollei valiokunta toisin päätä, sekä ulkoasioita hoitavan ministeriön ja Suomen edustustojen poliittiset tilannearvioinnit, poliittisista tai taloudellisista suhteista toisen valtion kanssa käytyjä neuvotteluja koskevat asiakirjat ja ulkoasiainhallinnon alaan kuuluvat salakirjoitetut viestit, jollei asianomainen ministeriö toisin päätä.

Julkisuuslain 24 §:n 1 momentin 2 kohdan nojalla salassa pidettäviä ovat muut kuin 1 kohdassa tarkoitetut asiakirjat, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön, asiakirjat, jotka liittyvät kansainvälisessä lainkäyttö- tai tutkintaelimessä tai muussa kansainvälisessä toimielimessä käsiteltävään asiaan, ja asiakirjat, jotka koskevat Suomen valtion, Suomen kansalaisten, Suomessa oleskelevien henkilöiden tai Suomessa toimivien yhteisöjen suhteita toisen valtion viranomaisiin, henkilöihin tai yhteisöihin, jos tiedon antaminen niistä aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai edellytyksille toimia kansainvälisessä yhteistyössä. On otettava huomioon, että tasavallan presidentin kansliasta annetun lain (100/2012) 83 §:n 1 momentin mukaan tasavallan presidentin ja kanslian asioiden ja asiakirjojen julkisuudesta on voimassa, mitä viranomaisten toiminnan julkisuudesta annetussa laissa säädetään.

Julkisuuslain 24 §:n 1 momentin 9 kohdan mukaan salassa pidettäviä viranomaisen asiakirjoja ovat, jollei erikseen toisin säädetä, suojelupoliisin ja muiden viranomaisten asiakirjat, jotka koskevat valtion turvallisuuden ylläpitämistä, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna valtion turvallisuutta. Pykälän 1 momentin 10 kohdan mukaan salassa pidettäviä ovat asiakirjat, jotka koskevat sotilastiedustelua, puolustusvoimien varustamista, kokoonpanoa, sijoitusta tai käyttöä taikka muuta sotilaallista maanpuolustusta taikka maanpuolustusta palvelevia keksintöjä, rakenteita, laitteita tai järjestelmiä taikka maanpuolustuksen kannalta muutoin merkityksellisiä kohteita taikka puolustusvalmiuteen varautumista, jollei ole ilmeistä, että tiedon antaminen niistä ei vahingoita tai vaaranna maanpuolustuksen etua.

Perustuslain 12 §:stä johtuu, että julkisuutta voidaan rajoittaa vain ”välttämättömien syiden vuoksi” lailla. Julkisuuden rajoituksen sitominen välttämättömään merkitsee, että rajoitus voi kohdistua vain sekä sisällöllisesti että ajallisesti välttämättömänä pidettävään syyhyn. Edellä jaksossa ” Nykytila ja sen arviointi” on esitetty perusteluita sille, miksi salassapitoajan pidentäminen näiden asiakirjojen osalta on välttämätöntä valtioneuvoston käsityksen mukaan. Tiivistettynä voidaan todeta ensinnäkin, että välttämätön syy salassapitoajan pidentämiselle liittyy ensinnäkin muuttuneeseen turvallisympäristöön, Suomen Nato-jäsenyyteen ja tarpeeseen varmistaa, ettei kansainvälisten järjestöjen ja toisten valtioiden salassa pitämää tietoa julkisteta vastoin niiden tahtoa Suomen kansalliseen käyttöön laadittujen asiakirjojen kautta. Toiseksi on huomioitava, että eräitä 25 vuotta sitten laadittuja raportteja ja TP UTVA-asiakirjoja on edelleen välttämätöntä pitää salassa, koska niiden julkitulo saattaisi paljastaa Suomen haavoittuvuuksia. Kolmas välttämätön syy salassapitoajan pidentämiselle on, että tiettyjen asiakirjojen julkiseksitulo liian varhaisessa vaiheessa voisi haitata Suomen diplomaattien toimintaedellytyksiä vieraissa valtioissa ja sitä kautta heikentää Suomen kansainvälisten suhteiden hoitamista.

Julkisuuslain 24 §:n 1 momentin 1 kohdassa tarkoitettujen asiakirjojen sekä 2 kohdassa tarkoitettujen asiakirjojen, siltä osin kun kyse olisi ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevista asiakirjoista, salassapitoaika olisi jatkossa 25 vuoden sijaan 40 vuotta. Kyseisessä 1 kohdassa tarkoitetut asiakirjat olisivat käytännössä TP UTVA-asiakirjoja, ulkoministeriön tai edustustojen poliittisia tilannearvioita, kuten raportteja, tai neuvotteluja koskevia asiakirjoja. Kyseisessä 2 kohdassa salassapitoajan pidennys rajoittuisi ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjoihin, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön. Nämä asiakirjat koskevat asiasisällöltään pitkälti samankaltaisia asioita kuin 1 kohdassa tarkoitetut asiakirjat eli kyse on perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvista asiakirjoista. Kyseisen 2 kohdan asiakirjat voivat olla esimerkiksi tasavallan presidentin kanslian virkamiesten laatimia asiakirjoja tapaamisista vieraiden valtioiden päämiesten kanssa tai niitä koskevia taustamuistiota. Toisinaan 2 kohdassa tarkoitettu asiakirja voi olla myös ulkoministeriön laatima asiakirja tasavallan presidentille tai asiakirja, joka on laadittu yhteistyössä ulkoministeriön ja tasavallan presidentin kanslian välillä. Näillä ulkoministeriön, tasavallan presidentin ja tasavallan presidentin kanslian asiakirjoilla olisi perusteltua olla sama salassapitoaika.

Salassapitoajan pidennys kohdistuisi siten 1 ja 2 kohdassa säädettyihin asiakirjoihin, jotka koskevat perinteisen ulkopolitiikan keskeiseen toimialueeseen kuuluvia asiakirjoja. Pidentynyt salassapito kohdistuisi siten nimenomaan vain uhkiin ulkoasiainhallinnon, TP UTVA:n sekä tasavallan presidentin ja tasavallan presidentin kanslian ydintoiminnassa ja kansainvälisten suhteiden hoidossa. Ehdotettu 2 kohdan pidennys ei koskisi muita kuin ulkoministeriötä, tasavallan presidenttiä ja tasavallan presidentin kansliaa. Muiden viranomaisten 2 kohdan nojalla salassa pidettävien asiakirjojen salassapitoaika säilyisi edelleen 25 vuodessa. Lisäksi pidennys koskisi

ulkoministeriön, tasavallan presidentin ja tasavallan presidentin kanslian osaltakin vain sellaisia asiakirjoja, jotka ”*koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön”*. Pidennys ei koskisi muita 2 kohdassa mainittuja asiakirjoja (”*asiakirjoja, jotka liittyvät kansainvälisessä lainkäyttö- tai tutkintaelimessä tai muussa kansainvälisessä toimielimessä käsiteltävään asiaan, ja asiakirjat, jotka koskevat Suomen valtion, Suomen kansalaisten, Suomessa oleskelevien henkilöiden tai Suomessa toimivien yhteisöjen suhteita toisen valtion viranomaisiin, henkilöihin tai yhteisöihin”*). Näiden muiden asiakirjojen osalta salassapitoaika olisi 25 vuotta myös ulkoministeriön, tasavallan presidentin ja tasavallan presidentin kanslian osalta. Ehdotus olisi näin ollen rajattu vain välttämättömään. Pidennys ei siten koskisi kaikkia ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjoja. Salassapito ei muuttuisi esimerkiksi ulkoministeriön määrärahojen käyttöä (kuten hankintoja, kehitysyhteistyöhankkeita, edustamista), eikä tavanomaista konsulitoimintaa, vienninedistämistä, henkilöstöhallintoa tai muita ministeriön hallinnollisia asioita koskevien asiakirjojen osalta. Nämä asiakirjat eivät ole lähtökohtaisesti 2 kohdassa tarkoitettuja asiakirjoja, vaan ne voivat olla joko julkisia asiakirjoja tai niiden salassapito voi perustua 24 §:n 1 momentin muihin kohtiin (esimerkiksi 21 kohdan liikesalaisuus), jolloin salassapitoaika olisi edelleen 25 vuotta. Vastaavasti salassapitoajan pidennys ei myöskään koskisi tasavallan presidentin kanslian hallinnollisia asioita koskevia asiakirjoja.

Salassapito pitenisi 1 kohdassa ja 2 kohdassa tarkoitettujen ulkoministeriön, tasavallan presidentin ja tasavallan presidentin kanslian suhteita toiseen valtioon tai kansainväliseen järjestöön säädettyjen asiakirjojen osalta 25 vuodesta 40 vuoteen. Ehdotettua 40 vuotta voidaan ajallisesti pitää perusteltuna, sillä salassapitoajan on yhtäältä oltava riittävän pitkä aika, mutta toisaalta julkisuutta ei saa rajoittaa enempää kuin on välttämätöntä. Valtioneuvosto katsoo, että 40 vuoden salassapitoaika on ajallisesti oikeasuhtainen, koska TP UTVA-asiakirjojen ja ulkoministeriössä ja edustustoissa sekä tasavallan presidentin kansliassa laadittujen asiakirjojen osalta 40 vuotta voidaan pitää riittävän pitkänä aikana, jolla suojataan Suomen kansainvälisiä suhteita. Myös agrementtien osalta diplomaattien urakiertoon ja uran pituuteen nähden 40 vuotta voidaan pitää sopivana, koska tyypillisesti suurlähettilääksi (jolle agrementti tarvitaan) päädytään uran loppuvaiheessa ja tyypillisesti diplomaatin ura pisimmillään kestää noin 40 vuotta.

Lisäksi on huomioitava, että TP UTVA tai ulkoministeriö voisivat edelleen, kuten nykyisinkin, ”päättää toisin” julkisuuslain 24 §:n 1 momentin 1 kohdan nojalla, eli ne voisivat päättää antaa salassa pidettävän asiakirjansa. Näin ollen, vaikka 1 kohdan asiakirjojen kohdalla on kyse ehdottomasta salassapidosta (ei tarvetta vahinkoedellytysarvioinnille), olisi niiden kohdalla myös mahdollista ”päättää toisin” eli tietoja ei salattaisi enempää tai kauempaa kuin olisi välttämätöntä. Julkisuuslain 24 §:n 1 momentin 2 kohdan mukainen salassapito puolestaan perustuisi jatkossakin vahinkoedellytyslausekkeeseen (julkisuusolettama) eikä salassapitoajan muuttamisella ole tarkoitus muuttaa tätä lähtökohtaa. Näin ollen 2 kohdan mukainen salassapito olisi siten mahdollista vain jos tiedon antaminen ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjasta aiheuttaisi vahinkoa tai haittaa Suomen kansainvälisille suhteille tai edellytyksille toimia kansainvälisessä yhteistyössä. Asiakirjoja ei siten salattaisi enempää tai kauempaa kuin olisi välttämätöntä. Huomioon on otettava, että julkisuuslain 17 §:n edellyttää tiedonsaantioikeuksien huomioon ottamista päätöksenteossa ja julkisuusmyönteistä tulkintaa.

Salassapitoajan pidennys kohdistuisi myös julkisuuslain 24 § 1 momentin 9 kohdassa tarkoitettuihin sisäministeriön ja suojelupoliisin asiakirjoihin, jotka koskevat kansallista turvallisuutta (valtioturvallisuutta). Kyseisessä 9 kohdassa tarkoitetut asiakirjat olisivat käytännössä tulosohjaukseen sekä talousarvioon ja sen valmisteluun, siviilitiedustelun ohjaukseen, kuten siviilitiedustelun painopisteiden asettamiseen, liittyvä asiakirjoja ja raportteja, sisäministeriön ja suojelupoliisin laillisuusvalvontakertomuksia tai sisäministeriön suojelupoliisiin kohdistamaan hallinnolliseen valvontaan liittyviä asiakirjoja. Edelleen asiakirjoihin lukeutuvat suojelupoliisin

salaista tiedonhankintaa koskevat lakisääteiset selvitykset sisäministeriölle ja sekä myös esimerkiksi tiedustelutoimintaa koskevat sisäministeriön laatimat asiakirjat TP UTVAan. Vaikka TP UTVA asiakirjojen salassapidosta on säädetty 24 §:n 1 momentin 1 kohdassa, niin esimerkiksi 24 §:n 1 momentin 9 tai 10 kohdassa salassa pidettäväksi säädetyn asiakirjan salassapitoaika määräytyy niitä koskevien lainkohtien perusteella. Salassapitoajan pidennys kohdistuisi myös julkisuuslain 24 § 1 momentin 10 kohdassa tarkoitettuihin sotilastiedustelun asiakirjoihin. Sotilastiedustelusta annetun lain 1 §:n mukaan kyseisessä laissa säädetään puolustusvoimien tiedustelutoiminnan (*sotilastiedustelu*) tarkoituksesta, viranomaisen tehtävistä ja toimivaltuuksista, päätöksenteosta sekä sotilastiedustelun ohjauksesta ja sotilastiedustelun valvonnasta puolustushallinnossa. Laissa säädetään myös tietoliikennetiedustelun teknisestä toteuttamisesta suojelupoliisin puolesta. Sotilastiedustelulain 11 §:n mukaan sotilastiedusteluviranomaisia ovat pääesikunta ja Puolustusvoimien tiedustelulaitos, ja 106 §:n mukaan puolustusministeriö valvoo sotilastiedustelutoimintaa. Kyseisessä 10 kohdassa tarkoitetut asiakirjat olisivat sotilastiedustelun osalta sotilastiedustelun ohjaukseen liittyviä asiakirjoja, raportteja, laillisuusvalvontakertomuksia sekä sotilastiedustelun salaista tiedonhankintaa koskevia lakisääteisiä selvityksiä. Näiden asiakirjojen tiedon salassapitoaika olisi jatkossa 60 vuotta.

Suojelupoliisin kansallista turvallisuutta (valtioturvallisuutta) koskevien asiakirjojen salassapitoaika perustuu nykyisin valtioneuvoston päätökseen suojelupoliisin asiakirjojen salassapitoajan pidentämisestä (SM/2024/77). Päätöksellä valtion turvallisuuden ylläpitämistä koskevien suojelupoliisin asiakirjojen salassapitoaikaa pidennettäisiin 30 vuotta siitä ajankohdasta, mitä säädetään julkisuuslain 31 §:n 2 momentissa salassapitoajan päättymisestä.

8 Lakia alemman asteinen sääntely

---

9 Voimaantulo

Ehdotetaan, että lait tulevat voimaan xx.xx.2026

10 Toimeenpano ja seuranta

11 Suhde muihin esityksiin

Esitys liittyy puolustusministeriössä valmisteltavana olevaan hallituksen esitykseen sotilastiedustelulainsäädännön muuttamisesta. [TÄYDENTYY LAUSUNTOKIERROKSEN JÄLKEEN]

12 Suhde perustuslakiin ja säätämisjärjestys

12.1 Yleistä

Perustuslain 2 §:n mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Julkisen vallan käytön tulee olla palautettavissa eduskunnan säätämässä laissa olevaan toimivaltaperusteeseen (HE 1/1998 vp).

Esitykseen sisältyy sääntelyä, joka on merkityksellistä perustuslaissa säädettyjen perusoikeuksien kannalta; siviilitiedustelutoiminnassa käytettävillä toimivaltuuksilla puututaan yksilön perusoikeuksiin. Perustuslain kannalta merkityksellisimpiä ovat säännösehdotukset, joilla annetaan viranomaisille uusia yksilöön kohdistuvia toimivaltuuksia tai joilla muuten rajoitettaisiin yksilön oikeuksia tai toimintavapautta.

Vaikka tiedustelumenetelmien käytöllä puututtaisiin joihinkin perusoikeuksiin, kuten perustuslain 10 §:n 1 momentissa säädettyyn yksityiselämän suojaan, pyritään s poliisilain ja tietoliikennetiedustelusta siviilitiedustelussa annettujen lakien soveltamisella kuitenkin suojaamaan ja turvaamaan muita perusoikeuksia, kuten perustuslain 7 §:ssä turvattua oikeutta elämään ja henkilökohtaiseen turvallisuuteen sekä perustuslain 1 luvussa säädettyjä 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.

Hyväksyttävänä perusteena pidetään myös kansallista turvallisuutta, jota koskien perustuslakivaliokunta on ottanut kantaa viimeaikaisessa lausuntokäytännössään. Viimeaikaisessa lausuntokäytännössä perustuslakivaliokunta on todennut, että valtion tulee pyrkiä takaamaan kansallinen turvallisuus sekä yleinen järjestys kaikissa olosuhteissa (PeVL 16/2022 vp, kappale 10). Perusoikeuksien välisessä intressipunninnassa on lisäksi otettava huomioon ehdotettujen toimien taustalla olevat intressit etenkin, jos toimet voivat ääritapauksessa palautua jopa henkilökohtaisen turvallisuuden perusoikeuteen (PeVL 37/2022 vp, kappale 8 ja siinä viitatut PeVL 16/2022 vp, kappale 5, ks. myös PeVL 5/1999 vp, s. 2 /II, ks. myös esim. PeVL 36/2020 vp, s. 3, PeVL 15/2018 vp, s. 8).

Siviilitiedustelua koskeva poliisilain 5 a luku ja laki tietoliikennetiedustelusta siviilitiedustelussa tulivat voimaan 1.6.2019. Siviilitiedustelussa voidaan hankkia tietoa ainoastaan laissa tyhjentävästi luetelluista kohteista, jotka on säädetty mahdollisimman yksilöidysti tiedustelutoiminnan erityispiirteet huomioon ottaen. Siviilitiedustelun kohteet ovat usein valtiollisia toimijoita perusoikeudet eivät suojaa (HE 309/1993 vp ja PeVL 4/2018 vp); perusoikeudet suojaavat luonnollisia henkilöitä. Myös tiedustelumenetelmistä on säädetty mahdollisimman tarkkarajaisesti ja täsmällisesti.

Tässä hallituksen esityksessä ehdotetuilla muutoksilla on tarkoitus säätää tarkennuksista, joilla tiedustelutoiminta kohdistuisi teknologian kehittyessä entistä paremmin tarkoitettuun kohteeseen aiempaa tehokkaammin. Lisäksi muutoksilla otettaisiin huomioon turvallisuusympäristössä tapahtuneet muutokset.

Ehdotuksessa poliisilain 5 a luvun ja tietoliikennetiedustelua siviilitiedustelussa koskevan lain muuttamista koskevat säännökset määrittäisivät viranomaisen toimivaltuudet mahdollisimman tarkasti ja siten, että valtuuksien käyttö olisi sallittu vain tehtävien edellyttämässä laajuudessa.

Ehdotetun lain mukaiset valtuudet puuttua kansalaisten perusoikeuksiin kuuluisivat vain virkavastuulla toimiville virkamiehille, jotka olisivat vastuussa myös heitä pyynnöstä avustavien henkilöiden toimista.

Toimivaltuuksia koskevia säännösehdotuksia on tarkasteltava kokonaisuutena voimassa olevan lain kanssa.

Lakiehdotuksia on arvioitava perustuslain 10 §:n lisäksi perustuslain 12:ssä säädetyn sananvapauden ja julkisuuden, perustuslain 15 §:ssä säädetyn omaisuuden suojan, 21 §:ssä säädetyn oikeusturvan sekä vastuuta virkatoimista koskevan 118 §:n ja hallintotehtävän antamista muulle kuin viranomaiselle koskevan 124 §:n kannalta. Perusoikeuksia ei ole asetettu keskinäiseen tärkeysjärjestykseen. Esitykseen liittyvät eri perus- ja ihmisoikeudet, joiden keskinäistä suhdetta ja yhteensovittamista on punnittava. Edelleen ihmis- ja perusoikeuksia on tarkasteltava suhteessa painaviin yhteiskunnallisiin intresseihin kuten kansallinen turvallisuus tai yleinen turvallisuus. Yleisen turvallisuuden intressit voivat ääritapauksessa palautua henkilökohtaisen turvallisuuden perusoikeuteen (ks. PeVL 5/1999 vp, s. 2). Huomioon on otettava myös perusoikeuksien yleiset rajoitusedellytykset (PeVM 25/1994 vp, s. 5), jotka muun ohessa edellyttävät, että rajoitukset ovat tarkkarajaisia ja riittävän täsmällisesti määriteltyjä ja niiden olennainen sisältö ilmenee laista. Rajoitusperusteiden tulee olla hyväksyttäviä ja rajoittamisen tulee olla painavan yhteiskunnallisen tarpeen vaatimaa. Tavallisella lailla ei voi säätää perusoikeuden ytimeen ulottuvaa rajoitusta. Edelleen rajoitusten on oltava suhteellisuusvaatimuksen mukaisia ja välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi. Perusoikeuksia rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä

Lakiehdotuksia tulee lisäksi tarkastella perusoikeuksien yleisten rajoitusedellytysten kannalta (HE 1/1998 vp, PeVM 25/1994 vp).

Poliisilaki (1.lakiehdotus) ja laki tietoliikennetiedustelusta siviilitiedustelussa (2. lakiehdotus)

Yksityiselämän suoja

Yleistä

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta. Sääntelyn lähtökohtana on, että yksilöllä on oikeus elää elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä. Säännös turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Tämä merkitsee esimerkiksi suojaa kirjeiden tai muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan.

Sääntely ei suojaa ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus. Viestin sisällön lisäksi perustuslain säännökset suojaavat myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle.

Perustuslain 10 §:n 4 momentissa säädetään, että lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. Nämä mahdollisuudet rajoittaa luottamuksellisen viestin suojaa on perusoikeusuudistuksen yhteydessä tarkoitettu tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54).

Säännös ei suojaa tavallisen kuuloetäisyydellä käytävän, aistihavainnoin kuultavissa olevan keskustelun sisältöä, mutta perinteisesti luottamukselliseksi tarkoitetun keskustelun

kuunteleminen teknisin apuvälinein merkitsee rajoitusta luottamuksellisen viestin salaisuuden suojaan (HE 309/1993 vp, s. 53, PeVL 11/2005 vp, s. 4, PeVL 36/2002 vp, s. 6, PeVL 2/1996 vp, PeVL 5/1999 vp, s. 4).

Perustuslakivaliokunta on aivan viimeaikaisessa lausuntokäytännössään (PeVL 26/2025 vp. s. 5) korostanut säännöksen soveltamisrajoituksista, että tiedonhankinta kansallista turvallisuutta uhkaavasta toiminnasta voitaisiin 10 §:n 4 momentin perusteella osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten tehtäväksi, joita tällä hetkellä on suojelupoliisi ja Puolustusvoimat.

Toiseksi rajoitusedellytys koskisi vain tiedon hankkimista sellaisesta toiminnasta, joka luonteensa takia voi muodostua vakavaksi uhkaksi kansalliselle turvallisuudelle.

Kolmanneksi lailla tulee säätää tyhjentävästi toimivaltuuksien kohdentumisesta kansallista turvallisuutta vakavasti uhkaavaan toimintaan.

Neljänneksi perustuslain 10 §:n 4 momentin sääntely ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa.

Välttämättömyys-kriteeri puolestaan tarkoittaa valiokunnan mukaan (PeVL 26/2025 vp, kohta 15), että luottamuksellisen viestin salaisuuteen kohdistunut rajoitus on sallittu vain, jos tiedonhankinta ei ole mahdollista vähemmän puuttuvin keinoin, ja että tiedon hankkimisessa puututaan luottamuksellisen viestin salaisuuteen mahdollisimman kohdennetusti ja rajoitetusti. Valtiosääntöoikeudellisen tulkinnan lähtökohtana valiokunta on tähdentänyt myös sitä, että perustuslaista johtuu tarve yhtäältä tulkita kansallisen turvallisuuden käsitettä suppeasti sekä toisaalta asettaa uhan vakavuusaste korkealle (ks. myös PeVM 4/2018 vp, s. 8-9).

Perustuslakivaliokunnan mukaan (PeVL 26/2025 vp, kohta 15) rajoitusperusteeseen vetoavalla on myös velvollisuus esittää riittävät perustelut sille, että jokin toiminta voi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle. Välttämättömyysvaatimuksen täyttymiseksi ei perustuslakivaliokunnan mielestä riitä, että tiedon hankkimisen luottamuksellisista viesteistä voidaan yleisesti katsoa edistävän kansallista turvallisuutta (PeVM 4/2018 vp, s. 8–9).

Perusoikeussäännökset suojaavat luonnollisia henkilöitä ja oikeushenkilöitä välillisesti. Valtio ja muut julkisyhteisöt jäävät perusoikeussuojan ulkopuolelle (HE 309/1993 vp, PeVL 9/2015 vp ja PeVL 4/2018). Vieraan valtion viranomaisorganisaation viestintä ei nauti luottamuksellisen viestin salaisuuden suojaa. Tällaisen viestinnän havaitsemiseksi on kuitenkin välttämätöntä puuttua luottamuksellisen viestinnän suojaan. Viestintä ammattitoiminnassa voi toiminnan luonteen ja viestinnän osapuolten viestien taltiointia koskevan tietoisuuden vuoksi jäädä luottamuksellisen viestin salaisuuden suojan ulkopuolelle, vaikka tällaisessa viestinnässä voitaisiinkin sinänsä välittää myös luottamuksellisia viestejä henkilöiden välillä (liikenteen ohjauksessa syntyvä puhe- ja viestiliikenne; PeVL 62/2010 vp).

Todettakoon vielä, että perustuslakivaliokunta on myös todennut nimenomaisesti, että viestin sisältö ei menetä perustuslain suojaa pelkästään sen perusteella, että esimerkiksi telekuuntelun avulla on saatu tieto siitä (PeVL 99/2022 vp, kappale 12).

Edelleen perustuslakivaliokunta on todennut yleisesti toimivaltuussääntelyn suhteen, että välttämättömyysarvioinnin kannalta toimivaltuutta ei tee välttämättömäksi pelkästään havainto valtuuden tehokkuudesta (PeVL 36/2002 vp s. 6). Valiokunta on mm. esitutkinta- ja pakkokeinolain muuttamisen yhteydessä katsonut, että rajoitusta voidaan pitää siinä mielessä

välttämättömänä, että säännöksessä tarkoitettuja rikoksia ei käytännössä pystytä useinkaan selvittämään tai estämään ilman televalvontaa (PeVL 32/2013 vp s. 4).

Viestin välitystiedot

Viestin sisällön lisäksi perustuslain säännökset suojaavat myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle.

Viestinnän välitystiedot kuuluvat perustuslain 10 §:n 2 momentin luottamuksellisen viestin salaisuuden suojan piiriin (HE 309/1993 vp, s. 53).

Arvioitavan sääntelyn kannalta on merkityksellistä, että perustuslakivaliokunnan aiemmassa vakiintuneessa käytännössä viestin tunnistamistietojen on katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle (ks. esim. PeVL 33/2013 vp, s. 3, PeVL 6/2012 vp, s. 3—4, PeVL 29/2008 vp, s. 2, PeVL 3/2008 vp, s. 2). Tämä on merkinnyt, ettei nykyisin perustuslain 10 §:n 4 momenttiin sisältyvää erityistä lakivarausta ole sellaisenaan sovellettu välitystietojen salaisuuden rajoittamiseen. Välitystietojen salaisuuden suojaan puuttuvan sääntelyn on kuitenkin valiokunnan käytännön mukaan tullut täyttää perusoikeuksien rajoittamisen yleiset edellytykset (PeVL 62/2010 vp, s. 4/II, PeVL 23/2006 vp, s. 2—3). Siten on ollut esimerkiksi mahdollista säätää televalvontatoimivaltuudesta myös tilanteessa, jossa ei välttämättä ole ollut kyse perustuslain 10 §:n 4 momentissa tarkoitetusta yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavista rikoksista (PeVL 33/2013 vp, s. 3). Tunnistamistietojen saamista on pidetty mahdollisena myös joissakin tilanteissa, joissa ei ole ollut kyse perustuslain 10 §:n 4 momentin mukaisista rajoitusperusteista (PeVL 62/2010 vp, s. 4/II).

Sittemmin perustuslakivaliokunta on tarkistanut käytäntöään, koska sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen (PeVL 18/2014 vp, s. 6/II). Valiokunta on viimeaikaisessa käytännössä pitänyt Rajavartiolaitoksen radioteknistä valvontaa koskevaa sääntelyä tuolloin ehdotetussa laajuudessa, ottaen erityisesti huomioon valvonnalle laissa ehdotetut rajoitukset, suhteellisen vähäisenä puuttumisena luottamuksellisen viestin salaisuuden suojaan ja arvioinut sääntelyä perusoikeuksien yleisten rajoitusedellytysten kannalta (PeVL 15/2024 vp, kappaleet 12—13).

Perustuslakivaliokunta on ottanut kantaa (PeVL 18/2014 vp.) tietojen säilyttämisaikoihin tilanteessa, jossa teleyritykset velvoitetaan säilyttämään kaikkiin tilaajiinsa liittyviä tietoja laissa tarkemmin säädetyn ajan. Hallituksen esitys, josta lausunto on annettu, koski niin kutsutun Data Retention -direktiivin kumoamista. Lausunnossaan perustuslakivaliokunta on katsonut, että 12 kuukauden aika siitä päivästä, jona viestintä tapahtui, on oikeasuhtaisuuden kannalta hyväksyttävää ja vastaavan viranomaisten tarpeita (PeVL 3/2008 vp.).

Nyt käsiteltävänä olevassa 2. lakiehdotuksen 10 a §:ssä säilytysaika olisi 18 kuukautta tietoliikenteen teknisten tietojen saamisesta Puolustusvoimien tiedustelulaitokselta. Puolustusvoimien tiedustelulaitoksella tietojen kerääminen kohdistuisi tietoliikenteen teknisiin tietoihin ja kohdistuisi tiettyyn Suomen rajan ylittävään viestiverkon osaan. Tietoliikenteen tekniset tiedot ovat myös välitystietoja, mutta niistä sellaisenaan ei voida tunnistaa välitystietoa käyttävää henkilöä tai muuten puuttua hänen oikeuksiinsa merkittävästi. Henkilön tunnistaminen edellyttää muita luvanvaraisia toimenpiteitä. Tallennuksen piiriin ei suodattuisi viestinnän sisältöä.

Esityksen 2. lakiehdotuksen 10 c §:ssä säilytysaika olisi 12 kuukautta siitä, kun suojelupoliisi saisi tietoliikenteen puolustusvoimien tiedustelulaitokselta. Tietoliikenteen määrä olisi rajoitettu fyysisesti kohdistamalla toimivaltuus tiettyyn Suomen rajan ylittävään viestinverkon osaan ja määrällisesti 5 prosenttiin kohteena olevan Suomen rajan ylittävän viestintäverkon osan teknisestä kapasiteetista. Hakuehtojen määrittäminen tapahtuu vaiheessa, jossa tietoliikenteestä ei voida selvittää viestin semanttista sisältöä. Tietoliikenteen tallennus tapahtuu samassa muodossa, joten tallennetun tietoliikenteen semanttisen sisällön selvittäminen ja se, onko tietoliikenteessä sotilastiedustelun kohteeseen liittyvää tietoa, edellyttää muita luvanvaraisia toimenpiteitä viranomaiselta.

Jotta tietoja voitaisiin käyttää, 2. lakiehdotuksen 10 b §:ssä ja 10 c §:ssä säädettäisiin, tuomioistuimen luvasta.

Teleyritysten velvollisuutta tunnistamistietojen yleisen ja kohdentamattoman säilyttämisen osalta perustuslakivaliokunta on todennut (PeVL 35/2004 vp.), että tunnistamistietojen säilyttämiseen liittyy valiokunnan mielestä aina riskejä yhtä hyvin luottamuksellisen viestinnän suojan kuin henkilötietojen suojan kannalta. Riskit kasvavat, mitä kauemmin tietoja säilytetään. Esimerkiksi kolmen vuoden säilyttämisaikaa on pidetty yleisen henkilötietolainsäädännön kannalta poikkeuksellisen pitkänä (PeVL 35/2004 vp, s. 4 ja PeVL 26/1998 vp, s. 3).

Edellä todetuin perustein ehdotettuja tallennusaikoja voidaan pitää perusteltuina, eivätkä säännösehdotukset ole ristiriidassa perustuslain 10 §:n 2 momentin luottamuksellisen viestin salaisuuden suojan kanssa.

Henkilötietojen suoja

Perustuslain 10 §:n 1 momentin mukaan henkilötietojen suojasta on säädettävä lailla. Perustuslakivaliokunnan käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa lisäksi se, että henkilötietojen suoja osittain sisältyy samassa säännöksessä turvatun yksityiselämän suojan piiriin (esim. PeVL 71/2014 vp, s. 2).

Perustuslakivaliokunta on vakiintuneesti katsonut, että lainsäätäjän on turvattava henkilötietojen suoja tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa (esim. PeVL 18/2012 vp, s. 2 ja PeVL 71/2012, s. 2). Perustuslakivaliokunta on vakiintuneesti katsonut, että erityisesti rekisteröinnin tavoitteista, rekisteröitävien henkilötietojen sisällöstä, henkilötietojen sallituista käyttötarkoituksista, henkilötietojen luovutettavuudesta ja erityisesti teknisellä käyttöyhteydellä luovuttamisesta, henkilötietojen säilytysajoista sekä rekisteröidyn oikeusturvasta tulee säätää lain tasolla kattavasti ja yksityiskohtaisesti (esim. PeVL 12/2002 vp, s. 5, 19/2012 vp, s. 2 ja PeVL 71/2014 vp, s .2).

Henkilötietojen käsittelystä suojelupoliisissa on säädetty henkilötietojen käsittelystä poliisitoimessa annetussa laissa (616/2019). Sen rinnalla sovelletaan tietosuojalainsäädännön yleisenä osana henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018). Näiden lakien muodostaman kokonaisuuden soveltamisalalla ei sovelleta lainkaan EU:n tietosuoja-asetusta eikä yleistä tietosuojalakia.

Suojelupoliisin henkilötietojen käsittelystä koskevassa laissa säädetään kattavasti rekistereistä, niiden käyttötarkoituksesta ja tietosisällöstä, henkilötietojen luovuttamisesta toiselle valtiolle ja kansainväliselle järjestölle, suojelupoliisin oikeudesta saada henkilötietoja siviilitiedustelutehtävien hoitamista varten sekä henkilötietojen poistamisesta rekistereistä.

12.1.1 Luottamuksellisen viestin suoja

Teknisten tietojen käsittely

Tietoliikennetiedustelusta siviilitiedustelusta annetun lain 10 §:n 2 momentin mukaan suojelupoliisi voi antaa Puolustusvoimien tiedustelulaitokselle toimeksiannon sotilastiedustelulain 66 §:ssä tarkoitettuun teknisten tietojen käsittelyyn. Käsiteltävänä olevan hallituksen esityksen 2. lakiehdotuksen 10 a §:n mukaan suojelupoliisi voisi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 66 §:ssä tarkoitettujen teknisten tietojen keräämiseksi. Tietoliikennetiedustelun kohdentamiseksi Puolustusvoimien tiedustelulaitoksella on oikeus tuomioistuimen myöntämän luvan perusteella kerätä ja tallentaa tietoliikenteen teknisiä tietoja eli muun muassa viestien tunnistamistietoja ja käsitellä niitä tilastollista analyysiä varten. Tietoliikenteen käsittely ei kohdistuisi viestin sisältöön vaan viestinnän teknisiin tietoihin, joiden avulla tietoliikennetiedustelua voitaisiin kohdistaan paremmin vain niihin viestintäverkon osiin, joissa liikkuisi tiedustelutehtävän kannalta olennaista viestintää. Vaikka oikeus kohdistuu sinänsä viestinnän tunnistamistietoihin, toimivaltuuden nojalla ei ole mahdollista käsitellä tunnistamistietoja niin, että niistä voitaisiin tunnistaa yksittäisiä henkilöitä tai heidän käyttäytymistään. Tämä ei myöskään ole toimivaltuuden tarkoitus.

Tietoliikenteen teknisissä tiedoissa on kyse lain määritelmän mukaisesti muista kuin viestin sisältöön kuuluvista tietoliikenteen tiedoista. Tietoliikenteen teknisten tietojen käsittelyä koskevassa 2. lakiehdotuksessa tietojen käsittely on sidottu viestintäverkon osan tunnistamiseen ja tietoliikenteen reitittymisen ja muutosten seurantaan. Tietoliikenteen teknisiä tietoja ei käsitellä kohteiden tai henkilöiden tunnistamiseksi, vaan kyse on teknisestä kohdentamisesta toimintaympäristössä ja tietoliikennetiedustelujärjestelmän teknisestä kehittämisestä tietoja analysoimalla.

Eduskunnassa samanaikaisesti käsiteltävänä olevan, ehdotetun sotilastiedustelulain 66 §:ssä esitetään, että toimivaltuuden osalta poistettaisiin vaatimus lyhytaikaisuudesta, kun puolustusvoimien tiedustelulaitos voimassa olevan lain mukaan voi viestintäverkon tietoliikenteestä hetkellisesti kerätä ja tallentaa tietoliikenteen teknisiä tietoja. Lyhytaikaisuus ei ole käytännössä osoittautunut toimivaksi rajoitteeksi. Teknisten tietojen käsittely kohdistuu ainoastaan tietoliikenteen teknisiin tietoihin, joita ei voida yhdistellä tai tarkemmin analysoida esimerkiksi yksittäisen henkilön tunnistamiseksi tai muuksi varsinaisen tiedustelutiedon tuottamiseksi. Näin ollen lyhytaikaisuusvaatimuksen poistamisen ei voida katsoa laajentavan puuttumista perustuslain 10 §:n suojaamaan yksityiselämän suojaan.

Siviiliedustelulainsäädäntöä koskevassa perustuslakivaliokunnan lausunnossa (PeVL 35/2018 vp. s. 20) todettiin, että ”perustuslain 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa (PeVM 4/2018 vp, s. 8). Tällainen kielto johtuu myös perusoikeuksien yleisistä rajoitusedellytyksistä. Säädösperustainen kielto on omiaan selventämään nyt vain hallituksen esityksen perusteluissa mainittuja tietoliikennetiedustelun rajoja. Lisäksi se konkretisoi tuomioistuimen päätösvallan käytön ja tiedustelutoiminnan käytäntöjen kannalta merkityksellisellä tavalla erityisesti EU:n perusoikeuskirjaan perustuvia luottamuksellisen viestin suojan perusvaatimuksia. Asian merkityksen vuoksi nyt käsillä olevassa sääntely-yhteydessä lakiin tulee lisätä nimenomainen säännös yleiseen ja kohdentamattomaan tietoliikenteen seurantaan kohdistuvasta kiellosta. Tällaisen yleissäännöksen lisääminen tietoliikennetiedustelulakiehdotukseen on edellytyksenä lain käsittelemiselle tavallisen lain säätämisjärjestyksessä”. Eduskuntakäsittelyssä päädyttiin perustuslakivaliokunnan lausunnon johdosta lisäämään tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin uusi lainkohta, 1 §:n 4 momentti, jonka mukaan tietoliikennetiedustelu ei saa olla yleistä ja kohdentamatonta tietoliikenteen seurantaa.

Perustuslakivaliokunta on sotilastiedustelusta annettua lakia koskevassa lausunnossaan (PeVL 36/2018 vp.) todennut, että sotilastiedustelulakiehdotuksen 63 §:n (nykyinen 66 §) sanamuoto vaikutti perustuslakivaliokunnan käsityksen mukaan mahdollistavan hyvin laajan viestintäverkon alueen kattavan tietojen keräämisen ja tallentamisen eikä ehdotetun lain 63 § (66 §) sisällä ollut "hetkellisyyttä" koskevaa mainintaa lukuun ottamatta nimenomaisia rajoittavia kriteereitä tietojen keräämiselle ja tallentamiselle. Ehdotetussa sääntelyssä voitiin tältä osin nähdä ns. massavalvonnan piirteitä, kun esityksen perustelujenkin mukaan (HE 203/2017 vp. s. 280) teknisten tietojen käsittely tietoliikenteestä voisi tapahtua hetkellisesti kaikkeen viestintäverkon osassa liikkuvaan tietoliikenteeseen kohdistuen. Ottaen huomioon, että perustuslakivaliokunnan lausunto (PeVL 36/2018 vp) 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa (PeVM 4/2018 vp, s. 8), ehdotettua 63 §:ää (66 §) oli tältä osin täsmennettävä nimenomaisella säännöksellä yleiseen ja kohdentamattomaan tietoliikenteen seurantaan kohdistuvasta kiellosta. Vaihtoehtoisesti tämä kielto voidaan ottaa lain yleissäännöksiin. Eduskuntakäsittelyssä päädyttiin perustuslakivaliokunnan ehdottaman mukaisesti lisäämään lakiin uusi 65 §, jossa säädetään yleisen ja kohdentamattoman tietoliikenteen seurannan kiellosta.

Käsiteltävänä olevan 2. lakiehdotuksen 10 § ja 10 a § sisältävät jo voimassa olevan rajoitteen, eli säännöksen nojalla voidaan kerätä ja käsitellä ainoastaan tietoliikenteen teknisiä tietoja. Muilta osin, kuten viestin sisältötiedon osalta, tiedot on poistettava. Eduskunnassa samanaikaisesti käsiteltävänä olevan sotilastiedustelulakia koskevan hallituksen esityksen 1. lakiehdotuksen 66 §:ssä ehdotetaan rajoitetta, eli tietoliikenteen teknisten tietojen käsittely voi kohdistua vain tiettyyn Suomen rajan ylittävän viestintäverkon osaan. Ehdotuksen mukaan kerättävien teknisten tietojen määrä ei voisi ylittää 5 prosenttia kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista.

Käsiteltävänä olevan 2. lakiehdotuksen 10 a §:n 2 momentin 2 kohdan mukaan suojelupoliisilla olisi oikeus käsitellä teknisiä tietoja tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Vastaavan kaltaisesti sotilastiedustelulakia koskevassa lakiesityksessä ehdotetun 66 §:n 1 momentin 2 kohdan mukaan teknisten tietojen käsittelyllä voitaisiin myös käsitellä tietoliikennettä sen reitittymisen ja muutosten seuraamiseksi. Vastaavasti kuin viestintäverkon osan kohdentamisessa, kyseessä ei ole yksittäisten viestien tai niiden sisällön analysoinnista. Lisäksi toiminnassa on käytettävä rajauksia ja teknisiä hakuehtoja, jotta tietoliikenteen reitittymistä ja muutosta voidaan seurata. Näin ollen ei voida katsoa, että kyse olisi yleisestä ja kohdentamattomasta tietoliikenteen seurannasta.

2. lakiehdotuksen 10 a §:n mukaan suojelupoliisi voisi tallentaa teknisiä tietoja enintään 18 kuukauden ajaksi. Näitä tietoja voitaisiin käyttää lain 10 a §:ssä tarkoitettuun teknisten tietojen käsittelyyn, mutta myös 2. lakiehdotuksen 10 c §:n tarkoituksessa hakuehtojen määrittämisessä. Säilytettävät tiedot ovat tietoliikenteen teknisiä tietoja eikä niistä voitaisi teknisten tietojen käsittely -toimivaltuudella hankkia tarkempia tietoja yksittäisesti henkilöstä tai organisaatiosta taikka niiden toiminnasta. Toimivaltuuden käyttö kohdistuisi tiettyihin viestintäverkon osiin, mikä teknisesti estää kaiken mahdollisen tietoliikenteen tallentamisen. Lisäksi globaalin viestintäverkon toiminnan luonteen takia analyysin ja tallennuksen kohteeksi joutuvat tietoliikenteen tekniset tiedot valikoituvat käytännössä sattumanvaraisesti. Jotta näitä tallennettuja tietoja voitaisiin käyttää 2. lakiehdotuksen 10 a §:n taikka 10 c §:n tarkoituksessa, edellytyksenä on tuomioistuimen lupa.

Asiaa voidaan arvioida ylimääräisen tiedon käytön näkökulmasta. Toimivaltuutta käytettäessä järjestelmään tulee väistämättä ylimääräistä tietoa, jota ei nykytilassa ole voitu käyttää esimerkiksi historiatiedon näkökulmasta teknisten tietojen käsittelyn tarkentamiseksi tai varsinaisessa tietoliikennetiedustelussa. Lakiehdotuksen mukaisesti tallennettujen tietojen käyttö edellyttää

uuden luvan hakemista tuomioistuimelta, jolloin täyttyisi myös edellytys vastaavan tasoisesta päätöksenteosta, mitä on alun perin edellytetty tiedonhankinnalle ja sen tallentamiselle.

Merkittävänä erona ylimääräisen tiedon käsittelyyn nähden on se, että viranomaisella ei ole tietoa siitä, mitä tietoja tallennetut tiedot sisältävät eikä viranomaisella ole myöskään pääsyä näihin tietoihin ilman tuomioistuimen lupaa.

Yksityiselämän suojan voidaan katsoa toteutuvan myös sitä kautta, että pelkkien tietoliikenteen teknisten tietojen perusteella lähettäjän ja vastaanottajan henkilöllisyyden selvittäminen on käytännössä mahdotonta.

Määrällisesti tallennettavan tiedon määrä olisi rajoitettu viiteen prosenttiin kohteena olevan Suomen rajan ylittävän viestintäverkon osan kapasiteetista, eli siitä, mitä viestintäverkon osa voi enimmillään kuljettaa tietoliikennettä.

Säännösehdotus puuttuu perustuslain 10 §:n suojaamaan yksityisyyden suojaan, mutta säännöksen nojalla tietoliikenteen teknisiä tietoja käsitellään ainoastaan teknisestä näkökulmasta. Tietoja ei voida analysoida tai yhdistellä niin, että niistä voitaisiin selvittää yksittäiseen henkilöön liittyviä tietoja henkilön perustuslain 10 §:n suojaamiin perusoikeuksiin puuttuvalla tavalla. Ehdotettujen muutosten perusteella tallennettujen tietojen käyttö edellyttäisi 2 lakiehdotuksen 10 a ja 10 c §:ssä tarkoitetussa toiminnassa tuomioistuimen lupaa ja muidenkin toimivaltuuden käytön edellytysten täyttymistä.

Edellä todetun perusteella säännösehdotus voidaan käsitellä perustuslain 10 §:n 4 momentin nojalla tavallisen lain säätämisjärjestyksessä.

Viestin sisältö

Esityksen 2. lakiehdotuksen 10 c § puuttuu viestin sisältöön. Suojelupoliisi voisi antaa toimeksiannon puolustusvoimien sotilastiedustelulaitokselle eduskunnassa käsiteltävänä olevan, ehdotetun sotilastiedustelulain 67 a §:n 1 momentissa tarkoitetun tietoliikenteen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaisi tuomioistuimen luvan mukaisen tietoliikenteen keräämisen ja luovuttaisi sen suojelupoliisille. Puuttumiseen syvyys rajoittuisi kuitenkin uusien hakuehtojen määrittämiseen. Hakuehdot on määritelty tietoliikennetiedustelusta siviilitiedustelussa annetun lain 2 §:n 4 kohdan mukaan tiedoksi, jonka perusteella tietoliikennetiedustelulla viestintäverkon osasta mahdollisimman rajatusti ja täsmällisesti valitaan tietoliikennetiedustelun kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu tiedustelun tarkoituksen kannalta välttämättömään. Määritelmä on tehty eduskunnan myötävaikutuksella (HaVM 36/2018 vp. sekä PeVL 35/2018 vp s.19-20 ja PeVL 75/2018 vp. s. 3).

Jotta tietoliikennetiedustelu olisi mahdollisimman kohdennettua ja sillä saataisiin odotettua tietoa tehokkaasti, tiedusteluviranomaisella on oltava ennakkotieto hakuehdon kohdistumisesta niin, että se puuttuu viestinnän suojaan mahdollisimman rajoitetuissa tilanteissa. Nyt käsiteltävänä olevassa säännösehdotuksessa satunnaista tietoliikennettä voitaisiin tutkia uusien hakuehtojen määrittämiseksi.

Ehdotetun sotilastiedustelulain 67 a §:n 1 momentin mukaan toimivaltuus voisi kohdistua satunnaiseen tietoliikenteeseen. Satunnaisuus kuvaisi tietoliikenteen liikkumista Suomen rajan ylittävän viestintäverkon osassa tiettynä ajanhetkenä. Satunnaisuus tarkoittaisi myös sitä, että tietoliikenteen reitittyminen huomioon ottaen kohteeksi joutuvaa tietoliikennettä ei analysoida

tietyn kohteen viestinnän selvittämiseksi vaan satunnaisessa tietoliikenteessä liikkuvissa tietoliikennepaketeissa olevien hakuehtojen tunnistamiseksi.

Hakuehtojen määrittämisessä ei saisi yhdistellä tietoja tavalla, josta voitaisiin tunnistaa yksittäinen henkilö. Yksittäisen henkilön tunnistaminen tai tietojen saaminen tämän henkilökohtaisesta elämästä ei ole myöskään ehdotetun toimivaltuuden tarkoitus, vaan tarkoituksena on määrittää hakuehtoja, jotta varsinainen tietoliikennetiedustelu kohdentuisi välttämättömään.

Toimivaltuuden käyttö olisi sidottu välttämättömyyteen. Tässä tapauksessa välttämättömyys tarkoittaisi sitä, että uusia hakuehtojen ei käytännössä pystyttäisi määrittämään toisella tavalla tai määrittäminen vaatisi kohtuuttomasti resursseja. Välttämättömyys edellyttää myös sitä, että kohteesta, jonka tietoliikenteestä on aiemmin saatu tietoa käytössä olevilla hakuehdoilla, ei enää saada vastaavalla tavalla tietoa.

Perustuslakivaliokunta on todennut sotilastiedustelulaista (HE 203/2017 vp) antamassaan lausunnossa (PeVL 36/2018 vp.), että ehdotetussa 63 §:ssä (nykyinen 66 §) tarkoitettu hetkellisyys ei ollut riittävän rajaava. Perustuslakivaliokunta totesi, että perustuslain 10 §:n 4 momentti ei mahdollista yleistä, kohdentamatonta ja kaikenkattavaa tietoliikenteen seurantaa tiedustelutoiminnassa (PeVM 4/2018 vp, s. 8), ehdotettua 63 §:ää on tältä osin täsmennettävä nimenomaisella säännöksellä yleiseen ja kohdentamattomaan tietoliikenteen seurantaan kohdistuvasta kiellosta. Vaihtoehtoisesti tämä kielto voidaan ottaa lain yleissäännöksiin. Esityksen jatkokäsittelyssä sotilastiedustelulakiin lisättiin nimenomainen säännös yleisen ja kohdentamattoman tietoliikennetiedustelun kiellosta (lain 65 §) ja vastaavasti tietoliikennetiedustelusta siviilitiedustelussa annettuun lakiin (1 § 4 mom.) ja koska suojelupoliisille tietoliikennetiedustelun teknisenä toteuttaja toimii puolustusvoimien tiedustelulaitos. (lain 10 § ja 2. lakiesityksen 10 c §)

Nyt käsiteltävänä olevaa toimivaltuutta olisi rajattu fyysisesti tiettyyn Suomen rajan ylittävään viestintäverkon osaan, minkä lisäksi tietojen määrää olisi rajoitettu 5 prosenttiin kyseisen viestintäverkon osan kapasiteetista. Toimivaltuuden käyttöä kohdennettaisiin edelleen tuomioistuimen luvassa, jossa olisi mainittava myös tiedustelutehtävä ja kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre.

Edellä kuvatusti ehdotetulla toimivaltuudella hankittavat tiedot eivät itsessään puutu syvällisesti yksityisen viestin suojaan. Syvällinen puuttuminen edellyttäisi tietojen yhdistelemistä ja muiden tiedustelumenetelmien käyttöä.

Esityksen 2. lakiehdotuksen 10 d §:ssä säädettäisiin 10 c §:n toimivaltuutta koskevasta päätöksenteosta. Vaatimuksessa ja päätöksessä olisi tuotava ilmi siviilitiedustelun kohde, jota varten hakuehtoja määritetään ja sitä koskevat tosiseikat. Lisäksi vaatimuksessa olisi perusteltava välttämättömyys.

Keskeisenä seikkana vaatimuksessa olisi tuotava ilmi kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään ja perustelut sille. Kohdan mukaisesti tiedusteluviranomaisella olisi oltava suuntaa antava käsitys kohteena olevan toimijan tietoliikenteestä, jotta hakuehtojen määrittämisessä ei jouduta käymään kaikkea mahdollista tietoliikennettä läpi. Vaatimuksessa olisi myös perusteltava, miksi tämän ennakkotiedon perusteella uusia hakuehtoja pystyttäisiin määrittelemään.

Lukuun ottamatta esityksen 2. lakiehdotuksen 10 c §:ssä erikseen säädettyä oikeutta tallentaa tietoja 12 kuukauden ajaksi, hankittuja tietoja koskisi laissa säädetty yleinen tietojen hävittämisvelvollisuus

Tietojen tallentaminen ja käyttäminen

Esityksen 2. lakiehdotuksen 10 a §:n 3 momentissa ja 10 c §:n 4 momentissa säädettäisiin erityisistä tallentamisajoista. Teknisten tietojen osalta tallentamisaika olisi 18 kuukautta ja hakuehtojen määrittämisessä käytettävien tietojen osalta tallennusaika olisi 12 kuukautta.

Puolustusvoimien tiedustelulaitos luovuttaa tiedot suojelupoliisille. Tietojen määrää rajautuu ensin fyysisesti tiettyyn viestintäverkon osaan ja määrällisesti enimmillään 5 prosenttiin viestintäverkon osan kokonaiskapasiteetista. Tiedot poistuisivat järjestelmästä todetun määräajan jälkeen.

Perustuslakivaliokunta on lausuntokäytännössään pitänyt ongelmattomana henkilötietojen säilyttämistä yhden vuoden ajan (PeVL 21/2013 vp. ja PeVL 13/2017) vaikka henkilön ei epäillä liittyvän esimerkiksi kansallista turvallisuutta vakavasti uhkaavaan toimintaan. Joka tapauksessa valiokunta on kiinnittänyt huomiota siihen, että mitä pidemmäksi tietojen säilytysaika muodostuu, sitä olennaisempaa on huolehtia tietoturvasta, tietojen käytön valvonnasta ja rekisteröidyn oikeusturvasta (mm. PeVL 28/2016 vp. s. 7).

Nyt käsiteltävänä olevien ehdotusten kannalta merkittävää on se, mitä tietoja tallennettaisiin, kuinka kattavaa tietojen tallentaminen on ja kuinka pitkä tallennusaika on.

Teknisten tietojen osalta kyse on tietoliikenteen teknisten tietojen käsittelystä. Tekniset tietojen käsittelyssä tietoliikenteen teknisiä tietoja käsitellään tietyn viestintäverkon osan tunnistamiseksi sekä tietoliikenteen reitittymisen ja muutosten seuraamiseksi. Kyse on teknisestä analyysistä eikä tietoihin sisälly viestin sisältöä. Käsiteltävät tiedot rinnastuvat IP-osoitteeseen, josta ei sellaisenaan EUT:n ratkaisukäytännön mukaan ei voi vetää syvällisiä johtopäätöksiä yksityiselämästä.

Tietojen tallentaminen on välttämätöntä esitetyn 2. lakiesityksen 10 c §:n hakuehtojen määrittämisen sekä varsinaisen tietoliikennetiedustelun kannalta, jotta tietoliikennetiedustelu kohdistuisi ainoastaan välttämättömään osaan tietoliikennettä. Tietoliikenteen teknisten tietojen historiatietoon vertaamisella on merkittävä osa määritettäessä uusia hakuehtoja ja hankittaessa tietoa tiedustelun kohteesta. Teknisten tietojen historiatiedon avulla varsinaisessa tietoliikennetiedustelussa pystyttäisiin todentamaan esimerkiksi se, onko kohde viestinyt jo aiemmin Suomen rajan ylittävän viestintäverkon osan kautta. Tieto voi olla välttämätöntä esimerkiksi kahden viestivän tahon pidempikestoisen kanssakäymisen varmistamiseksi (viestin sisällöllä ei ole merkitystä) tai mahdollisimman tarkkojen hakuehtojen määrittämisen varmistamiseksi.

Käsiteltävänä olevan säännöksen mukaisessa toiminnassa ei ole tarkoitus saada tietoa tiedustelun kohteista, vaan kyse on tietoliikenteen teknisesti seurannasta. Näin ollen 18 kuukauden säilytysaikaa ei voida pitää ongelmallisena perustuslain kannalta.

2. lakiehdotuksen 10 c §:n (tietoliikennetiedustelu hakuehtojen määrittämiseksi) mukaan suojelupoliisi voi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle ehdotetun sotilastiedustelulain 67 a §:ssä tarkoitetun tietoliikenteen keräämiseksi. Viimeksi mainitun säännösehdotuksen mukaan hakuehtojen määrittäminen kohdistuu Suomen rajan ylittävän viestinverkon osassa liikkuvaan satunnaiseen tietoliikenteeseen. Teknisen rajoitteen lisäksi säännöksessä olisi myös määrällinen rajoite, 5 prosenttia kyseisen viestintäverkon osan kokonaiskapasiteetista. Tietoliikennettä voitaisiin tallentaa 12 kuukauden ajaksi.

Kuten aiemmin on todettu, perustuslakivaliokunta on katsonut 12 kuukauden tietojen säilyttämisen ajan ongelmattomaksi henkilötietojen osalta, vaikka se kohdistuisi erittelemättä tiettyyn

ihmisryhmään (Suomen rajan ylittävät henkilöt). Nyt käsiteltävänä olevassa tilanteessa tallennettavat tiedot ovat järjestelmässä tavuina eli niistä ei suoraan pystytä lukemaan esimerkiksi viestin sisältöä. Toimivaltuuden nojalla ei voida myöskään hankkia tietoa esimerkiksi kohteena olevan henkilön toiminnasta.

Tietoliikenne sisältää henkilötietoja ja viestin sisältöä, vaikka niitä ei käsiteltäisi tai ne eivät selviäisi toimivaltuutta käytettäessä. Jotta näitä tietoja voitaisiin käsitellä ja selvittää, olisi käytettävä varsinaista tietoliikennetiedustelua.

EIT on ratkaisukäytännössään hyväksynyt myös massamaiset tiedonhankinta keinot eräin edellytyksin. EUT on taasen ratkaisukäytännössään todennut, että yleinen ja erittelemätön tietojen tallentaminen viranomaistarpeisiin on kielletty. Nyt käsiteltävänä olevassa tilanteessa kyseessä ei voida katsoa olevan tietojen yleinen ja erittelemätön tallentaminen, sillä toimivaltuudella tallennettavat tiedot on tallennettu tietystä Suomen rajan ylittävästä viestintäverkon osasta. EUT:n käytännöstä poiketen kyse on lisäksi viranomaisen itsensä suorittama toimenpide, ei yksityiselle toimijalle lailla asetetusta velvollisuudesta.

Jotta edellä tarkoitettujen ehdotusten mukaisista tallennetuista tiedoista voitaisiin tehdä yksittäisen henkilön toiminnasta johtopäätöksiä, edellyttäisi tämä aina tuomioistuimen varsinaista tietoliikennetiedustelua koskevaa lupaa ja luvassa todettujen hakuehtojen käyttöä.

Joka tapauksessa perustuslakivaliokunnan käytännön mukaisesti (mm. PeVL 28/2016 vp.) ehdotettujen säännösten mukaisesta toiminnassa huolehdittaisiin tietoturvasta, tietojen käytön valvonnasta ja rekisteröidyn oikeusturvasta. Valvonnasta huolehtivat sisäisen valvonnan lisäksi keskeisesti tiedusteluvalvontavaltuutettu ja tietosuojavaltuutettu sekä oikeusturvasta tuomioistuimen ennakkokontrollin lisäksi tiedusteluvalvontavaltuutettu ja tietosuojavaltuutettu.

Tallennetun tiedon käytön voidaan katsoa olevan lähellä ylimääräisen tiedon käyttöä. Ylimääräisellä tiedolla tarkoitetaan perinteisesti rikostorjunnassa telekuuntelulla, televalvonnalla, tukiasematietojen hankkimisella ja teknisellä tarkkailulla saatua tietoa, joka ei liity tiettyyn rikokseen tai vaaran torjumiseen taikka joka koskee muuta rikosta kuin sitä, jonka estämistä tai paljastamista varten lupa tai päätös on annettu.

Ylimääräisen tiedon käyttöä koskeva sääntely poliisilaissa on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 67/2010 vp, s. 4—5, PeVL 33/2013 vp, s. 5—7). Valiokunta on tarkastellut sääntelyä perustuslain 10 §:ssä turvatun luottamuksellisen viestin salaisuuden kannalta. Valiokunnan mukaan on selvää, että kaikki sinänsä laillisella salaisella pakkokeinolla saatu ylimääräinen tieto ei voi olla rajoituksetta käytettävissä minkä tahansa rikoksen selvittämiseen. Luottamuksellisen viestin salaisuutta turvaavan säännöksen ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Viestin sisältö ei menetä perustuslain suojaa pelkästään sen perusteella, että esimerkiksi telekuuntelun avulla on saatu tieto siitä. Perustuslain 10 §:n sääntely rajoittaa viestin sisällön käyttöä tämän jälkeenkin. Tämä on olennaista myös sen vuoksi, että salaisen pakkokeinon kohteeksi voi joutua kuuntelun varsinaisen kohteen lisäksi myös ulkopuolinen henkilö. Lisäksi on valiokunnan mukaan huomattava, että ylimääräisen tiedon käytön salliminen muiden vakavuusasteeltaan vähäisempien rikosten kuin kunkin telepakkokeinon perusterikosten selvittämiseen merkitsee eräänlaista välillistä telepakkokeinon käytön rajoittamisen väljennystä (PeVL 33/2013 vp, s. 6/II). (PeVL 99/2022 vp., PeVL 26/2025 vp s. 3).

Perustuslakivaliokunnan mukaan estettä ei ole ollut sille, että ylimääräisen tiedon käyttöä koskevan säännöksen piiriin otetaan joitakin sellaisiakin yksittäisiä rikoksia, joiden enimmäisrangaistus on kaksi vuotta vankeutta mutta jotka kuitenkin vakavuusasteeltaan rinnastuvat muihin

ylimääräisen tiedon käyttämisen edellytyksenä oleviin rikoksiin ja jotka täyttävät perustuslain 10 §:ssä luottamuksellisen viestin salaisuuden rajoittamiselle asetetut vaatimukset (PeVL 33/2013 vp, s. 7/I).

2. lakiehdotuksessa on ehdotettu oikeus suojelupoliisille tallentaa tietoliikenteen puolustusvoimien tiedustelulaitoksen suojelupoliisille luovuttamia tietoja. Ehdotetun sotilastiedustelulakiesityksen 1. lakiehdotuksen 66 §:ssä, 67 a §:ssä, 68 §:ssä ja 70 §:ssä on ehdotettu oikeus sotilastiedusteluviranomaiselle tallentaa tietoliikenteen teknisiä tietoja ja satunnaista tietoliikennettä voidaan pitää peruslähtökohdiltaan vastaavana tilanteena kuin rikostorjunnan ylimääräisen tiedon käyttöä. Ehdotetuilla muutoksilla tiedusteluviranomainen voi tallentaa tietoa, joka ei liity tilanteessa käsillä olevaan tuomioistuimen lupaan. Tallennettujen tietojen käyttö samassa tarkoituksessa tai eri tarkoituksessa edellyttää kuitenkin tuomioistuimen lupaa.

Luvan perusteena on aina kansallista turvallisuutta vakavasti uhkaava toiminta. Poliisilain 5 a luvun 3 §:ssä ja tietoliikennetiedustelusta siviilitiedustelussa annetun lain 3 §:ssä säädetään siviilitiedustelun kohteista. Sotilastiedustelusta annetun lain 4 §:ssä on tyhjentävästi lueteltu toiminta, jonka perusteella tiedustelumenetelmiä voidaan käyttää. Tästä johtuen voidaan katsoa, että luvan perusteena olevassa toiminnassa ei ole kyse lievemmästä ja vakavammasta toiminnasta, johon voitaisiin kohdistaa eri tiedustelumenetelmiä, vaan kaikki säännöksissä mainittu toiminta on yhtä vakavaa suojattavien oikeushyvien näkökulmasta.

Tallennettujen tietojen käyttö edellyttää tuomioistuimen lupaa, jossa muilta kuin teknisten tietojen käsittelyn osalta on mainittava siviilitiedustelun kohde. Lisäksi on mainittava kohdentamisessa olennaiset seikat, kuten tietoliikenteen säännönmukaisuus hakuehtojen määrittämisessä tai hakuehdot varsinaisessa tietoliikennetiedustelussa.

Edellä tarkoitettujen säännösten perusteella tallennettuja tietoja ei voida käyttää muiden tiedustelumenetelmien käytön yhteydessä.

Esityksessä ehdotetut tallennusajat olisivat rajattuja. Tietoihin, joita voidaan tallentaa, kohdistuu myös fyysisiä ja teknisiä rajauksia.

12.1.2 Omaisuuden suoja

Esityksen 1. lakiehdotuksen 16 §:n 3 momentilla on merkitystä perustuslain 15 §:n kannalta. Perustuslain 15 §:n 1 momentin mukaan jokaisen omaisuus on turvattu.

Perustuslakivaliokunta ei ole ottanut kantaa täysin vastaavaan tilanteeseen, mistä nyt käsiteltävänä olevassa säännösehdotuksessa olisi kyse. Perustuslakivaliokunta on vakiintuneessa lausuntokäytännössään todennut, että esimerkiksi Puolustusvoimien oikeudelle käyttää tilapäisesti kiinteistöjä on katsottu olevan perustuslain 15 §:ssä turvatun omaisuuden suojan kannalta sotilaalliseen maanpuolustukseen liittyvä painava yhteiskunnallinen tarve. Sotilaallisen harjoitustoiminnan ja puolustusvalmiuden kohottamisen tarpeet ovat perusoikeusjärjestelmän kannalta hyväksyttäviä perusteita rajoittaa omaisuuden suojaa. Kiinteistön tilapäisen käytön edellytetään olevan välttämätöntä säännöksessä mainittujen toimintojen kannalta (esimerkiksi PeVL 51/2006 vp. s. 5).

Nyt käsiteltävänä olevan säännösehdotuksen mukaan suojelupoliisilla on oikeus menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja tiedonsiirtämiseksi tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmää, jos se on välttämätöntä tiedustelumenetelmän

käyttämiseksi. Suojelupoliisi ei saa aiheuttaa vähäistä suurempaa haittaa tai vahinkoa käytettävälle laitteelle tai tietojärjestelmälle. Säännöksen mukaisesti tässä tarkoituksessa käytettävä ulkopuoliselle tai tämän laitteistolle tai tietojärjestelmälle ei saa aiheutua vahinkoa. Käyttö olisi myös rajattava ajallisesti välttämättömään, eikä yksittäistä laitteistoa tai tietojärjestelmää lähtökohtaisesti voitaisi käyttää kuin välttämättömän ajan esimerkiksi yksittäisen käskyn saattamiseksi tiedonhankinnan kohteeseen. Vastaavasti tietoja kotiutettaessa olisi arvioitava tiedon kotiuttamista useiden eri laitteistojen ja tietojärjestelmien kautta.

Selvää on se, että suojelupoliisi ei voisi hankkia tietoa välittäjänä olevan laitteen tai tietojärjestelmän sisältämistä tai sen kautta kulkevista muista tiedoista.

Säännösehdotus on välttämätön, jotta suojelupoliisin kohteena olevasta toiminnasta saataisiin tietoa. Kaikissa tilanteissa suojelupoliisilla ei ole mahdollisuutta päästä vaivihkaisesti suorittamaan säännösehdotuksessa tarkoitettuja toimenpiteitä. Toimenpiteen suorittamisen edellytyksenä olisi välttämättömyys, eli toimenpidettä ei käytännössä muilla keinoin voitaisi suorittaa.

Puuttuminen perusoikeuksiin voidaan arvioida vähäiseksi.

Esityksen 1. lakiehdotuksen 28 a §:ssä esitettävä aineen, omaisuuden tai esineen tilapäinen haltuunotto koskisi tilanteita, joissa lain esitetyssä 27 a §:n näytteenoton tai säädetyn 28 §:n jäljentämisen toimivaltuuden käyttö sitä välttämättä edellyttää, suojelupoliisilla on oikeus ottaa aine, omaisuus tai esine tilapäisestit haltuun. Aine, omaisuus tai esine on palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua. Ehdotettu 28 a § vastaisi toimintana sitä, mitä pakkokeinolain 7 luvun 8 §:n 1 momentissa säädetään, mutta keskeisenä erona on se, että toimivaltuutta ei ole tarkoitettu käytettäväksi pidempikestoisessa haltuunotossa. Lisäksi tiedustelutoiminnan luonne huomioon ottaen, aine, esine tai omaisuus olisi pyrittävä palauttamaan haltuunottohetken sijaintiin mahdollisimman muuttumattomana, jotta tiedustelutoiminta ei paljastuisi.

Säännösehdotus koskisi perustuslain 15 §:n 1 momenttia, joka suojaa omistajalle kuuluvaa oikeutta hallita, käyttää ja hyödyntää omaisuuttaan, kuten tavaroitaan ja asiakirjojaan, haluamallaan tavalla sekä valtaa määrätä niistä.

Esityksen 1. lakiehdotuksen 28 a §:n nojalla tehtävä haltuunotto tarkoittaisi esineen, aineen tai omaisuuden omistajan käyttöoikeuden ja määräämisvallan tilapäistä rajoitusta. Ehdotettua 28 a §:n sääntelyä voitaisiin kuitenkin pitää perusoikeusjärjestelmän kokonaisuuden kannalta hyväksyttävänä ja painavan yhteiskunnallisen tarpeen vaatimana, sillä toimivaltuutta käyttämällä suojelupoliisi voisi varmistaa laissa säädettyjen tehtäviensä asianmukaisen hoitamisen, esimerkiksi tarkastamalla kohteena olevan toimijan tiloissa olevan aineen koostumuksen.

Toimenpiteen kohteena olisi aine, esine tai omaisuus, joka on tai jota voidaan käyttää yhdessä tai erikseen ihmisten vahingoittamiseen taikka aineen, esineen tai omaisuuden hallussapito on jo muualla lainsäädännössä lähtökohtaisesti kielletty. Tallaisia lakeja voisivat olla esimerkiksi ampuma-aselaki (1/1998) ja kemikaalilaki (599/2013). Myös järjestyslaki (612/2003) kieltää tiettyjen aineiden ja esineiden hallussapidon yleisellä paikalla kokonaan (9 §). Nyt käsiteltävänä olevan ehdotuksen tilanteessa ei kuitenkaan olisi kyse vähäisistä tilanteista.

Toimivaltuuden käytöstä ilmoittamisessa sovellettaisiin ilmoittamisvelvollisuutta koskevia säännöksiä. Henkilö, jonka aine, esine tai omaisuus olisi joutunut toimivaltuuden käytön kohteeksi, voisi tehdä tutkimispyynnön tai kantelun tiedusteluvalvontavaltuutetulle. Puuttuminen perusoikeuksiin voidaan arvioida vähäiseksi.

Omaisuudensuojan tilapäinen rajoitus on välttämätön hyväksyttävän tavoitteen, eli viimekädessä Suomen suvereniteetin turvaamiseksi ja kansallisen turvallisuuden suojaamiseksi.

Oikeusturva

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.

Perustuslakivaliokunta toteaa perusoikeusuudistuksesta antamassaan mietinnössä, että perusoikeuksia rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä. (PeVM 25/1994 vp, s. 5.) Oikeusturvajärjestelyillä viitataan ennen kaikkea muutoksenhakumahdollisuuteen, mutta kysymykseen voivat tulla myös muut menettelylliset oikeusturvatakeet.

Euroopan ihmisoikeussopimuksen oikeutta tehokkaaseen oikeussuojakeinoon koskevan 13 artiklan mukaan jokaisella, jonka sopimuksessa 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.

Perustuslakivaliokunta on korostanut siviilitiedustelulainsäädännön käsittelyssä (PeVL 35/2018 vp.) vahvoja oikeusturvatakeita, laaja-alaista ja tehokasta tiedusteluvaltuuksien käytön valvontaa sekä riittäviä soveltamisrajoituksia. Kyse on poikkeuksellisesta rajoitusperusteesta, jossa on irtauduttu rikosperusteisesta toiminnasta ja joka tulee siten sovellettavaksi tilanteissa, joissa ei tiedonhankintavaiheessa tai muutoinkaan voida kohdistaa konkreettista ja yksilöityä rikosepäilyä (PeVM 4/2018 vp, s. 8).

Tiedustelun tarkoituksesta johtuen ennakollinen lupamenettely ja tiedustelun toimeenpanon valvonta eivät yleensä voi tulla tiedustelun kohteen tietoon. Menettelyn itsessään tulee siten antaa turva mielivaltaa vastaan. Valiokunnan mielestä EIT:n käytännöstä ilmenee, että oikeudellinen kontrolli tuomioistuimessa turvaa parhaiten kontrollin itsenäisyyden ja puolueettomuuden vaatimukset (PeVL 35/2018 vp., s 8).

Tiedustelumenetelmien osalta oikeusturvavaatimuksen täyttyminen asettaa erityisiä haasteita, koska toimivaltuuksien kohteet eivät voi turvautua tavanomaisiin oikeusturvakeinoihin varsinaisen tiedustelumenetelmän käyttöä koskevan päätöksen osalta. Tämän takia on oltava muita oikeusturvajärjestelyitä, joilla yksilön oikeusturva taataan riittävällä varmuudella samalla viranomaisten mielivaltaa ja väärinkäytöksiä ehkäisten.

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen ja valvonnan tehokkuus sekä asianmukaisuus. Myös ihmisoikeusvelvoitteet ja Euroopan unionin oikeusjärjestys edellyttävät luottamuksellisen viestin salaisuuden suojaan puuttuvien toimivaltuuksien käytön valvonnalta tehokkuutta ja riippumattomuutta. On tärkeää, että tiedusteluviranomaisella ei ole rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa.

Yksi tapa rajoittaa viranomaisen harkintavaltaa on osoittaa vakavinta puuttumista perusoikeussuojaan tarkoittava tiedustelumenetelmien käytöstä päättäminen riippumattomalle tuomioistuimelle (muun muassa Weber ja Saravia v. Saksa). Tietoliikennetiedustelun osalta

tiedusteluviranomaisella ei voi myöskään olla suoraa ja rajoittamatonta pääsyä tietoliikenneverkkoihin (Kennedy v. Yhdistynyt Kuningaskunta).

EIT:n ratkaisukäytännössä korostuu myös se, että ensisijainen vastuu toiminnan lainmukaisuudesta on viranomaisella. Tämä korostaa osaltaan sitä, että perusoikeuksien rajoittamisvaltuuksia annetaan vain henkilöille, joilla on riittävä koulutus ja pätevyys, mikä korostuu ennen kaikkea tilanteissa, joissa viranomaisen päätöksistä ei lähtökohtaisesti tehdä ilmoitusta päätöksen kohteelle (PeVL 17/1998 vp, s. 2–3). Riittävällä koulutuksella ja pätevyydellä varmistetaan myös perus- ja ihmisoikeusnormien tunnistaminen ja kyky perus- ja ihmisoikeusnormien soveltamiseen käsillä olevassa tilanteessa.

Ilmoitusvelvollisuuden toisena puolena on nähty sen preventiivinen vaikutus viranomaistoimintaan. Ilmoitusvelvollisuus toisin sanoen ohjaa viranomaista käyttämään tiedustelumenetelmiä oikeassa laajuudessa ja ehkäisten väärinkäytöksiä, koska tiedonhankinta tulee kohteen tietoisuuteen jossain vaiheessa.

Ilmoittamisella on katsottu lisäksi olevan merkitystä yleisesti tiedonhankintakeinojen käytön luotettavuuden kannalta. Yhteisöllä on yleisesti intressi valvoa, että tiedonhankintakeinoja käytetään hyväksyttävissä rajoissa.

Tiedustelumenetelmien osalta ei voida käyttää muutoksenhakumahdollisuutta tai ilmoitusvelvollisuutta oikeusturvan takeena. Voidaan kuitenkin katsoa, että tätä kompensoidaan muilla valvonta- ja oikeusturvajärjestelyillä. Näitä ovat riippumaton ulkopuolinen valvonta (tiedusteluvalvontavaltuutettu), joka valvoo laajasti toimintaa sekä tiedustelumenetelmien käyttöä etukäteisesti, reaaliaikaisesti ja jälkikäteisesti. Syvästi perusoikeuksiin puuttuvista tiedustelumenetelmistä päätöksen tekee tuomioistuin, jolle toimitettavassa vaatimuksessa esitettävistä seikoista on säädetty tarkoin laissa. Suojelupoliisin oman, sisäisen laillisuusvalvonnan lisäksi siviilitiedustelua valvoo tiedusteluvalvontavaltuutettu ja sisäministeriö. Toimintaa valvoo myös eduskunnan oikeusasiamies.

Edellä todettujen lisäksi sisäministeriön on toimitettava kertomus kerran vuodessa eduskunnan tiedusteluvalvontavaliokunnalle, eduskunnan oikeusasiamiehelle ja tiedusteluvalvontavaltuutetulle tiedustelumenetelmien käytöstä ja niiden suojaamisesta.

Kansalaisten ja yksittäisten henkilöiden osalta merkittävää on oikeus tehdä tiedusteluvalvontavaltuutetulle tutkimispyyntö (laki tiedustelutoiminnan valvonnasta 12 §) ja kantelu (laki tiedustelutoiminnan valvonnasta 11 §).

Vaikka sinänsä ilmoitusvelvollisuudella taataan yksilön mahdollisuus oikeusturvaan ja luodaan läpinäkyvyyttä, voidaan salaisessa viranomaistoiminnassa katsoa olevan kyse ennen kaikkea toiminnan vastuullisuudesta. Kyse on siitä, voidaanko virkamiehet saattaa oikeudelliseen vastuuseen mahdollisista laiminlyönneistä. Kuten edellä on todettu, siviilitiedustelutoiminnan valvontaan osallistuu useita ulkopuolisia, toiminnasta riippumattomia tahoja, jotka yksin ja yhdessä toteuttavat myös yksilön oikeusturvaa. Lisäksi vaatimuksia ja päätöksiä suojelupoliisissa tekevät erityisen koulutuksen ja perehtyneisyyden saaneet virkamiehet, tiedustelumenetelmän käytön edellytykset on tarkkaa säädetty, ja niitä koskevien vaatimusten ja päätösten sisällöstä on tarkkaan säädetty. Yksilö itse voi taas tehdä tutkimispyynnön tiedusteluvalvontavaltuutetulle tai tehdä kantelun tiedusteluvalvontavaltuutetulle.

Koska tiedusteluvalvontavaltuutetulle tehtävien tutkimispyyntöjen ja kanteluiden edellytyksenä ei ole kohteelle tai kohteeksi joutuneelle toimitettu ilmoitus, voidaan tämän osaltaan myös kompensoivan ilmoitusvelvollisuuden preventiivistä vaikutusta. Koska kuka vaan voi tehdä

tutkimispyynnön tai kantelun, voidaan suojelupoliisiin katsoa kohdistuvan laajaa valvontaa myös kansalaisten osalta. Tämä osaltaan ohjaa suojelupoliisia tarkkaan lainsoveltamiseen, jotta tiedusteluvalvontavaltuutetulle tehty tutkimispyyntö tai kantelu eivät johda jatkotoimenpiteisiin. Rikosvastuuseen saattaminen ja vahingonkorvausten maksaminen aiheuttavat koko siviilitiedustelutoiminnalle niin merkittäviä riskejä, kuten maineriski ja luottamuksen rapautuminen tiedusteluviranomaiseen, että tämäkin ohjaa suojelupoliisi toimimaan lakia tarkasti noudattaen ja toiminnan tarkkaan suuntaamiseen ja kohdentamiseen.

Tietoliikennetiedustelussa kokonaisuutena käsitellään henkilötietoja, joten sitä voidaan oikeusturvan osalta arvioida myös tästä näkökulmasta. Henkilötietojen käsittelystä suojelupoliisissa säädetään laissa henkilötietojen käsittelystä poliisitoimessa. Sen mukaan henkilö voi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 29 §:n mukaisesti pyytää tietosuojavaltuutettua tarkastamaan henkilötietojen ja niiden käsittelyn lainmukaisuus.

Vaikka tiedonhankinnan kohteelle ei annettaisi ilmoituksella tietoa häneen kohdistuneesta tietoliikennetiedustelusta tai muusta tiedustelusta, voidaan järjestelmän kokonaisuudessaan katsoa takaavan yksilön oikeusturvan asettamat vaatimukset ja viranomaisen vastuu toimenpiteistään voidaan toteuttaa. Tiedustelutoiminnassa yksilön oikeusturva toteutuukin useamman tekijän yhteisvaikutuksesta.

Ehdotetun sääntelyn ei siten katsota olevan ongelmallinen perustuslain 21 §:n kannalta.

12.1.3 Suomen täysivaltaisuus

Ehdotettu sääntely 1. lakiehdotuksen 57 §:ssä ulkomaisen virkamiehen osallistumisesta Suomen alueella tiedustelumenetelmän käyttöön on merkityksellistä perustuslain 1 §:ssä tarkoitetun Suomen täysivaltaisuuden kannalta.

Perustuslain 1 §:n 1 momentin mukaan Suomi on täysivaltainen tasavalta. Perustuslain 1 §:n 3 momentin mukaan Suomi osallistuu kansainväliseen yhteistyöhön rauhan ja ihmisoikeuksien turvaamiseksi sekä yhteiskunnan kehittämiseksi. Suomi on Euroopan unionin jäsen ja kuuluu Pohjois-Atlantin puolustusliittoon.

Perustuslain esitöissä on todettu, että ”valtion täysivaltaisuus kattaa sekä sisäisen että ulkoisen suvereenisuuden. Sisäisellä suvereenisuudella tarkoitetaan sitä, että valtion sisällä valtiovalta on korkein oikeudellinen muiden yläpuolella oleva valta. Sisäisen suvereenisuuden keskeisenä sisältönä on kyky säätää kaikkien valtion alueella julkista valtaa käyttävien viranomaisten ja muiden toimielinten toimivallasta. Siihen kuuluu myös valta päättää oikeusjärjestyksen sisällöstä, määrätä valtioelinten toiminnasta ja oikeus käyttää eri tavoin julkista valtaa valtion alueella oleviin ihmisiin ja esineisiin nähden. Ulkoisella suvereenisuudella tarkoitetaan valtion vapautta päättää itsenäisesti suhteistaan toisiin valtioihin ja kansainvälisiin järjestöihin.” (HE 1/1998 vp, s. 71). Suomi on myös solminut kahden välisiä puolustusyhteistyösopimuksia, joista keskeisenä Yhdysvaltain kanssa solmittu puolustusyhteistyösopimus.

Täysivaltaisuutta koskevan arvioinnin kannalta merkityksellistä on ennen kaikkea sillä, että vieraan valtion ja sen virkamiehen toiminta perustuu Suomen viranomaisten päätökseen (ks. myös PeVL 66/2016 vp, s. 3 ja PeVL 65/2016 vp, s. 3). Tiedustelumenetelmiä käytetään 1. lakiehdotuksen 57 §:n säännöksen mukaan suojelupoliisin kanssa ja tämän ohjauksessa ja valvonnassa. Lisäksi ulkomainen toimivaltainen virkamies on velvollinen noudattamaan suojelupoliisin hänelle antamia määräyksiä, rajoituksia ja ohjeita.

Ehdotetun sääntelyn ei siten katsota olevan ongelmallinen perustuslain 1 §:n kannalta.

Oikeusvaltioperiaate

Verrattuna voimassa olevaan poliisilain 5 a lukuun uutena säännöksenä 1. lakiehdotuksen 55 a §:ssä säädettäisiin, että Rajavartiolaitos voi suorittaa tiettyjen tiedustelumenetelmien käyttöön liittyvän yksittäisen toimenpiteen.

Ehdotus on merkityksellinen perustuslain 2 §:n 3 momentin kannalta. Sen mukaan julkisen vallan käyttämisen tulee perustua lakiin. Perustuslakivaliokunta on lausunnossaan PeVL 35/2008 vp arvioinut hallituksen esitykseen laiksi poliisin, tullin ja rajavartiolaitoksen yhteistoiminnasta sekä eräiksi siihen liittyviksi laeiksi (HE 26/2008 vp.) sisältynyttä vastaavanlaista säännöstä koskien poliisin, tullin ja rajavartiolaitoksen (PTR-viranomaiset) toimimista toisen PTR-viranomaisen tehtäväalueella. Perustuslakivaliokunnan lausunnon mukaan valiokunta on useasti katsonut, että yksityiseen kohdistuvan julkisen toimivallan siirtäminen sopimuspohjaisesti viranomaiselta toiselle ei ole valtiosääntöoikeudellisesti asianmukaista (ks. esim. PeVL 23/1994 vp, s. 2/I ja PeVL 11/1994 vp, s. 1/II). Valiokunta kuitenkin piti edellä mainittuun lakiehdotukseen sisältyvää järjestelyä PTR-viranomaisten yhteistyöstä eri viranomaisten voimavarojen tarkoituksenmukaisen käytön vaatimana ja myös valtiosääntöoikeudellisesti hyväksyttävänä.

Perustuslakivaliokunta piti aiempaan käytäntöönsä viitaten kuitenkin tarpeellisena, että säännöksiä oli sanonnallisesti täsmennettävä koskemaan vain "yksittäistä" rikostorjuntaan liittyvän toimenpiteen suorittamista. Vastaavasti mainintaa ilman pyyntöä suoritettavasta kiireellisestä toimenpiteestä on valiokunnan mielestä tarpeen kielellisesti tarkentaa osoittamaan, että myös näissä tapauksissa toinen PTR-viranomainen saa käyttää vain niitä toimivaltuuksia, jotka sillä on omalla tehtäväalueellaan.

Perustuslakivaliokunta on perustuslain 10 §:n tarkistamista koskevassa mietinnössään todennut, että ”tiedonhankinta kansallista turvallisuutta uhkaavasta toiminnasta voitaisiin säännöksen perusteella osoittaa vain kansallisesta turvallisuudesta huolehtivien viranomaisten (nykyisin suojelupoliisi, pääesikunta, puolustusvoimien tiedustelulaitos) tehtäväksi” (PeVM 4/2018 vp s. 8).

Ehdotetulla sääntelyllä ei tehtäisi perusoikeuksien kannalta ongelmallista tehtävien siirtämisestä viranomaiselta toiselle, vaan tehtävän suorittamisessa käytettäisiin toista viranomaista. Tiedustelumenetelmä, joita koskevia toimenpiteitä Rajavartiolaitos voisi tehdä, olisi rajattu tiettyihin yksittäisiin menetelmiin, joita vastaavia toimenpiteitä Rajavartiolaitos voi jo suorittaa rikosten ennalta, estämisessä ja paljastamisessa rikostorjunnasta Rajavartiolaitoksessa annetun lain mukaan. Lisäksi Rajavartiolaitoksen tehtävien suorittamiseen nimettävillä virkamiehillä on oltava riittävä koulutus suoriutua säännöksessä esitetyistä toimenpiteistä.

Hallituksen esityksen 1. lakiehdotuksen 55 a § on viranomaisten voimavarojen tarkoituksenmukaisen käytön vaatima ja siten linjassa perustuslakivaliokunnan kannanoton kanssa. Säännöstä voidaan pitää valtiosääntöoikeudellisesti hyväksyttävänä.

12.1.4 Tehtävän antaminen muulle kuin viranomaiselle

Säännösehdotuksia, jotka koskevat kansainvälistä yhteistyötä (1. lakiehdotuksen 57 §) , laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen (1. lakiehdotuksen 16 §), on arvioitava hallintotehtävän antamista muulle kuin viranomaiselle koskevan perustuslain sääntelyn kannalta.

Perustuslain 124 §:n mukaan julkinen hallintotehtävä voidaan antaa muulle kuin viranomaiselle vain lailla tai lain nojalla, jos se on tarpeen tehtävän tarkoituksenmukaiseksi hoitamiseksi eikä vaaranna perusoikeuksia, oikeusturvaa tai muita hyvän hallinnon vaatimuksia. Merkittävää julkisen vallan käyttöä sisältäviä tehtäviä voidaan kuitenkin antaa vain viranomaiselle (HE 1/1998 vp, s. 179).

Perustuslain esitöiden ja perustuslakivaliokunnan käytännön perusteella merkittävän julkisen vallan käyttämisenä on pidettävä esimerkiksi itsenäiseen harkintaan perustuvaa oikeutta käyttää voimakeinoja tai puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin. Poliisilain 5 a luvun 57 §:ssä ehdotetaan säädettäväksi ulkomaisen toimivaltaisen virkamiehen osallistumisesta tiedustelumenetelmien käyttöön ilman, että menetelmiä on tarkemmin rajattu. Kansainvälisen avun antamista ja pyytämistä koskevasta päätöksenteosta säädettäisiin erikseen siitä annetussa laissa (418/2017).

Vieraan valtion virkamiehen Suomessa toimimisen edellytyksenä olisi suojelupolisin päällikön nimenomainen päätös. Virkamiehen toiminta Suomessa olisi tilapäisluonteista sekä aina suomalaisen virkamiehen ohjaamaa ja valvomaa. Osallistuminen tiedustelumenetelmien käyttöön 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.

Hallituksen esityksen 1. lakiehdotuksen 16 §:n 2 momentissa ehdotetaan, että säännöksen tarkoittaman laitteen, menetelmän tai ohjelmiston asentamisen tai poisottamisen voisi suorittaa myös viranomaisen ulkopuolinen taho. Säännöksen tarkoittama toimi olisi rajattu asennukseen ja poisottamiseen.

Perustuslakiuudistuksen esitöiden mukaan merkittävänä julkisen vallan käyttämisenä on pidettävä esimerkiksi itsenäiseen harkintaan perustuvaa oikeutta käyttää voimakeinoja tai puuttua muuten merkittävällä tavalla yksilön perusoikeuksiin (HE 1/1998 vp, s. 179/II, ks. myös PeVL 28/2001 vp, s. 5—6). Valiokunta on käytännössään katsonut, että kotirauhan piiriin kohdistuvat tarkastusvaltuudet merkitsevät oikeutta puuttua merkittävällä tavalla perustuslaissa jokaiselle turvattuun kotirauhan suojaan eikä tällaista valtuutta voida näin ollen antaa yksityiselle tavallisella lailla (ks. PeVL 40/2002 vp, s. 3/II ja PeVL 46/2001 vp, s. 3/II).

Nyt käsiteltävänä olevan säännösehdotuksen mukaisesti viranomaisen ulkopuolisella ei ole itsenäiseen harkintaan perustuvaa oikeutta käyttää merkittävällä tavalla yksilön perusoikeuksiin puuttuvaa toimivaltaa. Säännöksen mukaisessa tilanteessa on kyse esineen, menetelmän tai ohjelmiston asentamisesta tai poisottamisesta, eli viranomaisen ulkopuolinen taho suorittaa teknisen toimenpiteen, jolla mahdollistetaan viranomaisen julkisen vallan käyttö. Asentaminen tai poisottaminen on suoritettava viranomaisen ohjeistuksen mukaisesti. Ulkopuolisella taholla ei ole myöskään pääsyä eikä tarkempaa tietoa siitä, mitä tietoa esineellä, menetelmällä tai ohjelmistolla hankitaan varsinaisesta kohteesta. Kyseessä ei olisi perustuslain 124 §:ssä tarkoitetusta julkisen hallintotehtävän antamisesta muulle kuin viranomaiselle.

Käsiteltävänä olevan säännösehdotuksen mukaan esineen, menetelmän tai ohjelmiston asentaminen ja poisottaminen tapahtuvat suojelupoliisin pyynnöstä. Näin ollen pyynnön kohteena oleva henkilö voi myös kieltäytyä toimenpiteen suorittamisesta; toiminta perustuisi henkilön vapaaehtoisuuteen eikä kyse olisi velvollisuudesta.

12.1.5 Perusoikeusrajoitusten täsmällisyys, tarkkarajaisuus ja oikeasuhtaisuus

Välttämättömyys

Luottamuksellisen viestin salaisuuden suojan rajoittamisen edellyttää perustuslain 10 §:n 4 momentin mukaan välttämättömyyttä. 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§; laki tietoliikennetiedustelusta siviilitiedustelussa 3 §), joka vakavasti uhkaa kansallista turvallisuutta. Siviilitiedustelun kohteet on määritelty laissa tyhjentävästi, joka vastaisi EIT:n ratkaisukäytännön vaatimuksia. 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).

Poliisilain ja tietoliikennetiedustelusta siviilitiedustelussa annettujen lakien kohteita koskevassa pykälissä yksilöidään ja konkretisoidaan perustuslain 10 §:n 4 momenttiin sisältyvää sääntelyä, jonka mukaan kansallista turvallisuutta vakavasti uhkaavalla toiminnalla tarkoitetaan seuraavia tiedustelun kohteita: 1) terrorismi, 2) ulkomainen tiedustelutoiminta, 3)joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö, 4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö, 5) kansanvaltaista yhteiskuntajärjestystä vakavasti uhkaava toiminta, 6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta, 7) vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille, 8) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi, 9)kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta, 10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta vakavasti uhkaava toiminta, 11) kansanvaltaista yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus. Koska jokainen kohta olisi johdettavissa yhdestä tai useammasta kansallisen turvallisuuskäsitteen kattamasta suojeluintressistä, pykälä on täyttänyt tältä osin korostuneet vaatimukset välttämättömyydestä ja ennakoitavuudesta.

Käsiteltävänä olevassa esityksessä esitetään uusia toimivaltuuksia, jotka kohdistuisivat edellä mainittuihin siviilitiedustelun kohteisiin. Koska kohteena oleva ennen kaikkea valtiollinen toiminta on vahvasti resursoitua ja toimijoiden toimintatavat kehittyvät kiihtyvää tahtia, on suojelupoliisin pystyttävä hankkimaan tarvittavaa tietoa myös varsinaisen viestin sisällön ulkopuolelta toimivaltuuksien asianmukaiseksi kohdentamiseksi.

Ehdotetulla sääntelyllä suojataan ennen kaikkea toisia perusoikeuksia, ja sääntelyyn on painava yhteiskunnallinen intressi

Täsmällisyys ja tarkkarajaisuus

Perustuslakivaliokunta on viranomaisten toimivaltuuksia koskevaa sääntelyä arvioidessaan pitänyt arvion lähtökohtana sitä, että viranomaisen toimivaltuuksien sääntely on merkityksellistä perustuslain 2 §:n 3 momentissa vahvistetun oikeusvaltioperiaatteen kannalta (ks. PeVL 51/2006 vp, s. 2). Julkisen vallan käytön tulee momentin mukaan perustua lakiin, ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Lähtökohtana on, että julkisen vallan käytön tulee olla aina palautettavissa eduskunnan säätämässä laissa olevaan toimivaltaperusteeseen (HE 1/1998 vp, s. 74/II). Lailla säätämiseen taas kohdistuu yleinen vaatimus lain täsmällisyydestä ja tarkkuudesta. Toimivaltasääntely on valiokunnan käsityksen mukaan yleensä merkityksellistä myös perustuslaissa turvattujen perusoikeuksien näkökulmasta (ks. PeVL 67/2016 vp, PeVL 10/2016 vp).

Tiedustelumenetelmien käytön yleiset edellytykset on koottu poliisilain 5 a luvun 4 §:ään ja tietoliikennetiedustelusta siviilitiedustelussa annetun lain 4 §:ään (Amann v. Sveitsi, Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska). Kaikkia tiedustelumenetelmiä koskevana yleisenä edellytyksenä on, että tiedustelumenetelmän käyttö on välttämätöntä ja että sillä voidaan perustellusti olettaa saatavan tärkeää tietoa tiedustelutehtävän kannalta. Jos tiedustelumenetelmä kohdistetaan valtiolliseen toimijaan, tiedustelumenetelmän käytön yleisenä edellytyksenä on, että tietojen saaminen on tarpeen tiedustelutehtävän kannalta. Kyse on niin sanotusta perustellusta tuloksellisuusodotuksesta.

Koska hakuehtojen määrittäminen ja muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuva tiedustelu voi sisältää merkittävää puuttumista yksityisen suojattuihin oikeushyviin, edellytyksenä on näiden menetelmien käytön osalta välttämättömyys. Lisäksi muun kuin valtiollisen toimijan tietoliikenteeseen kohdistuvassa tiedustelussa erityisenä edellytyksenä on, että tietoja ei saada hankittua muulla tiedustelumenetelmällä.

Lisäksi tiedustelumenetelmien käytölle säädettäisiin erityisiä edellytyksiä, joista ehdotetaan säädettäväksi kunkin tiedustelumenetelmän kohdalla (Amann v. Sveitsi, Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska). Toimivaltuuksia koskevasta sääntelystä käy ilmi, mitä valtuuksia käytettäessä saa tehdä ja miten tällöin on meneteltävä, vaatimuksen ja päätöksen tietosisältö, mikä taho tiedustelusta päättää, tiedustelua koskevan luvan, päätöksen tai määräyksen voimassaolo, mahdolliset kuuntelu-, katselu-, jäljentämis- ja tiedustelukiellot samoin kuin tiedustelun käytöstä ilmoittaminen tai ilmoittamatta jättäminen. Säännökset oikeusturvaan liittyen ovat selkeitä.

Hyväksyttävyys ja suhteellisuus

Siviilitiedustelussa on lain mukaan kunnioitettava perus- ja ihmisoikeuksia sekä noudatettava suhteellisuusperiaatetta, vähimmän haitan periaatetta, tarkoitussidonnaisuuden periaatetta ja syrjintäkieltoa. Periaatteet ohjaavat kaikkea tiedustelutoimintaa.

Suojelupoliisin on tiedustelutoimivaltuuksia käyttäessään valittava perusteltavissa olevista tiedustelumenetelmistä se, joka parhaiten edistää näiden perus- ja ihmisoikeuksien toteutumista.

Suhteellisuusperiaate edellyttää arvioimaan, onko tiedustelumenetelmän käyttö puolustettavaa suhteessa tiedustelua koskevan toimeksiannon tärkeyteen, kiireellisyyteen, tavoiteltavaan päämäärään ja muihin tilanteen kokonaisarviointiin vaikuttaviin seikkoihin. EIT ja EUT ovat ratkaisukäytännössään korostaneet suhteellisuusperiaatteen noudattamisen tärkeyttä erityisesti tietoliikennetiedustelun yhteydessä (esimerkiksi Zakharov v. Venäjä, Weber ja Saravia v. Saksa, Digital Rights Ireland). Tietoliikennetiedustelulta ja hakuehtojen määrittämiseltä edellytetään siksi viimesijaisuutta eli sitä, että tietojen hankkiminen muulla menetelmällä olisi mahdotonta tai kohtuuttoman vaikeaa, ja hakuehtojen määrittämiseltä välttämättömyyttä. Lisäksi muun kuin

valtiollisen toimijan tietoliikenteen tiedustelu edellyttää, että tietoja ei ole hankittavissa muulla tavalla.

Vähimmän haitan periaatteesta johtuu, että suojelupoliisin toimenpiteillä ei kenenkään oikeuksiin saa puuttua enempää eikä kenellekään saisi aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tiedustelutehtävän suorittamiseksi.

Suojelupoliisi saa tarkoitussidonnaisuuden periaatteen mukaisesti käyttää tiedustelutoimivaltuuksiaan vain säädettyyn tarkoitukseen.

Siviilitiedustelun toimenpiteiden kohdentaminen on toteutettava syrjimättömästi. Tästä on siviilitiedustelulainsäädännössä nimenomaiset säännökset. Siviilitiedustelun toimenpiteen kohdentaminen ei saa ilman hyväksyttävää perustetta perustua henkilöiden ikään, sukupuoleen, alkuperään, kansalaisuuteen, asuinpaikkaan, kieleen, uskontoon, vakaumukseen, mielipiteeseen, poliittiseen toimintaan, ammattiyhdistystoimintaan, perhesuhteisiin, terveydentilaan, vammaisuuteen, seksuaaliseen suuntautumiseen tai muuhun henkilöön liittyvään syyhyn. Sääntely vahvistaa perustuslain 6 §:n 2 momentin yhdenvertaisuusperiaatetta tiedustelutoiminnassa.

Oikeusturvajärjestelyt

Tiedustelutoiminnassa korostuvat oikeusturvajärjestelyjen ja valvonnan tehokkuus sekä asianmukaisuus. Myös ihmisoikeusvelvoitteet ja Euroopan unionin oikeusjärjestys edellyttävät luottamuksellisen viestin salaisuuden suojaan puuttuvien toimivaltuuksien käytön valvonnalta tehokkuutta ja riippumattomuutta.

Tiedusteluviranomaisella ei voi olla rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa. Yksi tapa rajoittaa viranomaisen harkintavaltaa on osoittaa vakavinta puuttumista perusoikeussuojaan aiheuttavien tiedustelumenetelmien käytöstä päättäminen tuomioistuimelle (muun muassa Weber ja Saravia v. Saksa). Tiedusteluviranomaisella ei myöskään voi olla suoraa ja rajoittamatonta pääsyä tietoliikenneverkkoihin (Kennedy v. Yhdistynyt Kuningaskunta). Tätä ehkäistään sillä, että tietoliikennetiedustelun kokonaisuuden edellyttämän tuomioistuimen luvan mukaisen kytkennän tietoliikenneverkkoon tekee jokin muu taho kuin tiedusteluviranomainen itse.

EIT:n mukaan lupaharkinnan alan on käytävä ilmi laista. Laissa ehdotetaan säädettäväksi lupaa koskevan hakemuksen ja päätöksen sisällöstä. Lupaharkinnan, joka perustuu hakuehtojen tai kansallista turvallisuutta vaarantavan toiminnan tai henkilöiden mahdollisen täsmällisen kuvauksen hyväksymiseen, voidaan katsoa täyttävän EIT:n vaatimukset.

Lupa nyt ehdotetuissa tiedustelumenetelmissä voitaisiin antaa enintään kuudeksi kuukaudeksi kerrallaan.

12.2 Säännösehdotukset Euroopan ihmisoikeustuomioistuimen ratkaisukäytännön kannalta

12.2.1 Tietoliikennetiedustelu

EIT on lukuisissa ratkaisuissaan todennut, että tietoliikennetiedustelu on mahdollista EIS:n 8 artiklan nojalla ja se kuuluu kansalliseen harkintavaltaan. EIT on myös todennut, että kansallisen turvallisuuden alalla kansallinen harkintavalta kansallisen turvallisuuden laajuudesta ja käytettävistä keinoista kuuluu jäsenvaltiolle.

Uusimmassa tietoliikennetiedustelu koskevassa ratkaisukäytännössään EIT on toistanut pitkäaikaista linjaansa tietoliikennetiedustelusta, mutta myös kehittänyt ratkaisukäytäntöään sallittavalle tietoliikennetiedustelulle asettamistaan edellytyksistä. Kuten aiemmin EIT:n ratkaisukäytäntöä koskevassa jaksossa 5.2.1 on tuotu ilmi, sallittavuuden edellytyksiä on nykyisin kahdeksan aiemman kuuden sijaan.

Huomattava on myös se, että EIT:n käsittelyssä olleissa ratkaisuissa tietoliikennetiedustelua ei ole jaettu eri toimivaltuuksiin, kuten Suomessa. Näin ollen saman toimivaltuuden nojalla on voitu suorittaa muun muassa tietoliikenteen teknisen kehittymisen seurantaa, määrittää uusia hakuehtoja sekä hankkia tietoja varsinaisesta uhasta. Kuvaavaa on se, että tapauksessa Centrum för Rättvisa EIT toteaa, että signaalitiedustelun tekninen kehittäminen on itsestään selvää (kohta 207). Vastaavasti hakuehtojen määrittämisestä on ruotsalaisessa signaalitiedustelua koskevassa lainsäädännössä todettu ainoastaan lain perusteluissa.

EIT ei torju ehdottomasti ns. massavalvonnan (bulk interception regime) käyttöä. EIT katsoo, että sillä torjuttavien uhkien vakavuus, uhkien takana olevien henkilöiden kyky toimia paljastumatta tietoverkoissa ja sähköisen viestinnän reitityksen ennakoimattomuus perustelevat kansallista turvallisuutta vaarantavien uhkien tunnistamiseen tähtäävän massavalvonnan käyttöönoton kuulumista kansallisen harkintamarginaalin alaan. EIT on pitänyt yleisemminkin harkintamarginaalia laajana kansallisen turvallisuuden turvaamisen keinovalikoiman valinnassa (mm. Weber ja Saravia kohta 106, Big Brother Watch kohta 274 ja Centrum för Rättvisa kohta 252). EIT painottaa kuitenkin, että sekä kohdistettujen että massavalvontajärjestelmien sääntelyn tulee vallan väärinkäytön estämiseksi täyttää ainakin edellä luetteloidut vähimmäisvaatimukset.

Nyt käsiteltävänä olevan esityksen 2. lakiesityksen 10 a, 10 b, 10 c, 10 d §:ää on arvioitava EIT:n uudemmassa ratkaisukäytännössä toteamien kahdeksan edellytyksen kautta. Laissa on säädettävä: 1) perusteista, joiden perusteella tiedon hankinta voidaan sallia, 2) olosuhteista, joissa tiedonhankinta voi kohdistua henkilön viestintään, 3) luvan myöntämismenettelystä, 4) tiedon valinnassa, tutkimisessa ja käytössä noudatettavista menettelyistä, 5) varotoimista, joita on noudatettava luovutettaessa materiaalia eri osapuolille, 6) toimenpiteen kestosta, tiedon säilyttämisen rajoituksista ja olosuhteista, joissa tieto on poistettava ja tuhottava, 7) menettelyistä ja yksityiskohtaisista säännöistä, joilla riippumaton viranomainen valvoo edellä mainittujen takeiden noudattamista, ja valvojan valtuudesta puuttua lainvastaiseen toimintaan sekä 8) riippumattomasta jälkikäteisestä valvonnasta ja seuraamuksista.

Esityksen 2. lakiehdotuksen edellä viitatut säännökset ovat huomattavasti yksityiskohtaisempia kuin mitä EIT on ratkaisukäytännössään edellyttänyt. Kuten esimerkiksi tapauksessa Centrum för Rättvisa EIT tuo ilmi, myös massamainen tiedustelutoiminta voi olla kansallisen harkintamarginaalin sisällä, kunhan edellytykset täyttyvät. Nyt käsiteltävänä olevassa esityksessä toimivaltuuksista olisi säädetty yksityiskohtaisesti käyttötarkoitusperusteisesti. Lisäksi jokaisen toimivaltuuden käyttöä on rajattu tiettyyn Suomen rajan ylittävän viestintäverkon osan lisäksi kohdentuvaksi tietoihin, joita kyseistä toimivaltuutta käyttämällä on tarkoitus hankkia, viime kädessä varsinaisessa tietoliikennetiedustelussa hakuehtoperusteisesti.

Yleisesti voidaan todeta, että tietoliikennetiedustelusta siviilitiedustelussa annetun lain 3 ja 4 §:ssä säädetään niistä kohteista ja edellytyksistä, joiden perusteella tietoliikennetiedustelua voidaan käyttää.

Luvan kaikkiin tietoliikennetiedustelun kokonaisuudessa oleviin toimivaltuuksiin myöntää riippumaton tuomioistuin. Tuomioistuimen luvassa määritetään myös toimenpiteen kesto, joka on korkeintaan kuusi kuukautta.

Tiedon hävittämisestä säädetään lain 15 §:ssä.

Toiminnan ensisijainen laillisuusvalvonta tapahtuu EIT:n vakiintuneen oikeuskäytännön mukaisesti viranomaisessa itsessään, eli suojelupoliisissa. Ulkopuolisesta valvonnasta säädetään tiedustelutoiminnan valvonnasta annetussa laissa. Lain mukaisesti tiedusteluvalvontavaltuutettu valvoo siviilitiedustelua etukäteisesti, reaaliaikaisesti ja jälkikäteisesti. Lisäksi tiedusteluvalvontavaltuutettu voi keskeyttää tiedustelumenetelmän käytön, jos katsoo valvottavan menetelleen lainvastaisesti. Tiedusteluvalvontavaltuutettu voi myös määrätä tiedot välittömästi hävitettäväksi ja ilmoittaa havaitsemansa lainvastaisen menettelyn esitutkintaan.

Lisäksi valvontaa suorittaa eduskunnan oikeusasiamies ja parlamentaarista valvontaa eduskunnan tiedusteluvalvontavaliokunta.

Teknisten tietojen käsittely ja hakuehtojen määrittäminen

EIT katsoi tapauksessa Centrum för Rättvisa, että Ruotsin laissa säädetty mahdollisuus kerätä tietoliikennettä signaalitiedustelun kehittämiseksi on kansallisen harkintamarginaalin rajoissa (päätöksen kohdat 291–293). EIT:n ratkaisukäytännössä tietoliikennetiedustelun kaltaista järjestelmää ei ole jaoteltu erilaisiin käyttötarkoituksiin, vaan järjestelmät kattavat kokonaisuudessaan sen, mitä nyt esitetyssä 2. lakiehdotuksessa olisi säädetty 10 a § ja 10 c §:ssä ja liittyen sotilastiedustelulain 66 §:ssä, 67 a §:ssä, 68 §:ssä ja 70 §:ssä säädettäväksi ehdotettuun. Lisäksi tapauksissa ei ole otettu kantaa siihen, pitäisikö toiminnan olla hetkellistä tai muuta vastaavaa.

Nyt käsiteltävän olevan esityksen 2. lakiehdotukseen ehdotetaan uutta 10 a §:ää. Suojelupoliisi voisi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulaitoksen 66 §:ssä tarkoitettujen teknisten tietojen keräämiseksi. Puolustusvoimien tiedustelulaitos luovuttaisi tiedot suojelupoliisille. Lisäksi teknisten tietojen käsittelyn toimivaltuutta voitaisiin käyttää voimassa olevassa laissa määritellyn viestintäverkon osan tunnistamisen lisäksi tietoliikenteen reitittymisen ja muutosten tunnistamiseen. Toimivaltuuden käyttö kohdistuu ainoastaan tietoliikenteen teknisiin tietoihin. Säännösehdotukseen liittyvän ehdotetun sotilastiedustelulain 66 §:ää ehdotetaan muutettavaksi niin, että siitä poistetaan hetkellisyys.

Esityksen 2. lakiehdotuksen 10 a §:ssä olisi säädetty niistä perusteista, joilla suojelupoliisilla olisi oikeus tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä. Perusteita olisivat 1) tilastollinen analyysi tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan ja 2) tietoliikenteen reitittymisen ja muutosten seuraaminen. Säännösehdotus ei kohdistuisi henkilön viestintään, koska säännös koskisi ainoastaan tietoliikenteen teknisiä tietoja.

Luvan myöntämismenettelystä säädettäisiin 2. lakiehdotuksen 10 b §:ssä. Luvan kesto olisi 10 b §:ssä ehdotetun mukaisesti 6 kuukautta.

Tietoliikenteen teknisiä tietoja voitaisiin käyttää myös 18 kuukauden ajan niiden saamisesta teknisten tietojen käsittelyssä ja 12 kuukauden ajan hakuehtojen määrittämiseen (2. lakiehdotus 10 a § ja10 c §) sekä varsinaisessa tietoliikennetiedustelussa. Muilta osin tiedot olisi hävitettävä laissa säädettyjen menettelyjen mukaisesti.

EIT ei ole ottanut suoranaisesti kantaa tietoliikennetiedustelussa hakuehtojen määrittämiseen. Centrum för Rättvisa -tapauksessa EIT toteaa, että Ruotsin laissa säädetty mahdollisuus kerätä tietoliikennettä signaalitiedustelun kehittämiseksi on kansallisen harkintamarginaalin rajoissa (päätöksen kohdat 291–293). EIT ei nähnyt estettä, että tietoliikennettä saatiin kerätä myös kehittämistarkoituksiin.

EIT ratkaisukäytännöstä ei ole havaittavissa tapauksia, joissa tietoliikennetiedustelun kaltaista järjestelmää olisi jaoteltu vastaavalla, yhtä yksityiskohtaisella tavalla kuin nykytilassa on Suomessa ja nyt esitettävien ehdotusten myötä. Näin ollen suomalaista järjestelmää voidaan pitää tarkkuudeltaan ja tarkkarajaisuudeltaan poikkeuksellisena. Lisäksi EIS:n kannalta merkittävää on myös se, että jokaisesta tietoliikennetiedustelun kokonaisuudessa olevasta toimivaltuudesta päätöksen tekee tuomioistuin.

Näin ollen voidaan katsoa, että 2. lakiehdotuksen10 a § ja 10 c § ovat EIS:n kannalta ongelmattomia.

Viestinnän sisältöön menevät hakuehdot

Esityksen 2. lakiehdotuksen 5 §:ään esitettyjen muutosten myötä säännöksestä poistettaisiin kielto käyttää Suomessa oleskelevan henkilön hallussa olevan tai tämän oletettavasti muuten käyttämän telepäätelaitteen tai teleosoitteen yksilöiviä tietoja.

EIT on ratkaisukäytännössään korostanut sitä, että tiedonhankinnan on kohdistuttava valtion rajan ylittävään tietoliikenteeseen (esim. Centrum för Rättvisa kohta 236 ja siinä viitatut tapaukset Weber ja Saravia sekä Liberty ja muut). Tätä voidaan toteuttaa muun muassa kohdistamalla tiedonhankinta tiettyihin valtion rajan ylittäviin pisteisiin ja suodattamalla joukosta valtion sisäinen tietoliikenne. Kotimaisen tietoliikenteen poistaminen on voitu toteuttaa myös jälkikäteisesti tämän tultua ilmi, vaikkei sitä voidakaan pitää optimaalisena.

EIT ei ole ottanut kantaa siihen, voiko toinen viestinnän osapuoli olla tiedustelumenetelmää käyttävän viranomaisen kotimaassa. EIT käsittelemissä tapauksissa on korostunut se, että kyse on oltava rajat ylittävästä uhkasta ja että valtion sisäiseen tietoliikenteeseen ei ole syytä kohdistaa näin pitkälle menevää tiedonhankintaa.

Kuten on jo tuotu esiin, EIT on pitänyt tietoliikennetiedustelunkaltaisia järjestelmiä arvioidessaan keskeisenä edellytyksenä sitä, että se perustuu hakuehtojen käyttöön. EIT on myös hyväksynyt sen, että tietoliikennettä käytetään järjestelmän kehittämiseen ja suuntaamiseen. EIT ei siis tee eroa sen suhteen, kohdistuvatko hakuehdot viestinnän välitystietoihin vai viestin semanttiseen sisältöön; huomiota ei ole kiinnitetty siihen, mihin tietoihin ja mihin osaan tietoliikennevirtaan hakuehto kohdistuu.

Yleisesti EIT:n ratkaisukäytännössä on korostunut se, että ulkopuolisen tuomioistuimen tai sitä vastaavan on hyväksyttävä käytettävät hakuehdot ennen kuin tiedustelumenetelmän käyttö aloitetaan.

Esityksen 2. lakiehdotuksen 5 §:n ei voi katsoa olevan ristiriidassa EIS:n kanssa.

10.4.2 Muuhun kuin valtiolliseen toimijaan kohdistuvasta tietoliikennetiedustelusta ilmoittamisesta luopuminen

EIT on lukuisissa ratkaisuissaan, viimeisimpänä Centrum för Rättvisa ja Big Brother Watch, ottanut kantaa, että EIS:n 8 artiklan ja 13 artiklan kannalta keskeistä on se, onko tiedustelumenetelmien kohteeksi joutuneella mahdollisuus saada tieto kohteeksi joutumisesta. Se, miten kohteeksi joutunut tai sellaista epäilevä saa riittävän tiedon asiasta, voidaan toteuttaa joko ilmoittamalla tai ulkopuolisen riippumattoman toimielimen toimesta. Centrum för Rättvisa ja Big Brother Watch -tapauksissa EIT toteaa, että henkilö voi saada parempaa suojaa viranomaisten toimintaa vastaan toimielimeltä, jolle kuka tahansa itsensä tiedustelumenetelmän käytön kohteeksi epäilevä voi saattaa asiansa tutkittavaksi. Tällöin korostuu toimielimen itsenäisyys tiedustelu-

viranomaisen toiminnasta sekä riittävät toimivaltuudet tosiasiallisesti puuttua viranomaisen toimintaan.

Järjestelmissä, joissa oikeussuoja perustuu ilmoittamiseen, voi käytännössä käydä niin, että erilaisten poikkeusjärjestelyiden takia kohteeksi joutunut henkilö ei voi kuitenkaan käytännössä koskaan saada tietoa tiedustelumenetelmän kohteeksi joutumisesta.

Nyt käsiteltävä olevassa hallituksen esityksessä ehdotetaan, että tietoliikennetiedustelusta ei ilmoitettaisi sen kohteeksi joutuneelle. Nykytilassa valtiolliselle toimijalle ei ilmoiteta missään tilanteessa. EIS:n kannalta ratkaisu noudattelisi yleiseurooppalaista linjaa; käytännössä missään maassa tietoliikennetiedustelusta ei ilmoiteta, tosin Ruotsissa on käynnissä lainmuutosprosessi tämän osalta.

EIS:n järjestelmässä ilmoittamisvelvollisuus voidaan korvata muilla järjestelyillä, jotka takaavat vastaavat lopputuloksen kohteeksi joutuneelle tai joka epäilee joutuneensa tiedustelumenetelmän käytön kohteeksi. EIT:n käytännössä todetusti tätä kautta kohteeksi joutunut saa usein asiansa käsiteltyä paremmin kuin ilmoituksen perusteella. Suomalaisessa tiedustelulainsäädännön kokonaisuudessa järjestely tarkoittaisi tiedusteluvalvontavaltuutettua. Lisäksi kokonaisuudessa on huomioitava, että syvimmin perusoikeuksiin puuttuvista tiedustelumenetelmien käytöstä päätöksen tekee rippumaton tuomioistuin.

12.3 Säännösehdotukset Euroopan unionin tuomioistuimen ratkaisukäytännön kannalta

Kuten aiemmin on todettu jaksossa 5.2.2, Euroopan unionilla ja sen tuomioistuimella ei ole sinänsä toimivaltaa ratkaista jäsenvaltioiden kansallisen turvallisuuteen liittyviä kysymyksiä. Toimivaltaa voi kuitenkin olla välillisesti, kuten tilanteessa, jossa palveluntarjoajat velvoitetaan tallentamaan ja siirtämään asiakkaistaan yksityisyyden suojan alaan kuuluvia tietoja kansallisen turvallisuuden suojaamisen tarpeisiin.

Euroopan unionin tuomioistuin on ratkaisussaan La Quadrature du Net ym. v. Premier ministre ym. (yhdistetyt asiat C-511/18, C-512/18 ja C-520/18) katsonut (kohta 103), että kun jäsenvaltiot panevat suoraan täytäntöön sähköisen viestinnän luottamuksellisuudesta poikkeavia toimenpiteitä asettamatta tällaisen viestinnän palveluntarjoajille käsittelyä koskevia velvollisuuksia, asianomaisten henkilöiden tietosuojaan ei sovelleta sähköisen viestinnän tietosuojadirektiiviä. Ehdotetussa sääntelyssä ei asetettaisi viestinnän palveluntarjoajille velvollisuuksia, joten sääntelyä ei ole tarpeen arvioida tarkemmin mainitun direktiivin näkökulmasta.

Kuitenkin voidaan todeta, että nyt käsiteltävät säännösehdotukset ovat yhteensopivia Euroopan unionin perusoikeuskirjan ja siihen liittyvän Euroopan unionin tuomioistuimen oikeuskäytännön kanssa, erityisesti viestintäsalaisuusdirektiivin (2002/58/EY) ja siihen liittyvän La Quadrature du Net -ratkaisun valossa. Edellä viitatun ratkaisun mukaisesti säännösehdotuksissa edellytyksenä on tuomioistuimen lupa, lainsäädännön on määriteltävä selkeästi ja tarkasti lain tarkoitus ja rajat sekä toimintaa on valvottava tuomioistuimen ennakollisen valvonnan lisäksi riippumaton ulkopuolinen valvoja, jonka toimivalta kattaa koko tiedustelutoiminnan ennakollisesti, reaaliaikaisesti ja jälkikäteisesti.

Unionin tuomioistuimen aiheeseen liittyvät ratkaisut (mm. Digital Rights Ireland (C-293/12 ja C-594/12), Schrems (C-362/14) ja Tele2 Sverige ja Watson (C-698/15 ja C-203/15)) koskevat teleyritysten yleistä ja erittelemätöntä tunnistamistietojen keräämistä ja säilyttämistä viranomaistarkoituksiin. Nyt käsiteltävänä olevassa esityksessä kyse on viranomaisen itsensä keräämistä ja säilyttämistä tiedoista, joiden hankkimista ja tallentamista rajataan fyysisesti, teknisesti,

määrällisesti ja ajallisesti. Perusperiaatteiden lisäksi näin ollen Euroopan unionin tuomioistuimen ratkaisuilla ei ole vaikutusta nyt esitettyjen lakiehdotusten kannalta.

Uutena toimivaltuutena ehdotetussa hakuehtojen määrittämisessä on kyse tietoliikenteen säännönmukaisuuksien tai ominaispiirteen, kuten käytettävien tai uusien protokollien, etsimisestä, jonka perusteella voidaan muodostaa parempia ja tarkempia hakuehtoja. Tietoliikennettä käsiteltäisiin muodossa, josta viestin semanttinen sisältö ei ole suoraan selvitettävissä. Semanttisen sisällön selvittäminen vaatisi muiden tuomioistuimen lupaa edellyttävien toimenpiteiden suorittamista.

Kuten EUT on ratkaisuissaan linjannut, esimerkiksi pelkkä IP-osoite ei ole sellainen tieto, jonka pohjalta voitaisiin tehdä henkilön yksityiselämään käyviä päätelmiä. Koska ehdotetussa toimivaltuudessa ei pyritä eikä sallita tiedon semanttisen sisällön hyödyntämistä taikka tietojen yhdistelemistä tällaisen tiedon saamiseksi kohteesta taikka kohteen seuraamiseksi, voidaan toimivaltuuden katsoa joka tapauksessa täyttävän myös EUT asettamat vaatimukset.

12.4 Julkisuus

Perustuslakivaliokunta on määrittänyt yleisiä perusoikeuksien rajoittamista koskevia edellytyksiä. Perusoikeusrajoituksen tulee ensinnäkin olla lailla säädetty sekä tarkkarajainen ja riittävän täsmällisesti laissa määritetty. Perusteen, jolla perusoikeutta rajoitetaan, tulee olla perusoikeusjärjestelmän kokonaisuuden kannalta hyväksyttävä. Perusoikeusrajoitusten tulee olla välttämättömiä hyväksyttävän tavoitteen saavuttamiseksi ja muutenkin suhteellisuusvaatimuksen mukaisia. Perusoikeuden rajoitus on sallittu vain, jos tavoite ei ole saavutettavissa perusoikeuteen vähemmän puuttuvin keinoin. Rajoitus ei saa mennä pidemmälle kuin on perusteltua ottaen huomioon rajoituksen taustalla olevan intressin painavuus suhteessa rajoitettavaan oikeushyvään. Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvaa rajoitusta. Perusoikeuksia rajoitettaessa on huolehdittava riittävistä oikeusturvajärjestelyistä. Rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa. Ks. PeVM 25/1994 vp, s. 4–5, PeVL 3/2014 vp, s. 3, PeVL 38/2013 vp, s. 4–5, PeVL 16/2013 vp, s. 2/1, PeVL 8/2013 vp, s. 3/I, PeVL 37/2013 vp, PeVL 14/2013 vp, s. 4/I, PeVL 2/2013 vp, s. 3, PeVL 5/2009 vp, s. 3, PeVL 8/2006 vp.

Perustuslain 12 §:n 2 momentin mukaan viranomaisen hallussa olevat asiakirjat ja muut tallenteet ovat julkisia, jollei niiden julkisuutta ole välttämättömien syiden vuoksi lailla erikseen rajoitettu. Jokaisella on oikeus saada tieto julkisesta asiakirjasta ja tallenteesta. Perustuslain 12 §:n 2 momentissa turvatun julkisuusperiaatteen kannalta olennainen julkisuuslaki on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 43/1998 vp).

Perustuslain 12 §:n 2 momentissa asiakirjajulkisuudesta säädetty merkitsee, että asiakirjojen julkisuutta voidaan rajoittaa perustuslain mukaan ainoastaan lailla ja vain, milloin siihen on välttämättömiä syitä. Kysymys ei perustuslakivaliokunnan mukaan siten ole siitä, että perustuslaissa esimerkiksi jätettäisiin kyseisen oikeuden sisältö lailla määriteltäväksi, vaan lainsäätäjän toimivaltaan kuuluu pelkästään sellaisten julkisuuden rajoitusten asettaminen, joita voidaan pitää perustuslaissa tarkoitetulla tavalla välttämättöminä (PeVL 43/1998 vp, s. 3/I). Julkisuuden rajoituksen sitominen välttämättömään merkitsee, että rajoitus voi kohdistua vain sekä sisällöllisesti että ajallisesti välttämättömänä pidettävään syyhyn. Edellä jaksossa ” Nykytila ja sen arviointi” ja säännöskohtaisissa perusteluissa on esitetty perusteluita sille, miksi salassapitoajan pidentäminen esityksen tarkoittamien asiakirjojen osalta on välttämätöntä. Välttämätön syy salassapitoajan pidentämiselle liittyy ensinnäkin muuttuneeseen turvallisympäristöön, Suomen Nato-jäsenyyteen ja tarpeeseen varmistaa, ettei kansainvälisten järjestöjen ja toisten valtioiden salassa pitämää tietoa julkisteta vastoin niiden tahtoa Suomen kansalliseen käyttöön laadittujen

asiakirjojen kautta. Toiseksi on huomioitava, että eräitä 25 vuotta sitten laadittuja ulkoministeriön, tasavallan presidentin tai tasavallan presidentin kanslian asiakirjoja, kuten muistioita, raportteja sekä TP UTVA-asiakirjoja, on edelleen välttämätöntä pitää salassa, koska niiden julkitulo saattaisi paljastaa Suomen haavoittuvuuksia. Kolmas välttämätön syy salassapitoajan pidentämiselle on, että tiettyjen asiakirjojen julkiseksitulo liian varhaisessa vaiheessa voisi haitata Suomen diplomaattien toimintaedellytyksiä vieraissa valtioissa ja sitä kautta heikentää Suomen kansainvälisten suhteiden hoitamista. Välttämätön syy on myös se, että suojelupoliisin, joka siviilitiedusteluviranomainen, asiakirjojen salassapito tulisi vahvistaa lain tasolla, koska asiakirjat koskevat kansallista turvallisuutta (valtioturvallisuutta) ja vastaava tarve on sotilastiedustelun osalta maanpuolustukseen liittyen.

Ehdotettu salassapitoajan pidentäminen vaikuttaa kansalaisten mahdollisuuksiin saada tietoja viranomaisten toiminnasta ja yhteiskuntaoloista. Julkisuuslain salassapitoajan pidentäminen 25 vuodesta 40 tai 60 vuoteen rajoittaa siten perustuslain 12 §:n 2 momentissa säädettyä kansalaisten oikeutta saada tietoa.

Julkisuusperiaate liittyy myös perustuslaissa turvattuun sananvapauteen. Perustuslain 12 §:n 1 momentissa säädetään jokaisen oikeudesta sananvapauteen. Lain 12 §:ssä turvattuun sananvapauteen sisältyy oikeus ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä kenenkään ennakolta estämättä. Sananvapaussäännöksen keskeisenä tarkoituksena on taata kansanvaltaisen yhteiskunnan edellytyksenä oleva vapaa mielipiteenmuodostus, avoin julkinen keskustelu, joukkotiedotuksen vapaa kehitys ja moniarvoisuus sekä mahdollisuus vallankäytön julkiseen kritiikkiin. Riittävän julkisuuden takaaminen on edellytys yksilöiden mahdollisuudelle vaikuttaa ja osallistua yhteiskunnalliseen toimintaan. Julkisuus on myös vallankäytön ja viranomaistoiminnan kritiikin ja valvonnan edellytys (HE 309/1993 vp, s. 58/I). Julkisuudella ja tiedonsaantioikeuksista säätämällä myös osaltaan edistetään perustuslain 14 §:ssä tarkoitetulla tavalla yksilön mahdollisuuksia osallistua yhteiskunnalliseen toimintaan ja vaikuttaa häntä itseään koskevaan päätöksentekoon (ks. ”Julkisuuslain ajantasaistaminen”, Työryhmän mietintö, Oikeusministeriön julkaisuja 2023:32, sivu 250). Salassapitoajan pidentäminen 25 vuodesta 40 tai 60 vuoteen rajoittaa siten myös kansalaisten sananvapautta ja oikeutta osallistua yhteiskunnalliseen toimintaan. Salassapitoajan pidentäminen vaikeuttaisi esimerkiksi lehdistön ja historiantutkijoiden mahdollisuuksia tutkia aineistoja.

Kuten julkisuuslakia koskevissa esitöissä (HE 30/1998) on todettu, vaikka julkisuus onkin pääsääntö viranomaistoiminnassa, se ei voi olla poikkeukseton. Yhteiskunnassa on monia tärkeitä yleisiä ja yksityisiä etuja, joita julkisuus voisi loukata. Yleiset ja yksityiset edut ilmenevät erityisesti julkisuuslain 24 §:ssä olevista ja muissa laeissa säädetyistä salassapitosäännöksistä. Yleisiä etuja ovat valtion turvallisuuden varmistaminen, Suomen kansainvälisten suhteiden ja tulo-, finanssi-, raha- ja valuuttapolitiikan hoitaminen, rikosten selvittäminen ja ehkäiseminen, julkinen taloudellinen etu, pääoma- ja rahoitusmarkkinoiden sekä rahoitus- ja vakuutusjärjestelmien toimivuus, viranomaisen tarkastus- ja valvontatoimen tehokkuus, luonnonarvojen suojelu, tiedonantajan luottamuksen suoja samoin kuin viranomaisten tasavertainen asema yksityiseen toiminnan harjoittajaan nähden sopimusosapuolena ja asianosaisena. Näillä eduilla on vaihtelevan kiinteä yhteys perusoikeuksiin. Kansainvälisiä suhteita koskeva salassapito perustuu kansainvälisen yhteisön yleiseen käytäntöön (HE 30/1998, s. 46).

Julkisuuden rajoittaminen eli salassapitoajan pidentäminen voidaan toisaalta nähdä myös suojaavan yksilön perus- ja ihmisoikeuksia, sillä suojaamalla Suomen kansainvälisiä suhteita ja kansallista turvallisuutta samalla suojataan kansalaisten turvallisuutta (perustuslain 7 §).

Suomi on myös osapuolena viranomaisten asiakirjojen julkisuudesta tehdyssä Euroopan neuvoston yleissopimuksessa (SopS 101-103/2020) Sopimus tuli kansainvälisesti voimaan

1.12.2020. Yleissopimuksen tarkoituksena on taata jokaiselle oikeus pyynnöstä saada tieto viranomaisen asiakirjasta ja se rakentuu nimenomaan julkisuusperiaatteelle. Sopimus sisältää määräykset oikeudesta saada tieto ja sen mahdollisista rajoituksista. Sopimuksen 3 artiklan 3 kohdassa jätetään tiedonsaantirajoituksille asetettavista määräajoista säätäminen kansalliseen harkintaan (ks. myös HE 116/2014, sivu 8). Näin ollen sopimus ei rajoita Suomen mahdollisuutta pidentää salassapitoaikaa 25 vuodesta 40 tai 60 vuoteen. Esitetty rajoitus ei siten ole ristiriidassa kansainvälisten ihmisoikeusvelvoitteiden kanssa.

Poikkeamiselle yleisestä 25 vuoden salassapitoajasta on hyväksyttävä ja painava yhteiskunnallinen intressi, ja se on rajoitettu välttämättömään. Poikkeus on siten oikeassa suhteessa rajoitukseen ja sen tavoitteeseen nähden. Asiakirjoista ei ole mahdollista laatia tyhjentävää listaa. Asiakirjat liittyisivät perinteisen ulkopolitiikan keskeiseen toimialueeseen. Lisäksi asiakirjat liittyisivät sisäministeriön tekemään suojelupoliisin ohjaukseen ja valvontaan sekä sotilastiedustelua koskeviin vastaaviin asiakirjoihin sekä kyseisten tiedusteluviranomaisten toimintaa koskeviin omiin asiakirjoihin. Täsmällinen ja tarkka rajaus toteutuu siinä, että kyse olisi julkisuuslain 24 §:n 1 momentin kohdista 1, 2, 9 ja 10, ja tahot, joiden asiakirjoja salassapitoajan pidennys koskisi, on nimetty ottaen huomioon säädetyt perusteet välttämättömyyden arvioinnille. Edelleen salassapito ei koskisi kaikkia kohtien 2 ja 9 asiakirjoja. Yleisestä salassapitoajasta poikkeaminen on kansallisen turvallisuuden (valtioturvallisuuden) ja valtion edun, Suomen Nato-jäsenyyteen ja nimettyjen tahojen kansainvälisen yhteistyön ja kansainvälisten suhteiden hoitamisen mukainen objektiivinen ja välttämätön peruste ottaen huomioon myös, että ulkopuolisella taholla ei ole subjektiivista oikeutta saada asiakirjoja. Kansallisessa turvallisuudessa on kyse koko suomalaisen yhteiskunnan yhteisestä turvallisuudesta ja Suomen suvereniteetista. Myös perinteisen ulkopolitiikan keskeisellä toimialueella pidempi salassapitoaika olisi rajoitettu välttämättömään eli sillä turvattaisiin ulkoasiainhallinnon, TP UTVA:n sekä tasavallan presidentin ja tasavallan presidentin kanslian ydintoimintaa kansainvälisissä suhteissa. Lisäksi TP UTVA tai ulkoministeriö voisivat edelleen, kuten nykyisinkin, ”päättää toisin” julkisuuslain 24 §:n 1 momentin 1 kohdan nojalla, eli ne voisivat päättää antaa salassa pidettävän asiakirjansa (kokonaan tai osajulkisena). Myös julkisuuslain 24 §:n 1 momentin 2 kohdan asiakirjojen osalta pidennys olisi rajattu vain asiakirjoihin, jotka koskevat Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön. Lisäksi pidennys on rajattu vain välttämättömään eli ulkoministeriöön, tasavallan presidenttiin ja tasavallan presidentin kansliaan ja salassapitoa rajaisi vahinkoedellytyslauseke. Ehdotettu sääntely muodostaisi rajoitetun ja hyväksyttävän poikkeuksen.

Yhteenveto

Ehdotettu sääntely sisältää täsmälliset säännökset. Perusoikeuksien rajoituksen olennainen sisältö ilmenee suoraan laista. Uudet toimivaltuudet edellyttävät tuomioistuimen päätöstä. Sääntely täyttää siten lailla säätämisen ja tarkkarajaisuuden vaatimukset. Suhteellisuusvaatimuksen kannalta olennaista on, että ehdotetun toimivaltuussääntelyn kohteena on poliisilain 5 a luvun 3 §:ssä ja tietoliikennetiedustelusta siviilitiedustelussa annetun lain 3 §.ssä mainittu toiminta. Lisäksi suojelupoliisin toimivallasta on jo aiemmin säädetty tarkkarajaisesti. Sääntelyn oikeasuhtaisuutta on arvioitava voimassa olevaa siviilitiedustelua koskevaa lainsäädäntöä sekä tiedustelutoiminnan valvonnasta annettua lakia vasten.

Tässä esityksessä ehdotettavan lainsäädännön arvioidaan täyttävän EIT:n ratkaisukäytännön ja perustuslakivaliokunnan tulkintakäytännön asettamat vaatimukset perus- ja ihmisoikeuksien huomioon ottamisesta.

Esitykseen sisältyvät lakiehdotukset voidaan hallituksen käsityksen mukaan käsitellä tavallisen lain säätämisjärjestyksessä.

Esitykseen liittyvät lakiehdotukset sisältävät uudentyyppistä sääntelyä. Tämän ja muiden valtiosääntöoikeudellisten näkökohtien vuoksi hallitus pitää tarkoituksenmukaisena, että eduskunta pyytää esityksestä perustuslakivaliokunnan lausunnon.

Ponsi

Edellä esitetyn perusteella annetaan eduskunnan hyväksyttäviksi seuraavat lakiehdotukset:

Lakiehdotukset

1.

Laki

poliisilain 5 a luvun muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan poliisilain (872/2011) 5 a luvun 2 §:n 2 ja 3 momentti, 6 §:n 1 momentti, 14 §:n 3 momentti, 16 -18 §, 25 §:n 5 momentti, 27 §:n 3 momentti, 39 §:n 1 ja 3 momentti, 41 §:n 1 ja 2 momentti, 46 §, 47 §:n 3 momentti, 51 §, 52 §, 55 §:n 3 momentti, 57 §:n 3 momentti, sellaisina kuin ne ovat laissa 581/2019, sekä

lisätään 4 §:ään uusi 6 momentti, jolloin nykyinen 6 momentti siirtyy 7 momentiksi, 14 a §, 14 b §, 18 a §, 18 b §, 27 a §, 28 a §, 39 a §, 39 b §, 41 a § ja 55 a § seuraavasti:

5 a luku

2 §

Tiedustelumenetelmät siviilitiedustelussa

— —

Tiedustelumenetelmiä ovat myös tässä luvussa tarkoitetut valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu, yksinomaan tietoverkossa toteutettava peitetoiminta, paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten.

Tässä luvussa säädetään siitä, millä edellytyksillä 1 momentissa tarkoitettuja tiedustelumenetelmiä sekä valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua, yksinomaan tietoverkossa toteutettavaa peitetoimintaa, paikkatiedustelua, jäljentämistä ja lähetyksen pysäyttämistä jäljentämistä varten käytetään siviilitiedustelussa.

— —

4 §

Tiedustelumenetelmien käytön edellytykset

— —

Valtiollisella toimijalla tarkoitetaan vieraan valtion tunnistettua viranomaista tai sellaiseen rinnastuvaa toimijaa sekä tarkoitetun tahon palveluksessa olevaa tai sen määräyksessä ja ohjauksessa toimivaa tahoa.

Tiedustelumenetelmien käytön järjestämisestä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

6 §

Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättäminen

Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta siviilitiedustelussa suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Jos telekuuntelua tai tietojen hankkimista telekuuntelun sijasta koskeva asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää telekuuntelusta tai tietojen hankkimisesta telekuuntelun sijasta 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 menetelmän käytön aloittamisesta.

— —

14 §

Teknisestä laitetarkkailusta siviilitiedustelussa päättäminen

— —

Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;

2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto taikka teknistä laitetta tai ohjelmistoa käyttävä henkilö;

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.

14 a §

Valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu

Valtiolliseen toimijaan kohdistuvalla tietojärjestelmätiedustelulla tarkoitetaan tiedonhankintaa valtiollisen tai siihen rinnastuvan tahon käyttämien tietojenkäsittelylaitteiden, tiedonsiirtolaitteiden ja tietoja käsittelevien ohjelmistojen muodostaman yhteen toimivan kokonaisuuden

siitä osasta, joka toteuttaa tai edesauttaa siviilitiedustelun kohteena olevaa toimintaa tai joka tallentaa tai välittää siviilitiedustelun kohteena olevaan toimintaan liittyviä tietoja.

Valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua saa käyttää vain siinä laajuudessa kuin on välttämätöntä tiedon hankkimiseksi tämän luvun 3 §:ssä tarkoitetusta toiminnasta.

14 b §

Valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta päättäminen

Tuomioistuin päättää valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta siviilitiedustelussa tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Tiedustelumenetelmän käytöstä päättämisestä erässä tilanteissa säädetään 39 §:ssä.

Lupa valtiolliseen toimijaan kohdistuvaan tietojärjestelmätiedusteluun voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua koskevassa vaatimuksessa ja päätöksessä on mainittava:

1) 3 §:ssä tarkoitettu toiminta;
2) toimenpiteen kohteena oleva valtiollinen tai siihen rinnastuva taho ja sen käyttämä tietojärjestelmä;
3) tosiseikat, joihin valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun edellytykset ja kohdistaminen perustuvat;
4) valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;
5) valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies;
6) mahdolliset valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun rajoitukset ja ehdot.

16 §

Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa

Suojelupoliisin palveluksessa olevalla virkamiehellä on oikeus siviilitiedustelussa sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan, tekniseen laitetarkkailuun ja valtiolliseen toimijaan kohdistuvaan tietojärjestelmätiedusteluun käytettävä laite, menetelmä tai ohjelmisto esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan tai 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 ja kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai

tietojärjestelmän suojaus tai haitata sitä. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.

Suojelupoliisin pyynnöstä viranomaisen ulkopuolisella henkilöllä on oikeus suojelupoliisin päällystöön kuuluvan poliisimiehen ohjeiden mukaisesti ja valvonnassa toteuttaa tiedustelumenetelmän käytön edellyttämä yksittäinen asennus- tai poistamistoimenpide.

Suojelupoliisilla on oikeus menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja tiedonsiirtämiseksi tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmää, jos se on välttämätöntä tiedustelumenetelmän käyttämiseksi. Suojelupoliisi ei saa aiheuttaa vähäistä suurempaa haittaa tai vahinkoa käytettävälle laitteelle tai tietojärjestelmälle.

17 §

Peitetoimintaa siviilitiedustelussa koskeva suunnitelma

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 siviilitiedustelussa päättäminen

Suojelupoliisin päällikkö päättää 17 §:ssä tarkoitetusta peitetoiminnasta.

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, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä;
6) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat;
7) peitetoiminnan tavoite ja toteuttamissuunnitelma;
8) päätöksen voimassaoloaika;
9) peitetoiminnan mahdolliset rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

18 a §

Yksinomaan tietoverkossa toteutettava peitetoiminta

Yksinomaan tietoverkossa toteutettavalla peitetoiminnalla siviilitiedustelussa tarkoitetaan luvun 3 §:ssä tarkoitettua toimintaa koskevaa tietoverkossa tapahtuvaa 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.

Yksinomaan tietoverkossa tehtävän peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava

18 b §

Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää yksinomaan tietoverkossa toteutettavasta peitetoiminnasta.

Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös 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) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat;
6) peitetoiminnan tavoite ja toteuttamissuunnitelma;
7) päätöksen voimassaoloaika;
8) peitetoiminnan mahdolliset rajoitukset ja ehdot.

Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.

25 §

Tietolähteen turvaaminen siviilitiedustelussa

— —

Suojelupoliisin päällikön päätöksellä suojelupoliisi voi antaa tietolähteelle yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja taikka avustaa maahantulon järjestämisessä rikoslain 17 luvun 8 §:n estämättä, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

27 §

Paikkatiedustelusta siviilitiedustelussa päättäminen

— —

Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta sekä kulkuneuvoon kohdistuvasta paikkatiedustelusta.

— —

27 a §

Näytteenotto paikkatiedustelussa

Suojelupoliisilla on oikeus paikkatiedustelussa ottaa aineesta, omaisuudesta tai esineestä näyte, jos se on tarpeen siviilitiedustelutehtävän suorittamiseksi.

28 a §

Aineen, omaisuuden tai esineen tilapäinen haltuunotto

Jos 27 a §:ssä tarkoitettu näytteenotto tai 28 §:ssä tarkoitettu jäljentäminen sitä välttämättä edellyttää, suojelupoliisilla on oikeus ottaa aine, omaisuus tai esine tilapäisesti haltuun. Aine, omaisuus tai esine on palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua.

Jollei omaisuutta, esinettä tai ainetta voida vaaratta palauttaa, suojelupoliisin päällystöön kuuluva poliisimies voi määrätä omaisuuden, esineen tai aineen hävitettäväksi. Hävittämisestä on tehtävä merkintä paikkatiedustelusta laadittavaan pöytäkirjaan tai tehtävä vastaava merkintä muuhun asiakirjaan.

39 §

Tiedustelumenetelmän käytöstä päättäminen eräissä tilanteissa

Muualla kuin Suomessa toteutettavasta siviilitiedustelusta päättää suojelupoliisin päällikkö. Tiedustelutoimintaan liittyvästä yksittäisen tiedustelumenetelmän käytöstä saa päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.

— —

Tämän luvun 44 ja 47 §:n säännöksiä ei sovelleta 1 momentissa tarkoitetussa siviilitiedustelussa ja tiedustelumenetelmien käytössä. Tämän lain 5 luvun 40 §:n 3 momentissa säädetty kielto pyytää tietoja hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä, ja 5 a luvun 4 §:n 4 momentin säännös voidaan yksittäistapauksessa jättää soveltamatta 1 momentissa tarkoitettuun siviilitiedusteluun ja tiedustelumenetelmän käyttöön, jos se on välttämätöntä kansallisen turvallisuuden suojaamiseksi.

39 a §

Tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi

Suojelupoliisilla on oikeus estää tietoteknisin menetelmin Suomen ulkopuolella olevan tietojärjestelmän käyttö sekä haitata tai muokata sen toimintaa, jos tietojärjestelmällä tai sen kautta voidaan aiheuttaa kansalliselle turvallisuudelle vakavaa vaaraa. Toimenpiteen käytön on oltava välttämätöntä vakavan vaaran torjumiseksi, eikä sillä saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi.

39 b §

Tietojärjestelmän käytön estämisestä tai sen toiminnan haittaamisesta vakavan vaaran torjumiseksi päättäminen

Suojelupoliisin päällikkö päättää tietojärjestelmän käytön estämisestä tai haittaamisesta. Päätös on tehtävä kirjallisesti.

Päätöksessä on mainittava:

1) toimenpiteen kohteena oleva tietojärjestelmä;

2) toimenpiteen perusteena olevaa vakavaa vaaraa ja toimenpiteen käytön edellytyksiä koskevat tosiseikat;

3) toimenpiteen tavoite ja toteuttamissuunnitelma;

4) toimenpiteen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;

5) mahdolliset toimenpiteen rajoitukset ja ehdot.

41 §

Kuuntelu- ja katselukiellot siviilitiedustelussa

Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua, teknistä laitetarkkailua ja valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua ei saa kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n tai 22 §:n 2 momentin nojalla.

Jos telekuuntelun, telekuuntelun sijasta toimitettavan tietojen hankkimisen, teknisen kuuntelun, teknisen katselun, teknisen laitetarkkailun tai valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun 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.

— —

41 a §

Telekuuntelun, televalvonnan, teknisen kuuntelun, teknisen laitetarkkailun ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun keskeyttäminen

Jos käy ilmi, että telekuuntelu tai televalvonta kohdistuu muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedonhankintakeinon käyttö on tältä osin keskeytettävä niin pian kuin mahdollista sekä tällaiset kuuntelulla saadut tallenteet ja televalvonnalla saadut tiedot sekä tällaisilla tiedonhankintakeinoilla saatuja tietoja koskevat muistiinpanot on heti hävitettävä.

Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee myös teknistä laitetarkkailua, jos käy ilmi, että tarkkailu kohdistuu sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta kuin laitetarkkailusta säädetään tässä luvussa, taikka että toimenpiteen kohteena oleva henkilö ei käytä tarkkailun kohteena olevaa laitetta. Jos käy ilmi, että tietojärjestelmätiedustelu kohdistuu sellaiseen tietojenkäsittelylaitteeseen, tiedonsiirtolaitteeseen tai tietoja käsittelevään ohjelmistoon, joka ei kuulu luvan kohteena olevaan tietojärjestelmään, on tietojärjestelmätiedustelu tältä osin keskeytettävä niin pian kuin mahdollista ja sillä saadut tallenteet ja tiedot sekä saatuja tietoja koskevat muistiinpanot on heti hävitettävä.

46 §

Kiiretilanteessa saadun tiedon hävittäminen

Jos suojelupoliisin päällystöön kuuluva poliisimies on 6 §:n 1 momentissa, 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 telekuuntelun, 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 ja 44 a §:n 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 ja 44 a §:n 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

— —

Jos tiedonhankinnan kohteen henkilöllisyys ja oleskelupaikka ei ole tiedossa 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden ja oleskelupaikan selvittyä.

— —

51 §

Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan velvollisuus avustaa siviilitiedustelussa

Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan on ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun, televalvonnan ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun edellyttämät kytkennät sekä annettava suojelupoliisin käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa telekuuntelu, televalvonta tai televerkkoon kohdistuva valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu toteutetaan suojelupoliisin toimesta teknisellä laitteella. Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan on lisäksi annettava suojelupoliisin päällystöön kuuluvan poliisimiehen käyttöön hallussaan olevat teknisen seurannan toimeenpanoa varten tarpeelliset tiedot.

Suojelupoliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua ja televerkkoon kohdistuvaa valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän tai tietoyhteiskunnan palvelun tarjoajan hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää suojelupoliisin päällystöön kuuluva poliisimies.

52 §

Korvaus viestinnän välittäjälle ja tietoyhteiskunnan palvelun tarjoajalle siviilitiedustelussa avustamisesta ja tietojen antamisesta

Viestinnän välittäjällä ja tietoyhteiskunnan palvelun tarjoajalla on oikeus saada valtion varoista korvaus 51 §:ssä tarkoitetusta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksesta säädetään sähköisen viestinnän palveluista annetun lain 299 §:ssä. Korvauksen maksamisesta päättää suojelupoliisi.

Päätökseen saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa (434/2003). Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Hallinto-oikeuden on varattava Liikenne- ja viestintävirastolle tilaisuus tulla kuulluksi.

55 §

Yhteistyö muiden viranomaisten, yritysten ja yhteisöjen kanssa

— —

Suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille salassapitosäännösten estämättä muita kuin henkilötietoja koskevia tietoja, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi.

— —

55 a §

Yhteistoiminta Rajavartiolaitoksen kanssa

Sen lisäksi, mitä luvun 55 §:ssä säädetään, Rajavartiolaitos voi tiedustelumenetelmien käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä suorittaa poliisilain 5 luvun 13 §:n 1 momentissa, poliisilain 5 a luvun 9, 11-16, 26 ja 28 §:ssä säädetyn yksittäisen toimenpiteen. Rajavartiolaitoksessa toimenpiteen suorittamisesta päättää pidättämiseen oikeutettu virkamies. Rajavartiolaitoksen on suojelupoliisin pyynnöstä ilman aiheetonta viivytystä keskeytettävä tässä momentissa tarkoitettu toimenpide.

Rajavartiolaitos voi tiedustelumenetelmien käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä suorittaa Rajavartiolaitokselle säädetyn tehtävän yhteydessä rajavartiolain (578/2005) 28 §:ssä tarkoitettuja toimenpiteitä, jotka ovat välttämättömiä siviilitiedustelutehtävän kannalta. Toimenpiteen kohteena oleva henkilö on velvollinen olemaan läsnä toimenpiteitä suoritettaessa enintään 12 tuntia kerrallaan. Rajavartiolaitoksessa toimenpiteen suorittamisesta päättää rajanylityspaikan esimies tai vähintään luutnantin arvoinen rajavartiomies.

Rajavartiolaitoksella on rajanylityspaikan esimiehenä toimivan rajavartiomiehen tai vähintään luutnantin arvoisen rajavartiomiehen päätöksellä oikeus käyttää vääriä, harhauttavia tai peiteltyjä tietoja silloin kun se on välttämätöntä toimenpiteen paljastumisen estämiseksi.

Rajavartiolaitoksen on luovutettava tässä pykälässä tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat käsittelemättöminä suojelupoliisille sekä hävitettävä toimenpiteen suorittamisessa syntyneet tallenteet ja asiakirjat, jollei tietojen käsittely ole tarpeen Rajavartiolaitokselle säädettyjen muiden tehtävien suorittamiseksi. Tallenteiden ja asiakirjojen tarkastamisesta sekä muista tiedonkäsittelyyn liittyvistä tehtävistä vastaa suojelupoliisi siten kuin tässä laissa säädetään.

57 §

Kansainvälinen yhteistyö

— —

Suojelupoliisin päällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja siihen liittyvästä tiedustelumenetelmien käytöstä. Ulkomaisella toimivaltaisella virkamiehellä on suojelupoliisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa osallistua Suomen alueella tiedustelumenetelmien käyttöön. -Ulkomainen virkamies on velvollinen noudattamaan suojelupoliisin hänelle antamia määräyksiä, rajoituksia ja ohjeita. Rikoslain 16 luvun 20 §:n 4 momentissa, 21 luvun 18 §:ssä ja 40 luvun 12 §:n 4 momentissa säädetään mainittujen lukujen säännösten soveltamisesta tiedustelumenetelmää Suomen alueella käyttävän tai Suomen alueella toimivan ulkomaisen virkamiehen tekemään tai häneen kohdistuneeseen rikokseen.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

2.

Laki

tietoliikennetiedustelusta siviilitiedustelussa annetun lain muuttaminen

Eduskunnan päätöksen mukaisesti
kumotaan tietoliikennetiedustelusta siviilitiedustelussa annetun lain (582/2019) 13 §,
muutetaan 4 §:n 2 momentti., 5 §, 7 §:n 3 momentti, 10 § ja 20 §, sekä
lisätään uusi 10 a § - 10 d § seuraavasti:

4 §

Tietoliikennetiedustelun käytön edellytykset

— —

Jos tietoliikennetiedustelun kohteena on valtiollinen toimija tai siihen rinnastuva taho, tietoliikennetiedustelun käytön tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

5 §

Tietoliikennetiedustelun kohdistaminen

Tietoliikennetiedustelu kohdistetaan tietoliikenteen automatisoidun erottelun avulla ja se voi kohdistua myös 10 a ja 10 c §:n perusteella tallennettuihin tietoihin. Automatisoitu erottelu perustuu 7 tai 9 §:n mukaisessa menettelyssä hyväksyttyjen hakuehtojen käyttöön.

7 §

Tietoliikennetiedustelua koskeva tuomioistuimen lupa

— —

Lupa tietoliikennetiedusteluun voidaan myöntää enintään kuudeksi kuukaudeksi kerrallaan ja se voi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.

— —

10 §

Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa

Puolustusvoimien tiedustelulaitos toteuttaa tietoliikennetiedustelun teknisesti suojelupoliisin puolesta keräämällä tämän lain 7, 9, 10 b ja 10 d §:ssä tarkoitettujen lupien tai päätösten mukaiset tiedot tietoliikenteessä.

Suojelupoliisin muuhun yhteistyöhön sotilastiedusteluviranomaisen kanssa sovelletaan poliisilain 5 a luvun 54 §:ää.

10 a §

Teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi

Suojelupoliisi voi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 66 §:ssä tarkoitettujen teknisten tietojen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaa 10 b §:ssä tarkoitetun tuomioistuimen luvan mukaisen teknisten tietojen keräämisen ja luovuttaa kyseiset tiedot suojelupoliisille.

Suojelupoliisilla on oikeus tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä:

1) tilastollista analyysia varten tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan; ja

2) tietoliikenteen reitittymisen ja muutosten seuraamiseksi.

Suojelupoliisi voi tallentaa puolustusvoimien tiedustelulaitoksen luovuttamat tekniset tiedot enintään 18 kuukauden ajaksi, minkä jälkeen ne on viimeistään hävitettävä. Tallennettuja tietoja voidaan käyttää 1 momentissa tarkoitettuun tarkoitukseen.

Suojelupoliisilla ja puolustusvoimien tiedustelulaitoksella on oikeus pyynnöstä tai oma-aloitteisesti luovuttaa tilastollisen analyysin tuloksia toisilleen siviili- ja sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi poliisilain 5 a luvun 54 §:ssä ja sotilastiedustelulain 17 §:ssä tarkoitetulla tavalla.

10 b §

Teknisten tietojen käsittelystä päättäminen viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi

Tuomioistuin päättää teknisten tietojen käsittelystä viestintäverkon osan tunnistamiseksi tai tietoliikenteen reitittymisen ja muutosten tunnistamiseksi tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Lupa voidaan antaa luvan antopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa voi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.

Vaatimuksessa ja päätöksessä on mainittava:

1) maantieteellinen alue tai verkkoalue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan, taikka kohde, jonka tietoliikenteen reitittymistä tai muutosta seurataan;

2) viestintäverkon osat, joista tietoa haetaan;

3) käsittelyä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt suojelupoliisin päällystöön kuuluva poliisimies; ja

4) suunnitelma käsittelyn toteuttamisesta.

10 c §

Tietoliikennetiedustelu hakuehtojen määrittämiseksi

Suojelupoliisi voi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 67 a §:n 1 momentissa tarkoitetun tietoliikenteen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaa 10 d §:ssä tarkoitetun tuomioistuimen luvan mukaisen tietoliikenteen keräämisen ja luovuttaa sen suojelupoliisille.

Suojelupoliisilla on oikeus tallentaa luovutettua tietoliikennettä ja käsitellä sitä, jos se on välttämätöntä kohdetta kuvaavien uusien hakuehtojen määrittämiseksi. Hakuehtojen määrittämisessä ei saa käsitellä viestin merkityssisällössä olevia tietoja. Hakuehtojen määrittämisessä voidaan käyttää 10 a §:ssä tarkoitettuja teknisiä tietoja.

Suojelupoliisi voi tallentaa puolustusvoimien tiedustelulaitoksen luovuttaman tietoliikenteen enintään 12 kuukauden ajaksi, minkä jälkeen ne on viimeistään hävitettävä

10 d §

Hakuehtojen määrittämisestä päättäminen

Tuomioistuin päättää hakuehtojen määrittämisestä tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.

Lupa voidaan antaa luvan antopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa voi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.

Vaatimuksessa ja päätöksessä on mainittava:

1) siviilitiedustelun kohde, jota varten hakuehtoja määritetään ja sitä koskevat tosiseikat;
2) kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään ja perustelut sille;
3) viestintäverkon osat, joista tietoa haetaan;
4) suunnitelma hakuehtojen määrittämisestä;
5) luvan voimassaoloaika kellonajan tarkkuudella;
6) hakuehtojen määrittämistä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt suojelupoliisin päällystöön kuuluva poliisimies;
7) mahdolliset hakuehtojen määrittämistä koskevat rajoitukset ja ehdot.

20 §

Tietoliikennetiedustelun käytöstä ilmoittaminen

Tietoliikennetiedustelusta ei ole velvollisuutta ilmoittaa.

Jos tietoliikennetiedustelussa kuitenkin on selvitetty sellainen tieto, josta on velvollisuus tai oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla, ilmoitetaan tietoliikennetiedustelusta 12 §:ssä tarkoitetulle taholle noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta.

Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei ole, jos todistamiskiellon tai todistamatta jättämisoikeuden alainen tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

3.

Laki

rajavartiolain muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan rajavartiolain (578/2005) 3 §:n 3 momentti, sellaisena kuin se on laissa 749/2014 sekä

lisätään uusi 25 b § seuraavasti:

3 §

Rajavartiolaitoksen tehtävät

— —

Rajavartiolaitos suorittaa poliisi- ja tullitehtäviä, etsintä-, pelastus- ja ensihoitotehtäviä sekä osallistuu sotilaalliseen maanpuolustukseen ja sotilastiedusteluun sekä siviilitiedusteluun. Rajavartiolaitoksen tehtävistä meripelastustoimen alalla säädetään meripelastuslaissa.

25 b §

Rajavartiolaitoksen osallistuminen siviilitiedusteluun

Rajavartiolaitos osallistuu suojelupoliisin pyynnöstä siviilitiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä suojelupoliisin tiedustelutehtävien tukemiseksi.

Rajavartiolaitoksen toimivaltuuksista siviilitiedusteluun osallistumisessa säädetään poliisilaissa (872/2011).

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

4.

Laki

henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain 32 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain (639/2019) 32 §:ään, sellaisena kuin se on laissa 430/2024, uusi 3 momentti seuraavasti:

32 §

— —

Rajavartiolaitos saa luovuttaa salassapitosäännösten estämättä 15 b §:ssä tarkoitettuja tietoja suojelupoliisille poliisilain 5 a luvussa (872/2011) säädettyjä tehtäviä varten.

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

5.

Laki

rikoslain 17 luvun 7 §:n 2 momentin muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan rikoslain (39/1889) 17 luvun 7 §:n 2 momentti, sellaisena kuin se osaksi laeissa 563/1998 ja 650/2004, seuraavasti

7 §

Valtionrajarikos

— —

Valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena tai joka on tehnyt 1 momentissa tarkoitetun teon poliisilain 5 a luvun 25 §:n 5 momentin perusteella.

———

Tämä laki tulee voimaan päivänä kuuta 20 .

———————

6.

Laki

viranomaisten toiminnan julkisuudesta annetun lain 31 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan viranomaisten toiminnan julkisuudesta annetun lain (612/1999) 31§:n 2 momentti, sellaisena kuin se on laissa 495/2005, seuraavasti*:*

31 §

Viranomaisen asiakirjan salassapidon lakkaaminen

— —

Viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty tai lain nojalla määrätty. Yksityiselämän suojaamiseksi 24 §:n 1 momentin 24–32 kohdassa salassa pidettäväksi säädetyn asiakirjan tai niitä vastaavan muussa laissa salassa pidettäväksi säädetyn tai muun lain nojalla salassa pidettäväksi määrätyn asiakirjan salassapitoaika on 50 vuotta sen henkilön kuolemasta, jota asiakirja koskee tai, jollei tästä ole tietoa, 100 vuotta. Salassa pidettäväksi 24 §:n 1 momentin 1 kohdassa säädetyn asiakirjan salassapitoaika on 40 vuotta. Salassa pidettäväksi 24 §:n 1 momentin 2 kohdassa säädetyn Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevan ulkoministeriön, tasavallan presidentin ja tasavallan presidentin kanslian asiakirjan salassapitoaika on 40 vuotta. Valtion turvallisuuden ylläpitämiseksi 24 §:n 1 momentin 9 kohdassa säädetyn suojelupoliisin ja sisäministeriön asiakirjan salassapitoaika on 60 vuotta. Salassa pidettäväksi 24 §:n 1 momentin 10 kohdassa säädetyn sotilastiedustelua koskevan asiakirjan salassapitoaika on 60 vuotta.

— —

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

Helsingissä x.x.20xx

Pääministeri

Etunimi Sukunimi

..ministeri Etunimi Sukunimi

Valitse kohde.
Valitse kohde.

Rinnakkaistekstit
1.

Laki

poliisilain 5 a luvun muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan poliisilain (872/2011) 5 a luvun 2 §:n 2 ja 3 momentti, 6 §:n 1 momentti, 14 §:n 3 momentti, 16 - 18 §, 25 §:n 5 momentti, 27 §:n 3 momentti, 39 §:n 1 ja 3 momentti, 41 §:n 1 ja 2 momentti, 46 §, 47§:n 3 momentti, 51 §, 52 §, 55 §:n 3 momentti, 57 §:n 3 momentti, sellaisina kuin ne ovat laissa 581/2019, sekä
lisätään 4 §:ään uusi 6 momentti, jolloin nykyinen 6 momentti siirtyy 7 momentiksi, 14 a §, 14 b §, 18 a §, 18 b §, 27 a §, 28 a §, 39 a §, 39 b §, 41 a § ja 55 a § seuraavasti:

Voimassa oleva laki	*Ehdotus*
5 a luku	**5 a luku**
Siviilitiedustelu	**Siviilitiedustelu**
2 §	2 §
Tiedustelumenetelmät siviilitiedustelussa	*Tiedustelumenetelmät siviilitiedustelussa*
Tiedustelumenetelmiä ovat telekuuntelu, tietojen hankkiminen telekuuntelun sijasta, televalvonta, tukiasematietojen hankkiminen, suunnitelmallinen tarkkailu, peitelty tiedonhankinta, tekninen kuuntelu, tekninen katselu, tekninen seuranta, tekninen laitetarkkailu, teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen, peitetoiminta, valeosto ja ohjattu tietolähdetoiminta.	— — — — — — — — — — — — — —
Tiedustelumenetelmiä ovat myös tässä luvussa tarkoitetut paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten.	Tiedustelumenetelmiä ovat myös tässä luvussa tarkoitetut *valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu, yksinomaan tietoverkossa toteutettava peitetoiminta*, paikkatiedustelu, jäljentäminen ja lähetyksen jäljentäminen sekä lähetyksen pysäyttäminen jäljentämistä varten.
Tässä luvussa säädetään siitä, millä edellytyksillä 1 momentissa tarkoitettuja tiedustelumenetelmiä sekä paikkatiedustelua,	

Voimassa oleva laki

jäljentämistä ja lähetyksen pysäyttämistä jäljentämistä varten käytetään siviilitiedustelussa.

Tietoliikennetiedustelusta tiedustelumenetelmänä siviilitiedustelussa säädetään tietoliikennetiedustelusta siviilitiedustelussa annetussa laissa (582/2019).]

4 §

Tiedustelumenetelmien käytön edellytykset

Tiedustelumenetelmän käytön yleisenä edellytyksenä siviilitiedustelussa on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

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 rinnastuvaan tahoon, tiedustelumenetelmän käytön tulee olla tarpeen tietojen saamiseksi sellaisesta siviilitiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Tiedustelumenetelmää ei saa kohdistaa pysyväisluonteiseen asumiseen käytettävään tilaan.

Tiedustelumenetelmän käyttö on lopetettava ennen päätöksessä mainitun määräajan päättymistä, jos käytön tarkoitus on saavutettu tai sen edellytyksiä ei enää ole.

(uusi 6 mom.)

Ehdotus

Tässä luvussa säädetään siitä, millä edellytyksillä 1 momentissa tarkoitettuja tiedustelumenetelmiä sekä *valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua, yksinomaan tietoverkossa toteutettavaa peitetoimintaa,* paikkatiedustelua, jäljentämistä ja lähetyksen pysäyttämistä jäljentämistä varten käytetään siviilitiedustelussa.

— — — — — — — — — — — — — —

4 §

Tiedustelumenetelmien käytön edellytykset

— — — — — — — — — — — — — —

Valtiollisella toimijalla tarkoitetaan vieraan valtion tunnistettua viranomaista tai sellaiseen rinnastuvaa toimijaa sekä tarkoitetun

Voimassa oleva laki	*Ehdotus*
Tiedustelumenetelmien käytön järjestämisestä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella. (*6 momentti siirtyy 7 momentiksi*)	*tahon palveluksessa olevaa tai sen määräyksessä ja ohjauksessa toimivaa tahoa.* Tiedustelumenetelmien käytön järjestämisestä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.
6 §	6 §
Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättäminen	*Telekuuntelusta ja muusta vastaavasta tietojen hankkimisesta siviilitiedustelussa päättäminen*
Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta siviilitiedustelussa suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.	Tuomioistuin päättää telekuuntelusta ja tietojen hankkimisesta telekuuntelun sijasta siviilitiedustelussa suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. *Jos telekuuntelua tai tietojen hankkimista telekuuntelun sijasta koskeva asia ei siedä viivytystä, suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies saa päättää telekuuntelusta tai tietojen hankkimisesta telekuuntelun sijasta 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 menetelmän käytön aloittamisesta.* — — — — — — — — — — — — — —
14 §	14 §
Teknisestä laitetarkkailusta siviilitiedustelussa päättäminen	*Teknisestä laitetarkkailusta siviilitiedustelussa päättäminen*
Tuomioistuin päättää teknisestä laitetarkkailusta siviilitiedustelussa 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	

Voimassa oleva laki	*Ehdotus*
saatettava tuomioistuimen ratkaistavaksi heti, kun se on mahdollista, kuitenkin viimeistään 24 tunnin kuluttua tiedonhankinta menetelmän 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.	Teknistä laitetarkkailua koskevassa vaatimuksessa ja päätöksessä on mainittava: 1) 3 §:ssä tarkoitettu toiminta; 2) toimenpiteen kohteena oleva tekninen laite tai ohjelmisto *taikka teknistä laitetta tai ohjelmistoa käyttävä henkilö;* 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.
	14 a §
	Valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu
(uusi)	*Valtiolliseen toimijaan kohdistuvalla tietojärjestelmätiedustelulla tarkoitetaan tiedonhankintaa valtiollisen tai siihen rinnastuvan tahon käyttämien tietojenkäsittelylaitteiden, tiedonsiirtolaitteiden ja tietoja käsittelevien ohjelmistojen muodostaman yhteen toimivan kokonaisuuden siitä osasta, joka toteuttaa tai edesauttaa siviilitiedustelun kohteena olevaa toimintaa tai joka tallentaa tai välittää siviilitiedustelun kohteena olevaan toimintaan liittyviä tietoja.* *Valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua saa käyttää vain siinä laajuudessa kuin on välttämätöntä tiedon hankkimiseksi tämän luvun 3 §:ssä tarkoitetusta toiminnasta.*

Voimassa oleva laki	*Ehdotus*
	14 b §
	Valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta päättäminen
(uusi)	*Tuomioistuin päättää valtiolliseen toimijaan kohdistuvasta tietojärjestelmätiedustelusta siviilitiedustelussa tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta. Tiedustelumenetelmän käytöstä päättämisestä erässä tilanteissa säädetään 39 §:ssä.* *Lupa valtiolliseen toimijaan kohdistuvaan tietojärjestelmätiedusteluun voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.* *Valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua koskevassa vaatimuksessa ja päätöksessä on mainittava:* *1) 3 §:ssä tarkoitettu toiminta;* *2) toimenpiteen kohteena oleva valtiollinen tai siihen rinnastuva taho ja sen käyttämä tietojärjestelmä;* *3) tosiseikat, joihin valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun edellytykset ja kohdistaminen perustuvat;* *4) valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua koskevan luvan voimassaoloaika kellonajan tarkkuudella;* *5) valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun suorittamista johtava ja valvova tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies;* *6) mahdolliset valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun rajoitukset ja ehdot.*

Voimassa oleva laki	*Ehdotus*
16 §	16 §
Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa	*Laitteen, menetelmän tai ohjelmiston asentaminen ja poisottaminen siviilitiedustelussa*
Suojelupoliisin palveluksessa olevalla virkamiehellä on oikeus siviilitiedustelussa 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 tai 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 ja kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.	Suojelupoliisin palveluksessa olevalla virkamiehellä on oikeus siviilitiedustelussa sijoittaa telekuunteluun, tietojen hankkimiseen telekuuntelun sijasta, televalvontaan, tekniseen kuunteluun, tekniseen katseluun, tekniseen seurantaan, tekniseen laitetarkkailuun *ja valtiolliseen toimijaan kohdistuvaan tietojärjestelmätiedusteluun* käytettävä laite, menetelmä tai ohjelmisto esineeseen, aineeseen, omaisuuteen, tilaan tai muuhun paikkaan tai 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 ja kiertää, purkaa tai muulla vastaavalla tavalla tilapäisesti ohittaa kohteen tai tietojärjestelmän suojaus tai haitata sitä. Laitteen, menetelmän tai ohjelmiston asentaminen tai sen poisottaminen ei saa tapahtua pysyväisluonteiseen asumiseen käytettävässä tilassa.
(uusi 2 momentti)	*Suojelupoliisin pyynnöstä viranomaisen ulkopuolisella henkilöllä on oikeus suojelupoliisin päällystöön kuuluvan poliisimiehen ohjeiden mukaisesti ja valvonnassa toteuttaa tiedustelumenetelmän käytön edellyttämä yksittäinen asennus- tai poistamistoimenpide.*
(uusi 3 momentti)	*Suojelupoliisilla on oikeus menetelmän tai ohjelmiston asentamiseksi tai poisottamiseksi ja tiedonsiirtämiseksi tilapäisesti käyttää yksityisen tai yhteisön laitetta tai tietojärjestelmää, jos se on välttämätöntä tiedustelumenetelmän käyttämiseksi. Suojelupoliisi ei saa aiheuttaa vähäistä suurempaa haittaa tai vahinkoa käytettävälle laitteelle tai tietojärjestelmälle.*

Voimassa oleva laki

17 §

Peitetoimintaa siviilitiedustelussa koskeva ***esitys ja*** *suunnitelma*

Peitetoimintaa koskevassa esityksessä on mainittava:
1) toimenpiteen esittäjä;
2) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöityinä;
3) 3 §:ssä tarkoitettu toiminta;
4) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat;
5) peitetoiminnan tavoite;
6) peitetoiminnan tarpeellisuus;
7) 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 siviilitiedustelussa päättäminen

Suojelupoliisin päällikkö päättää 17 §:ssä tarkoitetusta peitetoiminnasta. *Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta voi päättää myös 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;

Ehdotus

17 §

Peitetoimintaa siviilitiedustelussa koskeva ***suunnitelma***

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 siviilitiedustelussa päättäminen

Suojelupoliisin päällikkö päättää 17 §:ssä tarkoitetusta peitetoiminnasta.

(uusi 18 b § 1 mom.)

Peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.

Päätös peitetoiminnasta on tehtävä kirjallisesti. Päätöksessä on mainittava:
1) toimenpiteen esittäjä;

Voimassa oleva laki	*Ehdotus*
2)peitetoiminnan toteuttamisesta vastaava poliisimies; 3)tunnistetiedot peitetoiminnan suorittavista poliisimiehistä; 4)3 §:ssä tarkoitettu toiminta; 5) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä; 6)tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat; 7)peitetoiminnan tavoite ja toteuttamissuunnitelma; 8)päätöksen voimassaoloaika; 9)peitetoiminnan mahdolliset rajoitukset ja ehdot. Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava. *Peitetoiminnan lopettamisesta on tehtävä kirjallinen päätös*.	2) peitetoiminnan toteuttamisesta vastaava poliisimies; 3) tunnistetiedot peitetoiminnan suorittavista poliisimiehistä; 4) 3 §:ssä tarkoitettu toiminta; 5) tiedonhankinnan kohteena oleva henkilö tai, jos tiettyä henkilöä ei voida yksilöidä, henkilöryhmä riittävästi yksilöitynä; 6) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat; 7) peitetoiminnan tavoite ja toteuttamissuunnitelma; 8) päätöksen voimassaoloaika; 9) peitetoiminnan mahdolliset rajoitukset ja ehdot. Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.
	18 a §
	Yksinomaan tietoverkossa toteutettava peitetoiminta
(uusi)	*Yksinomaan tietoverkossa toteutettavalla peitetoiminnalla siviilitiedustelussa tarkoitetaan luvun 3 §:ssä tarkoitettua toimintaa koskevaa tietoverkossa tapahtuvaa 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.* *Yksinomaan tietoverkossa tehtävän peitetoiminnan toteuttamisesta on laadittava kirjallinen suunnitelma, jonka tulee sisältää päätöksenteon ja peitetoiminnan toteuttamisen kannalta oleelliset ja riittävän yksityiskohtaiset tiedot. Suunnitelmaa on olosuhteiden muuttuessa tarvittaessa tarkistettava*

Voimassa oleva laki	*Ehdotus*
	18 b §
	Yksinomaan tietoverkossa toteutettavasta peitetoiminnasta päättäminen
(uusi)	*Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää yksinomaan tietoverkossa toteutettavasta peitetoiminnasta.* *Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös voidaan antaa enintään kuudeksi kuukaudeksi kerrallaan.* *Yksinomaan tietoverkossa toteutettavaa peitetoimintaa koskeva päätös 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) tosiseikat, joihin peitetoiminnan edellytykset ja kohdistaminen perustuvat;* *6) peitetoiminnan tavoite ja toteuttamissuunnitelma;* *7) päätöksen voimassaoloaika;* *8) peitetoiminnan mahdolliset rajoitukset ja ehdot.* *Päätöstä on olosuhteiden muuttuessa tarvittaessa tarkistettava.*
25 §	25 §
Tietolähteen turvaaminen siviilitiedustelussa	*Tietolähteen turvaaminen siviilitiedustelussa*
Suojelupoliisi voi tietolähteen suostumuksella siviilitiedustelussa valvoa tämän asuntoa tai muuta tietolähteen asumiseen käyttämää tilaa ja sen välitöntä lähiympäristöä kameran tai muun paikkaan sijoitetun teknisen laitteen,	

Voimassa oleva laki *Ehdotus*

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 tarkoitetussa valvonnassa 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 tämän turvallisuuden varmistamiseksi. Kuuntelu ja katselu saadaan tallentaa. Tallenteet on hävitettävä heti sen jälkeen, kun niitä ei tarvita tietolähteen turvaamiseen.

— — — — — — — — — — — — — —

Suojelupoliisin päällikkö saa päättää, että tietolähteelle annetaan yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

Suojelupoliisin päällikön päätöksellä *suojelupoliisi voi antaa* tietolähteelle yksittäistapauksessa käytettäväksi vääriä, harhauttavia tai peiteltyjä tietoja tai rekisterimerkintöjä taikka tietolähteen käytettäväksi valmistettavia vääriä asiakirjoja *taikka avustaa maahantulon järjestämisessä rikoslain 17 luvun 8 §:n estämättä*, jos se on välttämätöntä tietolähteen hengen ja terveyden suojaamiseksi. Rekisterimerkintä on oikaistava sen jälkeen, kun tässä momentissa tarkoitettuja edellytyksiä ei enää ole.

Voimassa oleva laki	*Ehdotus*
27 §	27 §
Paikkatiedustelusta siviilitiedustelussa päättäminen	*Paikkatiedustelusta siviilitiedustelussa päättäminen*
Tuomioistuin päättää paikkatiedustelusta siviilitiedustelussa, jos se kohdistuu muuhun kotirauhan suojaamaan paikkaan kuin pysyväisluonteiseen asumiseen käytettävään paikkaan tai paikkaan, johon ei ole yleistä pääsyä tai johon yleinen pääsy 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 menetelmän käytön aloittamisesta.	
Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta.	Suojelupoliisin päällikkö tai tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies päättää muusta kuin 1 momentissa tarkoitetusta paikkatiedustelusta *sekä kulkuneuvoon kohdistuvasta paikkatiedustelusta.*
Lupa voidaan antaa ja päätös tehdä enintään kuukaudeksi kerrallaan.	
Paikkatiedustelua koskevassa vaatimuksessa ja 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.	

Voimassa oleva laki

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 tai 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.

Ehdotus

27 a §

Näytteenotto paikkatiedustelussa

(uusi)

Suojelupoliisilla on oikeus paikkatiedustelussa ottaa aineesta, omaisuudesta tai esineestä näyte, jos se on tarpeen siviilitiedustelutehtävän suorittamiseksi.

28 a §

Aineen, omaisuuden tai esineen tilapäinen haltuunotto

(uusi)

Jos 27 a §:ssä tarkoitettu näytteenotto tai 28 §:ssä tarkoitettu jäljentäminen sitä välttämättä edellyttää, suojelupoliisilla on oikeus ottaa aine, omaisuus tai esine tilapäisesti haltuun. Aine, omaisuus tai esine on palautettava viivytyksettä haltuunoton tarkoituksen toteuduttua.

Jollei omaisuutta, esinettä tai ainetta voida vaaratta palauttaa, suojelupoliisin päällystöön kuuluva poliisimies voi määrätä omaisuuden, esineen tai aineen hävitettäväksi. Hävittämisestä on tehtävä merkintä paikkatiedustelusta laadittavaan pöytäkirjaan tai tehtävä vastaava merkintä muuhun asiakirjaan.

Voimassa oleva laki	*Ehdotus*
39 §	39 §
Tiedustelumenetelmän käytöstä päättäminen eräissä tilanteissa	*Tiedustelumenetelmän käytöstä päättäminen eräissä tilanteissa*
Muualla kuin Suomessa toteutettavasta siviilitiedustelusta ja *tiedustelumenetelmän käytöstä p*äättää suojelupoliisin päällikkö.	Muualla kuin Suomessa toteutettavasta siviilitiedustelusta päättää suojelupoliisin päällikkö. *Tiedustelutoimintaan liittyvästä yksittäisen tiedustelumenetelmän käytöstä saa päättää myös tehtävään määrätty tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies.*
Tiedustelumenetelmän käyttöä koskevan esityksen, suunnitelman, vaatimuksen ja päätöksen sisältöön sovelletaan, mitä esityksestä, suunnitelmasta, vaatimuksesta ja päätöksestä tässä luvussa säädetään.	— — — — — — — — — — — — — — —
Tämän luvun 44 ja 47 §:n säännöksiä ei sovelleta 1 momentissa tarkoitetussa siviilitiedustelussa ja tiedustelumenetelmien käytössä. *Tämän luvun* 4 §:n 4 momentin säännös voidaan yksittäistapauksessa jättää soveltamatta 1 momentissa tarkoitettuun siviilitiedusteluun ja tiedustelumenetelmän käyttöön, jos se on välttämätöntä kansallisen turvallisuuden suojaamiseksi.	Tämän luvun 44 ja 47 §:n säännöksiä ei sovelleta 1 momentissa tarkoitetussa siviilitiedustelussa ja tiedustelumenetelmien käytössä. *Tämän lain 5 luvun 40 §:n 3 momentissa säädetty kielto pyytää tietoja hankittavaksi sellaisella tavalla, joka edellyttäisi viranomaiselle kuuluvien toimivaltuuksien käyttöä, ja 5 a luvun 4 §:n 4 momentin säännös* voidaan yksittäistapauksessa jättää soveltamatta 1 momentissa tarkoitettuun siviilitiedusteluun ja tiedustelumenetelmän käyttöön, jos se on välttämätöntä kansallisen turvallisuuden suojaamiseksi.
Suojelupoliisin virkamiehen osallistuminen tässä pykälässä tarkoitettuun ulkomailla tapahtuvaan siviilitiedusteluun edellyttää asianomaisen virkamiehen suostumusta.	— — — — — — — — — — — — — — —
	39 a §
	Tietojärjestelmän käytön estäminen tai sen toiminnan haittaaminen vakavan vaaran torjumiseksi
(uusi)	*Suojelupoliisilla on oikeus estää tietoteknisin menetelmin Suomen ulkopuolella olevan tietojärjestelmän käyttö sekä haitata tai muokata sen toimintaa, jos tietojärjestelmällä tai sen kautta voidaan aiheuttaa kansalliselle*

Voimassa oleva laki	*Ehdotus*
	turvallisuudelle vakavaa vaaraa. Toimenpiteen käytön on oltava välttämätöntä vakavan vaaran torjumiseksi, eikä sillä saa aiheuttaa suurempaa vahinkoa tai haittaa kuin on välttämätöntä tehtävän suorittamiseksi.
	39 b §
	Tietojärjestelmän käytön estämisestä tai sen toiminnan haittaamisesta vakavan vaaran torjumiseksi päättäminen
(uusi)	*Suojelupoliisin päällikkö päättää tietojärjestelmän käytön estämisestä tai haittaamisesta. Päätös on tehtävä kirjallisesti.* *Päätöksessä on mainittava:* *1) toimenpiteen kohteena oleva tietojärjestelmä;* *2) toimenpiteen perusteena olevaa vakavaa vaaraa ja toimenpiteen käytön edellytyksiä koskevat tosiseikat;* *3) toimenpiteen tavoite ja toteuttamissuunnitelma;* *4) toimenpiteen suorittamista johtava ja valvova suojelupoliisin päällystöön kuuluva poliisimies;* *5) mahdolliset toimenpiteen rajoitukset ja ehdot.*
41 §	41 §
Kuuntelu- ja katselukiellot siviilitiedustelussa	*Kuuntelu- ja katselukiellot siviilitiedustelussa*
Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua ja teknistä laitetarkkailua ei saa kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n tai 22 §:n 2 momentin nojalla.	Telekuuntelua, telekuuntelun sijasta toimitettavaa tietojen hankkimista, teknistä kuuntelua, teknistä katselua, teknistä laitetarkkailua ja *valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua* ei saa kohdistaa sellaiseen viestintään, josta viestinnän osapuoli ei saa todistaa tai josta hänellä on oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n tai 22 §:n 2 momentin nojalla.

Voimassa oleva laki

Jos telekuuntelun, telekuuntelun sijasta toimitettavan tietojen hankkimisen, teknisen kuuntelun, teknisen katselun tai teknisen laitetarkkailun 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, teknisestä katselusta tai teknisestä laitetarkkailusta.

Ehdotus

Jos telekuuntelun, telekuuntelun sijasta toimitettavan tietojen hankkimisen, teknisen kuuntelun, teknisen katselun, teknisen laitetarkkailun *tai valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun* 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.

— — — — — — — — — — — — — —

41 a §

(uusi)

Telekuuntelun, televalvonnan, teknisen kuuntelun, teknisen laitetarkkailun ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun keskeyttäminen

Jos käy ilmi, että telekuuntelu tai televalvonta kohdistuu muuhun kuin luvan kohteena olevalta henkilöltä lähtöisin olevaan tai hänelle tarkoitettuun viestiin taikka että teknisen kuuntelun kohteena oleva henkilö ei oleskele kuunneltavassa tilassa tai muussa paikassa, tiedonhankintakeinon käyttö on tältä osin keskeytettävä niin pian kuin mahdollista sekä tällaiset kuuntelulla saadut tallenteet ja televalvonnalla saadut tiedot sekä tällaisilla tiedonhankintakeinoilla saatuja tietoja koskevat muistiinpanot on heti hävitettävä.

Velvollisuus keskeyttämiseen sekä tallenteiden ja muistiinpanojen hävittämiseen koskee myös teknistä laitetarkkailua, jos käy ilmi, että tarkkailu kohdistuu sellaiseen luottamukselliseen viestiin, jota koskevasta telekuuntelusta, televalvonnasta ja muusta teknisestä tarkkailusta kuin laitetarkkailusta säädetään tässä luvussa, taikka että toimenpiteen kohteena oleva henkilö ei käytä tarkkailun kohteena

Voimassa oleva laki

Ehdotus

olevaa laitetta. Jos käy ilmi, että tietojärjestelmätiedustelu kohdistuu sellaiseen tietojenkäsittelylaitteeseen, tiedonsiirtolaitteeseen tai tietoja käsittelevään ohjelmistoon, joka ei kuulu luvan kohteena olevaan tietojärjestelmään, on tietojärjestelmätiedustelu tältä osin keskeytettävä niin pian kuin mahdollista ja sillä saadut tallenteet ja tiedot sekä saatuja tietoja koskevat muistiinpanot on heti hävitettävä.

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 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

46 §

Kiiretilanteessa saadun tiedon hävittäminen

Jos suojelupoliisin päällystöön kuuluva poliisimies on *6 §:n 1 momentissa*, 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 *telekuuntelun*, 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 *ja 44 a §:n 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

Voimassa oleva laki	*Ehdotus*
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.	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 *ja 44 a §:n 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 §	47 §
Tiedustelumenetelmän käytöstä ilmoittaminen	*Tiedustelumenetelmän käytöstä ilmoittaminen*
Telekuuntelusta, tietojen hankkimisesta telekuuntelun sijasta, televalvonnasta ja teknisen tarkkailun käytöstä ja viestiin kohdistuvasta jäljentämisestä tai viestiin kohdistuvasta lähetyksen jäljentämisestä siviilitiedustelussa 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	

Voimassa oleva laki

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 nojalla, 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 siviilitiedustelussa ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos asiassa ei ole aloitettu esitutkintaa 44 §:ssä tarkoitetun ilmoituksen perusteella. Jos esitutkinta aloitetaan, noudatetaan, mitä pakkokeinolain 10 luvun 60 §:n 2–7 momentissa säädetään. Silloin, kun käsitellään pakkokeinolain 10 luvun 60 §:n 3 momentissa tarkoitettua tiedustelumenetelmän käyttöä koskevan ilmoituksen lykkäämistä tai ilmoituksen tekemättä jättämistä, vaatimuksen tekee suojelupoliisin päällystöön kuuluva poliisimies. (23.3.2023/492)

Tiedustelumenetelmän käytöstä ei ole velvollisuutta ilmoittaa tiedonhankinnan kohteelle, jos kohteena on ollut valtiollinen toimija tai siihen rinnastuva taho.

Ilmoitusta koskevan asian käsittelyssä tuomioistuimessa noudatetaan mitä 35 §:ssä säädetään.

51 §

Teleyrityksen velvollisuus avustaa siviilitiedustelussa

Teleyrityksen velvollisuuteen avustaa siviilitiedustelussa sovelletaan, mitä 5 luvun 61

Ehdotus

— — — — — — — — — — — — — — —

Jos tiedonhankinnan kohteen henkilöllisyys *ja oleskelupaikka* ei ole tiedossa 1 tai 2 momentissa tarkoitetun määräajan tai lykkäyksen päättyessä, tiedustelumenetelmän käytöstä on ilmoitettava kirjallisesti hänelle ilman aiheetonta viivytystä henkilöllisyyden ja oleskelupaikan selvittyä.

— — — — — — — — — — — — — — —

51 §

Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan *velvollisuus avustaa siviilitiedustelussa*

Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan on ilman aiheetonta viivytystä tehtävä televerkkoon telekuuntelun,

Voimassa oleva laki	*Ehdotus*
§:ssä säädetään teleyrityksen avustamisvelvollisuudesta.	*televalvonnan ja valtiolliseen toimijaan kohdistuvan tietojärjestelmätiedustelun edellyttämät kytkennät sekä annettava suojelupoliisin käyttöön telekuuntelun toimeenpanoa varten tarpeelliset tiedot, välineet ja henkilöstö. Sama koskee myös niitä tilanteita, joissa telekuuntelu, televalvonta tai televerkkoon kohdistuva valtiolliseen toimijaan kohdistuva tietojärjestelmätiedustelu toteutetaan suojelupoliisin toimesta teknisellä laitteella. Viestinnän välittäjän ja tietoyhteiskunnan palvelun tarjoajan on lisäksi annettava suojelupoliisin päällystöön kuuluvan poliisimiehen käyttöön hallussaan olevat teknisen seurannan toimeenpanoa varten tarpeelliset tiedot.* *Suojelupoliisilla sekä toimenpiteen suorittajalla ja avustavalla henkilöstöllä on oikeus telekuuntelua ja televerkkoon kohdistuvaa valtiolliseen toimijaan kohdistuvaa tietojärjestelmätiedustelua varten tarpeellisen yhteyden kytkemiseksi päästä myös muihin kuin viestinnän välittäjän tai tietoyhteiskunnan palvelun tarjoajan hallinnassa oleviin tiloihin, ei kuitenkaan vakituiseen asumiseen käytettyihin tiloihin. Toimenpiteestä päättää suojelupoliisin päällystöön kuuluva poliisimies.*
52 §	52 §
*Korvaus **teleyritykselle** siviilitiedustelussa avustamisesta ja tietojen antamisesta*	*Korvaus **viestinnän välittäjälle ja tietoyhteiskunnan palvelun tarjoajalle** siviilitiedustelussa avustamisesta ja tietojen antamisesta*
Teleyrityksen oikeuteen saada korvausta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista sovelletaan, mitä 5 luvun 62 §:ssä säädetään.	Viestinnän välittäjällä ja tietoyhteiskunnan palvelun tarjoajalla on oikeus saada valtion varoista korvaus 51 §:ssä tarkoitetusta viranomaisten avustamisesta ja tietojen antamisesta aiheutuneista välittömistä kustannuksista. Korvauksesta säädetään sähköisen viestinnän palveluista annetun lain 299 §:ssä. Korvauksen maksamisesta päättää suojelupoliisi. Päätökseen saa vaatia oikaisua. Oikaisuvaatimuksesta säädetään hallintolaissa (434/2003) . Muutoksenhausta hallintotuomioistuimeen säädetään oikeudenkäynnistä hallintoasioissa annetussa laissa (808/2019).

Voimassa oleva laki | *Ehdotus*

Hallinto-oikeuden on varattava Liikenne- ja viestintävirastolle tilaisuus tulla kuulluksi.

55 §

Yhteistyö muiden viranomaisten, yritysten ja yhteisöjen kanssa

Suojelupoliisin on tarpeen mukaan toimittava yhteistyössä muiden viranomaisten kanssa siviilitiedustelun tarkoituksenmukaiseksi hoitamiseksi.

Suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi luovuttaa muille viranomaisille salassapitosäännösten estämättä muita kuin henkilötietoja koskevia tietoja, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi.

Suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille salassapitosäännösten estämättä muita kuin henkilötietoja koskevia tietoja, jos tietojen luovuttaminen on *välttämätöntä* kansallisen turvallisuuden suojaamiseksi.

Tietojen luovuttamisesta rikostorjuntaan säädetään 44 §:ssä.

Henkilötietojen käsittelystä säädetään henkilötietojen käsittelystä poliisitoimessa annetussa laissa.

Suojelupoliisin ja muiden viranomaisten välisen yhteistyön järjestämisestä voidaan antaa tarkempia säännöksiä valtioneuvoston asetuksella.

Sisäministeriön asetuksella voidaan antaa tarkempia säännöksiä suojelupoliisin ja muun sisäasiainhallinnon välisen yhteistyön järjestämisestä.

55 §

Yhteistyö muiden viranomaisten, yritysten ja yhteisöjen kanssa

— — — — — — — — — — — — — —

Suojelupoliisi voi siviilitiedustelutehtävänsä toteuttamiseksi luovuttaa yrityksille ja muille yhteisöille salassapitosäännösten estämättä muita kuin henkilötietoja koskevia tietoja, jos tietojen luovuttaminen on *tarpeen* kansallisen turvallisuuden suojaamiseksi.

— — — — — — — — — — — — — —

(uusi)

55 a §

Yhteistoiminta Rajavartiolaitoksen kanssa

Sen lisäksi, mitä luvun 55 §:ssä säädetään, Rajavartiolaitos voi tiedustelumenetelmien

Voimassa oleva laki *Ehdotus*

käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä suorittaa poliisilain 5 luvun 13 §:n 1 momentissa, poliisilain 5 a luvun 9, 11-16, 26 ja 28 §:ssä säädetyn yksittäisen toimenpiteen. Rajavartiolaitoksessa toimenpiteen suorittamisesta päättää pidättämiseen oikeutettu virkamies. Rajavartiolaitoksen on suojelupoliisin pyynnöstä ilman aiheetonta viivytystä keskeytettävä tässä momentissa tarkoitettu toimenpide.

Rajavartiolaitos voi tiedustelumenetelmien käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen pyynnöstä suorittaa Rajavartiolaitokselle säädetyn tehtävän yhteydessä rajavartiolain (578/2005) 28 §:ssä tarkoitettuja toimenpiteitä, jotka ovat välttämättömiä siviilitiedustelutehtävän kannalta. Toimenpiteen kohteena oleva henkilö on velvollinen olemaan läsnä toimenpiteitä suoritettaessa enintään 12 tuntia kerrallaan. Rajavartiolaitoksessa toimenpiteen suorittamisesta päättää rajanylityspaikan esimies tai vähintään luutnantin arvoinen rajavartiomies.

Rajavartiolaitoksella on rajanylityspaikan esimiehenä toimivan rajavartiomiehen tai vähintään luutnantin arvoisen rajavartiomiehen päätöksellä oikeus käyttää vääriä, harhauttavia tai peiteltyjä tietoja silloin kun se on välttämätöntä toimenpiteen paljastumisen estämiseksi.

Rajavartiolaitoksen on luovutettava tässä pykälässä tarkoitetulla toimenpiteellä saadut tallenteet ja asiakirjat käsittelemättöminä suojelupoliisille sekä hävitettävä toimenpiteen suorittamisessa syntyneet tallenteet ja asiakirjat, jollei tietojen käsittely ole tarpeen Rajavartiolaitokselle säädettyjen muiden tehtävien suorittamiseksi. Tallenteiden ja asiakirjojen tarkastamisesta sekä muista tiedonkäsittelyyn liittyvistä tehtävistä vastaa suojelupoliisi siten kuin tässä laissa säädetään.

Voimassa oleva laki	*Ehdotus*
57 §	57 §
Kansainvälinen yhteistyö	*Kansainvälinen yhteistyö*
Suojelupoliisi voi tehdä yhteistyötä sekä hankkia tietoja 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 tiedustelumenetelmien käytön rajoituksia ja ehtoja, jotka kyseinen valtio asettaa.	— — — — — — — — — — — — — — — —
Suojelupoliisin päällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja siihen liittyvästä 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 niitä tiedustelumenetelmiä, joiden käytöstä päättämisestä säädetään 9, 10, 18, 20 ja 24 §:ss*ä. Ulkomainen virkamies on velvollinen noudattamaan suojelupoliisin hänelle antamia määräyksiä, rajoituksia ja ohjeita. Rikoslain 16 luvun 20 §:n 4 momentissa, 21 luvun 18 §:ssä ja 40 luvun 12 §:n 4 momentissa säädetään mainittujen lukujen säännösten soveltamisesta tiedustelumenetelmää Suomen alueella käyttävän tai Suomen alueella toimivan ulkomaisen virkamiehen tekemään tai häneen kohdistuneeseen rikokseen.	Suojelupoliisin päällikkö päättää kansainväliseen yhteistyöhön osallistumisesta ja siihen liittyvästä tiedustelumenetelmien käytöstä. *Ulkomaisella* toimivaltaisella virkamiehellä on suojelupoliisin päällikön päätöksellä oikeus Suomen alueella kansallisen turvallisuuden suojaamiseksi toimia yhteistyössä suojelupoliisin kanssa ja suojelupoliisin poliisimiehen ohjauksessa ja valvonnassa *osallistua Suomen alueella tiedustelumenetelmien käyttöön.* Ulkomainen virkamies on velvollinen noudattamaan suojelupoliisin hänelle antamia määräyksiä, rajoituksia ja ohjeita. Rikoslain 16 luvun 20 §:n 4 momentissa, 21 luvun 18 §:ssä ja 40 luvun 12 §:n 4 momentissa säädetään mainittujen lukujen säännösten soveltamisesta tiedustelumenetelmää Suomen alueella käyttävän tai Suomen alueella toimivan ulkomaisen virkamiehen tekemään tai häneen kohdistuneeseen rikokseen.
Suojelupoliisi voi salassapitosäännösten estämättä luovuttaa muita kuin henkilötietoja kansainvälisessä yhteistyössä, jos tietojen luovuttaminen on tarpeen kansallisen turvallisuuden suojaamiseksi eikä tietojen luovuttaminen ole vastoin kansallista etua.	— — — — — — — — — — — — — — — —
Tietojen luovuttamisessa ja vastaanottamisessa on noudatettava Suomea velvoittavia kansainvälisiä sopimuksia. Kansainvälinen yhteistyö ja tietojen vaihto on kielletty, jos on perusteltua aihetta epäillä, että jotakin	

Voimassa oleva laki	*Ehdotus*
henkilöä tämän yhteistyön tai tietojen luovuttamisen vuoksi uhkaa kuolemanrangaistus, kidutus, muu ihmisarvoa loukkaava kohtelu, vaino, mielivaltainen vapaudenriisto tai epäoikeudenmukainen oikeudenkäynti. Henkilötietojen luovuttamisesta säädetään henkilötietojen käsittelystä poliisitoimessa annetussa laissa.	

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

_____

2.

Laki

tietoliikennetiedustelusta siviilitiedustelussa annetun lain muuttamisesta

Eduskunnan päätöksen mukaisesti
kumotaan tietoliikennetiedustelusta siviilitiedustelussa annetun lain (582/2019) 13 §, muutetaan 4 §:n 2 momentti, 5 §, 7 §:n 3 momentti, 10 § ja 20 §, sekä lisätään uusi 10 a § - 10 d § seuraavasti:

Voimassa oleva laki	*Ehdotus*
4 §	*4 §*
Tietoliikennetiedustelun käytön edellytykset	*Tietoliikennetiedustelun käytön edellytykset*

Voimassa oleva laki

Tietoliikennetiedustelun käytön yleisenä edellytyksenä on, että sen käyttäminen on välttämätöntä tärkeiden tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta, eikä tietoja ole hankittavissa muulla tiedustelumenetelmällä.

Jos tietoliikennetiedustelun *hakuehtojen käyttö* koskee ainoastaan valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, tietoliikennetiedustelun käytön tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Ehdotus

— — — — — — — — — — — — — —

Jos tietoliikennetiedustelun kohteena on valtiollinen toimija tai siihen rinnastuva taho, tietoliikennetiedustelun käytön tulee olla tarpeen tietojen saamiseksi sellaisesta tietoliikennetiedustelun kohteena olevasta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta.

Voimassa oleva laki

5 §

Tietoliikennetiedustelun kohdistaminen

Tietoliikennetiedustelu kohdistetaan 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.

Ehdotus

5 §

Tietoliikennetiedustelun kohdistaminen

Tietoliikennetiedustelu kohdistetaan tietoliikenteen automatisoidun erottelun avulla. Automatisoitu erottelu perustuu 7 tai 9 §:n mukaisessa menettelyssä hyväksyttyjen hakuehtojen käyttöön.

Voimassa oleva laki

7 §

Tietoliikennetiedustelua koskeva tuomioistuimen lupa

Ehdotus

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 ja tehokkuus perustuvat;

4) tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat sekä perustelut niille;

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.

— — — — — — — — — — — — — —

Lupa tietoliikennetiedusteluun voidaan myöntää enintään kuudeksi kuukaudeksi kerrallaan *ja se voi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.*

— — — — — — — — — — — — — —

10 §

Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa

Tietoliikennetiedustelun teknisenä toteuttajana toimii Puolustusvoimien tiedustelulaitos.

10 §

Tietoliikennetiedustelun tekninen toteuttaminen ja muu yhteistyö sotilastiedusteluviranomaisen kanssa

Puolustusvoimien tiedustelulaitos toteuttaa tietoliikennetiedustelun teknisesti

Voimassa oleva laki

Ehdotus

suojelupoliisin puolesta keräämällä tämän lain 7, 9, 10 b ja 10 d §:ssä tarkoitettujen lupien tai päätösten mukaiset tiedot tietoliikenteessä.

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 sekä toimittaa mainitun lain 66 §:n 2 momentissa tarkoitetun tilastollisen analyysin tuloksen suojelupoliisille sen jälkeen, kun se on saanut luvan teknisten tietojen käsittelyyn ja toteuttanut luvan mukaiset toimenpiteet.

Suojelupoliisi toimittaa 7 tai 9 §:ssä tarkoitetun päätöksen Puolustusvoimien tiedustelulaitokselle, joka suorittaa 5 §:n mukaiset toimenpiteet suojelupoliisin puolesta. Puolustusvoimien tiedustelulaitos toimittaa toimeksiannon toteuttamisella erottelemansa tietoliikenteen suojelupoliisille.

Suojelupoliisin muuhun yhteistyöhön sotilastiedusteluviranomaisen kanssa sovelletaan poliisilain 5 a luvun 54 §:ää.

Suojelupoliisin muuhun yhteistyöhön sotilastiedusteluviranomaisen kanssa sovelletaan poliisilain 5 a luvun 54 §:ää.

10 a §

Teknisten tietojen käsittely viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi

(uusi)

Suojelupoliisi voi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 66 §:ssä tarkoitettujen teknisten tietojen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaa 10 b §:ssä tarkoitetun tuomioistuimen luvan mukaisen teknisten tietojen keräämisen ja luovuttaa kyseiset tiedot suojelupoliisille.

Voimassa oleva laki	*Ehdotus*
	Suojelupoliisilla on oikeus tallentaa tietoliikenteen teknisiä tietoja ja automaattisen tietojenkäsittelyn avulla käsitellä niitä: *1) tilastollista analyysia varten tietoliikennetiedustelun kohdentamiseksi viestintäverkon osaan; ja* *2) tietoliikenteen reitittymisen ja muutosten seuraamiseksi.* *Suojelupoliisi voi tallentaa puolustusvoimien tiedustelulaitoksen luovuttamat tekniset tiedot enintään 18 kuukauden ajaksi, minkä jälkeen ne on viimeistään hävitettävä. Tallennettuja tietoja voidaan käyttää 1 momentissa tarkoitettuun tarkoitukseen.* *Suojelupoliisilla ja puolustusvoimien tiedustelulaitoksella on oikeus pyynnöstä tai oma-aloitteisesti luovuttaa tilastollisen analyysin tuloksia toisilleen siviili- ja sotilastiedustelun tarkoituksenmukaiseksi hoitamiseksi poliisilain 5 a luvun 54 §:ssä ja sotilastiedustelulain 17 §:ssä tarkoitetulla tavalla.*
	10 b §
	Teknisten tietojen käsittelystä päättäminen viestintäverkon osan sekä tietoliikenteen reitittymisen ja muutosten tunnistamiseksi
(uusi)	*Tuomioistuin päättää teknisten tietojen käsittelystä viestintäverkon osan tunnistamiseksi tai tietoliikenteen reitittymisen ja muutosten tunnistamiseksi tehtävään määrätyn tiedustelumenetelmien käyttöön perehtyneen suojelupoliisin päällystöön kuuluvan poliisimiehen vaatimuksesta.* *Lupa voidaan antaa luvan antopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa voi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.* *Vaatimuksessa ja päätöksessä on mainittava:* *1) maantieteellinen alue tai verkkoalue, jolta tulevaan tai jolle menevään tietoliikenteeseen teknisten tietojen käsittely kohdistetaan, taikka kohde, jonka tietoliikenteen reitittymistä tai muutosta seurataan;*

Voimassa oleva laki	*Ehdotus*
	2) viestintäverkon osat, joista tietoa haetaan; *3) käsittelyä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt suojelupoliisin päällystöön kuuluva poliisimies; ja* *4) suunnitelma käsittelyn toteuttamisesta.*
	10 c §
	Tietoliikennetiedustelu hakuehtojen määrittämiseksi
(uusi)	*Suojelupoliisi voi antaa toimeksiannon puolustusvoimien tiedustelulaitokselle sotilastiedustelulain 67 a §:n 1 momentissa tarkoitetun tietoliikenteen keräämiseksi. Puolustusvoimien tiedustelulaitos toteuttaa 10 d §:ssä tarkoitetun tuomioistuimen luvan mukaisen tietoliikenteen keräämisen ja luovuttaa sen suojelupoliisille.* *Suojelupoliisilla on oikeus tallentaa luovutettua tietoliikennettä ja käsitellä sitä, jos se on välttämätöntä kohdetta kuvaavien uusien hakuehtojen määrittämiseksi. Hakuehtojen määrittämisessä ei saa käsitellä viestin merkityssisällössä olevia tietoja. Hakuehtojen määrittämisessä voidaan käyttää 10 a §:ssä tarkoitettuja teknisiä tietoja.* *Suojelupoliisi voi tallentaa puolustusvoimien tiedustelulaitoksen luovuttaman tietoliikenteen enintään 12 kuukauden ajaksi, minkä jälkeen ne on viimeistään hävitettävä.*
	10 d §
	Hakuehtojen määrittämisestä päättäminen
(uusi)	*Tuomioistuin päättää hakuehtojen määrittämisestä tehtävään määrätyn tiedustelumenetelmien käyttöön erityisesti perehtyneen suojelupoliisin päällystöön kuuluvan virkamiehen vaatimuksesta.*

Voimassa oleva laki	*Ehdotus*
	Lupa voidaan antaa luvan antopäivästä alkaen enintään kuudeksi kuukaudeksi kerrallaan ja lupa voi koskea myös luvan antamista edeltänyttä määrättyä aikaa, joka voi olla kuutta kuukautta pidempi.
	Vaatimuksessa ja päätöksessä on mainittava:
	1) siviilitiedustelun kohde, jota varten hakuehtoja määritetään ja sitä koskevat tosiseikat;
(uusi)	*2) kohteen tietoliikenteen oletettu säännönmukaisuus tai ominaispiirre, jonka perusteella hakuehtoja määritetään ja perustelut sille;*
	3) viestintäverkon osat, joista tietoa haetaan;
	4) suunnitelma hakuehtojen määrittämisestä;
	5)luvan voimassaoloaika kellonajan tarkkuudella;
	6) hakuehtojen määrittämistä johtava ja valvova tiedustelumenetelmien käyttöön erityisesti perehtynyt suojelupoliisin päällystöön kuuluva poliisimies;
	7) mahdolliset hakuehtojen määrittämistä koskevat rajoitukset ja ehdot.
13 §	
Tallenteiden ja asiakirjojen tarkastaminen	*(kumotaan)*
Poliisilain 5 luvun 7 §:ssä tarkoitetun suojelupoliisin päällystöön kuuluvan poliisimiehen tai hänen määräämänsä virkamiehen on ilman aiheetonta viivytystä tarkastettava tietoliikennetiedustelun käytössä kertyneet tallenteet ja asiakirjat.	
20 §	*20 §*
Tietoliikennetiedustelun käytöstä ilmoittaminen	*Tietoliikennetiedustelun käytöstä ilmoittaminen*
Jos 6 §:ssä tarkoitetussa käsittelyssä on manuaalisesti selvitetty Suomessa tietoliikennetiedustelun käytön aikana olleen henkilön	*Tietoliikennetiedustelusta ei ole velvollisuutta ilmoittaa.*

Voimassa oleva laki

luottamuksellisen viestin tai tallentaman tiedon sisältö tai poliisilain 5 luvun 8 §:ssä tarkoitettu tunnistamistieto, ilmoitetaan hänelle tietoliikennetiedustelusta noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei kuitenkaan ole, jos tieto on hävitetty 9 §:n 2 momentin tai 15 §:n perusteella.

Ehdotus

Jos tietoliikennetiedustelussa kuitenkin on selvitetty sellainen tieto, josta on velvollisuus tai oikeus olla todistamatta oikeudenkäymiskaaren 17 luvun 13, 14, 16 tai 20 §:n taikka 22 §:n 2 momentin nojalla, ilmoitetaan tietoliikennetiedustelusta 12 §:ssä tarkoitetulle taholle noudattaen, mitä poliisilain 5 a luvun 47 §:ssä säädetään telekuuntelusta ilmoittamisesta. Velvollisuutta ilmoittaa tietoliikennetiedustelusta ei ole*, jos todistamiskiellon tai todistamatta jättämisoikeuden alainen tieto on hävitetty* 9 §:n 2 momentin tai 15 §:n perusteella.

Tämä laki tulee voimaan päivänä kuuta 20 . .

3.

Laki

rajavartiolain muuttamisesta

Eduskunnan päätöksen mukaisesti
muutetaan rajavartiolain (578/2005) 3 §:n 3 momentti, sellaisena kuin se on laissa 749/2014 sekä
lisätään uusi 25 b § seuraavasti:

Voimassa oleva laki	*Ehdotus*
3 §	3 §
Rajavartiolaitoksen tehtävät	*Rajavartiolaitoksen tehtävät*
Rajavartiolaitoksen tehtävänä on rajaturvallisuuden ylläpitäminen. Rajavartiolaitos toimii rajaturvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa. Rajavartiolaitos vastaa yhteistyöstä Euroopan raja- ja merivartioviraston kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä. (8.9.2017/619).	— — — — — — — — — — — — — —
Rajavartiolaitos suorittaa erikseen säädettyjä valvontatehtäviä sekä toimenpiteitä rikosten ennalta estämiseksi, paljastamiseksi, selvittämiseksi ja syyteharkintaan saattamiseksi yhteistyössä muiden viranomaisten kanssa.	
Rajavartiolaitos suorittaa poliisi- ja tullitehtäviä, etsintä-, pelastus- ja ensihoitotehtäviä sekä osallistuu sotilaalliseen maanpuolustukseen. Rajavartiolaitoksen tehtävistä meripelastustoimen alalla säädetään meripelastuslaissa.	Rajavartiolaitos suorittaa poliisi- ja tullitehtäviä, etsintä-, pelastus- ja ensihoitotehtäviä sekä osallistuu sotilaalliseen maanpuolustukseen ja sotilastiedusteluun *sekä siviilitiedusteluun*. Rajavartiolaitoksen tehtävistä meripelastustoimen alalla säädetään meripelastuslaissa.
	— — — — — — — — — — — — — —
	25 b §
	Rajavartiolaitoksen osallistuminen siviilitiedusteluun
(uusi)	

Voimassa oleva laki	*Ehdotus*
	Rajavartiolaitos osallistuu suojelupoliisin pyynnöstä siviilitiedusteluun hankkimalla tietoja ja tekemällä toimenpiteitä suojelupoliisin tiedustelutehtävien tukemiseksi. *Rajavartiolaitoksen toimivaltuuksista siviilitiedusteluun osallistumisessa säädetään poliisilaissa (872/2011).*

_____

Tämä laki tulee voimaan päivänä kuuta 20 .

4.

Laki

henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain 32 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

lisätään henkilötietojen käsittelystä Rajavartiolaitoksessa annetun lain (639/2019) 32 §:ään, sellaisena kuin se on laissa 430/2024, uusi 3 momentti seuraavasti:

Voimassa oleva laki	*Ehdotus*
32 §	32 §
Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle	*Henkilötietojen luovuttaminen toiselle rikosasioiden tietosuojalaissa tarkoitetulle toimivaltaiselle viranomaiselle*
— — — — — — — — — — — — — — — —	— — — — — — — — — — — — — — — —
(uusi)	Rajavartiolaitos saa luovuttaa salassapitosäännösten estämättä 15 b §:ssä tarkoitettuja tietoja suojelupoliisille poliisilain 5 a luvussa (872/2011) säädettyjä tehtäviä varten.]

Voimassa oleva laki

Ehdotus

Tämä laki tulee voimaan päivänä kuuta 20 . .

5.

Laki

rikoslain 17 luvun 7 §:n 2 momentin muuttamisesta

Eduskunnan päätöksen mukaisesti muutetaan rikoslain (39/1889) 17 luvun 7 §:n 2 momentti, sellaisena kuin se osaksi on laeissa 563/1998 ja 650/2004, seuraavasti:

Voimassa oleva laki

7 §

Valtionrajarikos

— — — — — — — — — — — — — — — —

Valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena.

Ehdotus

7 §

Valtionrajarikos

— — — — — — — — — — — — — — — —

Valtionrajarikoksesta ei tuomita ulkomaalaista, joka 1 momentissa tarkoitetun teon johdosta käännytetään tai karkotetaan maasta, eikä ulkomaalaista, joka pakolaisuuden perusteella hakee turvapaikkaa tai oleskelulupaa Suomessa. Valtionrajarikoksesta ei tuomita myöskään ulkomaalaista, joka on tehnyt 1 momentissa tarkoitetun teon sen vuoksi, että hän on ollut 25 luvun 3 tai 3 a §:ssä tarkoitetun ihmiskaupan kohteena *tai joka on tehnyt 1 momentissa tarkoitetun teon poliisilain 5 a luvun 25 §:n 5 momentin perusteella*.

]

Tämä laki tulee voimaan päivänä kuuta 20 . .

6.

Laki

viranomaisten toiminnan julkisuudesta annetun lain 31 §:n muuttamisesta

Eduskunnan päätöksen mukaisesti

muutetaan viranomaisten toiminnan julkisuudesta annetun lain (612/1999) 31§:n 2 momentti, sellaisena kuin se on laissa 495/2005, seuraavasti*:*

Voimassa oleva laki	*Ehdotus*
31 §	31 §
Viranomaisen asiakirjan salassapidon lakkaaminen	*Viranomaisen asiakirjan salassapidon lakkaaminen*
Viranomaisen asiakirjaa ei saa pitää salassa, kun salassapidolle laissa säädetty tai lain nojalla määrätty aika on kulunut tai kun asiakirjan salassa pidettäväksi määrännyt viranomainen on peruuttanut salassapitoa koskevan määräyksen.	— — — — — — — — — — — — — — — —
Viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty tai lain nojalla määrätty. Yksityiselämän suojaamiseksi 24 §:n 1 momentin 24–32 kohdassa salassa pidettäväksi säädetyn asiakirjan tai niitä vastaavan muussa laissa salassa pidettäväksi säädetyn tai muun lain nojalla salassa pidettäväksi määrätyn asiakirjan salassapitoaika on 50 vuotta sen henkilön kuolemasta, jota asiakirja koskee tai, jollei tästä ole tietoa, 100 vuotta.	Viranomaisen asiakirjan salassapitoaika on 25 vuotta, jollei toisin ole säädetty tai lain nojalla määrätty. Yksityiselämän suojaamiseksi 24 §:n 1 momentin 24–32 kohdassa salassa pidettäväksi säädetyn asiakirjan tai niitä vastaavan muussa laissa salassa pidettäväksi säädetyn tai muun lain nojalla salassa pidettäväksi määrätyn asiakirjan salassapitoaika on 50 vuotta sen henkilön kuolemasta, jota asiakirja koskee tai, jollei tästä ole tietoa, 100 vuotta. *Salassa pidettäväksi 24 §:n 1 momentin 1 kohdassa säädetyn asiakirjan salassapitoaika on 40 vuotta. Salassa pidettäväksi 24 §:n 1 momentin 2 kohdassa säädetyn Suomen suhteita toiseen valtioon tai kansainväliseen järjestöön koskevan ulkoministeriön, tasavallan presidentin ja tasavallan presidentin kanslian asiakirjan salassapitoaika on 40 vuotta. Valtion turvallisuuden ylläpitämiseksi*

Voimassa oleva laki

Asiakirja, joka sisältää kansainvälisistä tietoturvallisuusvelvoitteista annetun lain mukaan turvallisuusluokiteltua tietoa, tai tietoa sellaisesta kiinteistöstä, rakennuksesta, rakennelmasta, järjestelmästä, laitteesta tai menetelmästä, joka on käytössä 2 momentissa tarkoitetun 25 vuoden määräajan jälkeenkin, samoin kuin sellainen maanpuolustusta tai väestönsuojelua tai poikkeusoloihin varautumista varten laadittu suunnitelma ja arvio, jonka tietoja sisältyy voimassa olevaan vastaavaan suunnitelmaan, on kuitenkin pidettävä salassa 1 momentissa tarkoitetun ajan jälkeenkin, jos tiedon antaminen asiakirjasta aiheuttaisi edelleen tämän lain 24 §:n 1 momentin 2, 7 ja 8 tai 10 kohdassa tarkoitetun seurauksen. Tällaiset asiakirjat tulevat julkisiksi, kun kiinteistöä, rakennelmaa tai laitetta ei enää käytetä sellaiseen käyttötarkoitukseen, jonka johdosta asiakirjat ovat olleet salassa pidettäviä, taikka kun tiedot eivät enää sisälly voimassa olevaan suunnitelmaan taikka kun turvallisuusluokitus on kumottu.

Jos on ilmeistä, että asiakirjan tuleminen julkiseksi aiheuttaisi tässä pykälässä tarkoitetun määräajan päätyttyäkin merkittävää haittaa niille eduille, joiden suojaamiseksi salassapitovelvollisuus on säädetty, valtioneuvosto voi pidentää määräaikaa enintään 30 vuodella. Mitä edellä säädetään, ei kuitenkaan sovelleta 3 momentissa tarkoitettuihin asiakirjoihin.

Viranomaisen laatiman asiakirjan salassapitoaika lasketaan asiakirjaan merkitystä päivämäärästä tai, jollei asiakirjassa ole päivämäärää, sen valmistumisesta. Yksityisen viranomaiselle antaman asiakirjan salassapitoaika lasketaan päivästä, jona viranomainen on asiakirjan saanut.

Ehdotus

24 §:n 1 momentin 9 kohdassa säädetyn suojelupoliisin ja sisäministeriön asiakirjan salassapitoaika on 60 vuotta. Salassa pidettäväksi 24 §:n 1 momentin 10 kohdassa säädetyn sotilastiedustelua koskevan asiakirjan salassapitoaika on 60 vuotta.

— — — — — — — — — — — — — —

Tämä laki tulee voimaan päivänä kuuta 20 . .