Tampereen yliopisto

Katariina Tasala

LUPAVAATIMUS JA -PÄÄTÖS SIVIILITIEDUSTELUSSA SUORITETTAVASSA TIETOLIIKENNETIEDUSTELUSSA

Kansallinen lainsäädäntö Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa

Johtamisen ja talouden tiedekunta
Pro gradu –tutkielma
Maaliskuu 2020

TIIVISTELMÄ

Katariina Tasala: ”Lupavaatimus ja -päätös siviilitiedustelussa suoritettavassa tietoliikennetiedustelussa : Kansallinen lainsäädäntö Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa”
Pro gradu -tutkielma, V + 99 s.
Tampereen yliopisto
Hallintotieteiden tutkinto-ohjelma
Maaliskuu 2020

Tämän tutkimuksen aiheena on vuonna 2019 voimaan astuneen tietoliikennetiedustelulain ennakollinen lupamenettely keskittyen nimenomaisesti lupavaatimuksen ja -päätöksen sisältöön. Tutkimuksen pääasiallinen tutkimuskysymys on, miten lupavaatimuksella ja -päätöksellä voidaan varmistaa, että perus- ja ihmisoikeuksien rajoituksia sovelletaan niin kuin on tarkoitettu. Tutkimuskysymystä tarkasteltaessa kiinnitetään erityistä huomiota siihen, miten perus- ja ihmisoikeuksien rajoitusvaatimukset on huomioitu lupavaatimusta ja -päätöstä koskevassa lainsäädännössä ja miten rajoitusvaatimusten toteutuminen voidaan turvata. Tutkimuskysymystä tarkastellaan erityisesti Euroopan ihmisoikeustuomioistuimen oikeuskäytännön sekä niistä johtuvien rajoitusvaatimusten näkökulmasta.

Tutkimuksessa havaittiin, että Euroopan ihmisoikeussopimuksesta ja Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä johtuvat rajoitusvaatimukset on lupavaatimusta ja -päätöstä koskevassa lainsäädännössä ainakin sanatasolla huomioitu pitkälti hyvin. Lupavaatimuksen ja -päätöksen yksittäisiä osa-alueita tarkasteltaessa suurin osa kiinnittyy välttämättömyysvaatimukseen. Välttämättömyysvaatimuksen ollessa myös tietoliikennetiedustelun yleinen edellytys, on sen varmistaminen nähtävä tutkimuksen perusteella erityisesti sellaiseksi tekijäksi, johon tulee kiinnittää huomiota.

Tutkiessaan salaiseen tiedonhankintaan ja tiedusteluun liittyviä tapauksia Euroopan ihmisoikeustuomioistuin on pitänyt tuomioistuinkontrollia hyvänä oikeussuojakeinona. On kuitenkin tärkeää, että tuomioistuinkontrolli on todellista. Lupapäätöksellä tuomioistuin luo raamit kullekin yksittäiselle tiedustelutehtävälle, ja se määrittää, millä ehdoilla suojelupoliisi saa toteuttaa tietoliikennetiedustelua. Lupavaatimusta laatiessaan suojelupoliisilla on vastuu antaa tuomioistuimelle sellaiset tiedot, joiden varassa tuomioistuin pystyy tosiasiallisesti testaamaan rajoitusvaatimusten toteutumisen ja vastaavasti tuomioistuimella on velvollisuus varmistaa, että tietoliikennetiedustelun toteutumiselle on olemassa edellytykset. Tällaisten tosiasioiden esittämistä on vaadittu laissa, mutta esimerkiksi pakkokeinoasioista päätettäessä on tämänkaltaisen tuomioistuinmenettelyn nähty jäävän osittain puutteelliseksi lain asettamista vaatimuksista huolimatta.

Ratkaisevaksi tekijäksi jääkin siis se, millaiseksi tietoliikennetiedustelussa vaadittava lupavaatimus ja -päätös käytännössä muodostuu. Tietoliikennetiedustelu on tiedustelujärjestelmänä täysin uusi ja siksi on tärkeää seurata sen toimimista käytännössä, tunnistaa sen heikkoudet ja kehittää järjestelmää ja lainsäädäntöä niiden pohjalta. Järjestelmän heikkouksien tunnistaminen ja jatkuva kehittäminen on Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä nähty hyväksi asiaksi, ja siihen on kiinnitetty huomiota myös kansallisella tasolla.

Avainsanat: tietoliikennetiedustelu, siviilitiedustelu, Euroopan ihmisoikeustuomioistuin, ennakollinen lupamenettely, Euroopan ihmisoikeussopimus

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck –ohjelmalla.

Sisällysluettelo

LÄHTEET ..... **I**

OIKEUSTAPAUSLUETTELO ..... **V**

1. JOHDANTO **1**
1.1. TUTKIMUKSEN AIHEPIIRI JA TUTKIMUKSEN KULKU 1
1.1.1. Tutkimuksen aihe ja tausta *1*
1.1.2. Lyhyesti siviilitiedustelusta *3*
1.1.3. Tutkimuksen kulku *6*
1.2. TUTKIMUSKYSYMYS JA AIEMPI TUTKIMUS 8
1.3. METODISET VALINNAT JA LÄHDEAINEISTO 12

2. TIETOLIIKENNETIEDUSTELU **16**
2.1. TIETOLIIKENNETIEDUSTELUN KÄSITE JA TOTEUTUS 16
2.2. TIEDUSTELUTOIMINNAN VALVONTA 22
2.2.1. Tiedusteluvalvontavaltuutettu *22*
2.2.2. Tiedusteluvalvontavaliokunta *25*
2.2.3. Suojelupoliisin sisäinen valvonta *27*

3. YKSITYISELÄMÄN JA LUOTTAMUKSELLISEN VIESTIN SALAISUUDEN SUOJA **30**
3.1. YKSITYISELÄMÄN SUOJA JA SEN RAJOITTAMINEN 30
3.1.1. Yksityiselämän suojan ulottuvuus *30*
3.1.2. Yksityiselämän suojan rajoittaminen *34*
3.2. LUOTTAMUKSELLISEN VIESTIN SALAISUUDEN SUOJAN RAJOITTAMINEN 37
3.2.1. Rajoituksen lakiperusta *37*
3.2.2. Välttämättömyys ja vakava uhka kansalliselle turvallisuudelle *39*

4. ENNAKOLLINEN LUPAMENETTELY **43**
4.1. TUOMIOISTUIMEN JA SUOJELUPOLIISIN ROOLI ENNAKOLLISESSA LUPAMENETTELYSSÄ 43
4.2. TUOMIOISTUIMEN KOKOONPANO 49
4.3. KIIREMENETTELY 53

5. LUPAVAATIMUS JA –PÄÄTÖS ENNAKOLLISESSA LUPAMENETTELYSSÄ **57**
5.1. LUPAVAATIMUS JA -PÄÄTÖS 57
5.2. LUVAN VOIMASSAOLO 62
5.3. TIETOLIIKENNETIEDUSTELUN KOHDE 65
5.4. TIETOLIIKENNETIEDUSTELUN KÄYTÖN YLEISET EDELLYTYKSET JA TEHOKKUUS 73
5.5. HAKUEHDOT JA HAKUEHTOJEN LUOKKA 79
5.6. VIESTINTÄVERKON OSAN YKSILÖINTI 86

6. JOHTOPÄÄTÖKSET **91**

Lähteet

Virallislähteet

Eduskunnan työjärjestys 40/2000

Laki poliisin hallinnosta 110/1992

Laki Suomen perustuslain 10 §:n muuttamisesta 817/2018

Laki tiedustelutoiminnan valvonnasta 121/2019

Laki sotilastiedustelusta 590/2019

Laki tietoliikennetiedustelusta siviilitiedustelussa 582/2019

Perustuslaki 731/1999

Poliisilaki 872/2011

Euroopan ihmisoikeussopimus SopS 63/1999

Euroopan unionin perusoikeuskirja EUVL C 326, 26.10.2012, s. 391-407

Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus SopS 8/1976

HE 198/2017 vp. Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.

HE 199/2017 vp. Hallituksen esitys eduskunnalle laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta.

HE 202/2017 vp. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi (Siviilitiedustelulaki).

HE 203/2017 vp. Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi (Sotilastiedustelulaki).

PNE 1/2018 vp. Puhemiesneuvoston ehdotus eduskunnan työjärjestyksen ja eduskunnan virkamiehistä annetun lain 9 §:n muuttamisesta.

PeVL 35/2018 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

PeVL 75/2018 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

LaVL 27/2018 vp. Lakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta.

PeVM 4/2018 vp. Perustuslakivaliokunnan mietintö hallituksen esityksestä eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta.

PeVM 25/1994 vp. Perustuslakivaliokunnan mietintö hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta.

PeVM 9/2018 vp. Perustuslakivaliokunnan mietintö puhemiesneuvoston ehdotuksesta eduskunnan työjärjestyksen ja eduskunnan virkamiehistä annetun lain 9 §:n muuttamisesta.

PeVM 10/2018 vp. Perustuslakivaliokunnan mietintö hallituksen esityksestä eduskunnalle laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta

HaVM 30/2018 vp. Hallintovaliokunnan mietintö hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

EV 291/2018 vp Eduskunnan vastaus. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi.

SMDno-2016-329. Sisäministeriön ja sen hallinnonalan laillisuusvalvontaohje 20.06.2016

Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö. Puolustusministeriö 2015.

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportti. Sisäministeriön julkaisu 28/2014.

Fredman, Markku: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 19.10.2018 (Fredman 2018)

Laitinen, Katriina: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 17.10.2019. (Laitinen 2018)

Melander, Sakari: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 18.10.2018. (Melander 2018)

Ojanen, Tuomas: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 20.02.2019. (Ojanen 2019)

Scheinin, Martin: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 20.02.2019. (Scheinin 2019)

Vainio, Niklas: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 24.10.2018. (Vainio 2018)

Viljanen, Jukka: Asiantuntijalausunto perustuslakivaliokunnalle hallituksen esityksestä eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. 25.10.2018. (Viljanen J. 2018)

Kirjallisuus ja artikkelit

Aarnio, Aulis: Tulkinnan taito. Ajatuksia oikeudesta, oikeustieteestä ja yhteiskunnasta. Vantaa 2006.

Aarnio, Aulis: Luentoja lainopillisen tutkimuksen teoriasta. Helsinki 2011.

de Godzinsky, Virve-Maria - Niemi, Johanna: Telepakkokeinojen oikeussuojajärjestelmä. Oikeuspoliittisen tutkimuslaitoksen tutkimuksia 243. Helsinki 2009.

Fredman, Markku: Pakkokeinoasiat Helsingin käräjäoikeudessa. Defensor Legis 3/2017, s. 353-367.

Hirvelä, Päivi - Heikkilä, Satu: Ihmisoikeudet. Käsikirja EIT:n oikeuskäytäntöön. 2., uudistettu painos. Helsinki 2017.

Hirvonen, Ari: Mitkä metodit? Opas oikeustieteen metodologiaan. Helsinki 2011.

Husa, Jarkko - Mutanen, Anu - Pohjolainen, Teuvo; Kirjoitetaan Juridiikkaa: Ohjeita oikeustieteellisten kirjallisten töiden laatijoille. 2., uud.p. Helsinki 2008.

Lohse, Mikael - Viitanen, Marko: Johdatus tiedusteluun. Helsinki 2019.

Neuvonen, Riku: Yksityisyyden suoja Suomessa. Helsinki 2014.

Pellonpää, Matti - Gullans, Monica - Pölönen, Pasi - Tapanila, Antti: Euroopan ihmisoikeussopimus. 6., uudistettu painos. Helsinki 2018.

Porvali, Mikko: Tiedustelun näkymätön historia. Antiikista maailmansotiin. Atena Kustannus Oy, Jyväskylä, 2018.

Tuori, Kaarlo: Kriittinen oikeuspositivismi. Helsinki 2000.

Viljanen, Veli-Pekka: Perusoikeuksien rajoitusedellytykset. Helsinki, 2001. (Viljanen V-P 2001)

Viljanen, Veli-Pekka: Perusoikeuksien rajoittaminen. Teoksessa Hallberg, Pekka - Karapuu, Heikki - Ojanen, Tuomas - Scheinin, Martin - Tuori, Kaarlo - Viljanen, Veli-Pekka: Perusoikeudet. Jatkuva verkkojulkaisu (Viljanen V-P I)

Viljanen, Veli-Pekka: Yksityiselämän suoja. Teoksessa Hallberg, Pekka - Karapuu, Heikki - Ojanen, Tuomas - Scheinin, Martin - Tuori, Kaarlo - Viljanen, Veli-Pekka: Perusoikeudet. Jatkuva verkkojulkaisu. (Viljanen V-P II)

Eduskunnan oikeusasiamiehen toimintakertomus 2015.

Eduskunnan oikeusasiamiehen toimintakertomus 2016.

Eduskunnan oikeusasiamiehen toimintakertomus 2017.

Eduskunnan oikeusasiamiehen toimintakertomus 2018.

Pro gradu -tutkielmat

Havulinna, Mika: Kansallinen turvallisuus vs. perusoikeudet: Lainsäädäntötutkimus tiedustelulakihankkeesta. Turku 2018.

Kuhanen, Katariina: Kansallinen turvallisuus rajoitusperusteena yksityiselämän suojaan Euroopan ihmisoikeustuomioistuimen ratkaisukäytännössä – Erityishuomiona salaisen tiedonhankinnan valvonnalle asetetut vaatimukset. Helsinki 2019.

Pekola, Sami: Tiedustelu oikeusvaltiossa: tiedustelutoimivaltuuksien laajentaminen tiedustelun valvonnan näkökulmasta. Rovaniemi 2018.

Pietiläinen, Tanja: Yksityiselämän suoja tietoliikennetiedustelussa. Helsinki 2018.

Tokoi, Petra: Yksityiselämän suoja perusoikeutena ja tietoliikennetiedustelun toteuttaminen kansallisessa lainsäädännössä. Helsinki 2016.

Internetlähteet

”Tiedustelulakikokonaisuus eteni eduskunnan käsiteltäväksi”. Uutinen 5/2018. https://intermin.fi/artikkeli/-/asset_publisher/10616/tiedustelulakikokonaisuus-eteni-eduskunnan-kasiteltavaksi Viitattu 3.12.2018

Suojelupoliisin verkkosivut: Suojelupoliisin alkuvaiheet: https://www.supo.fi/historia/alkuvaiheet Viitattu 24.1.2019.

Suojelupoliisin verkkosivut: Suojelupoliisin tehtävien laajentuminen: https://www.supo.fi/historia/tehtavien_laajentuminen Viitattu 24.1.2019

Valtioneuvoston yleisistunto 17.4.2019: Tiedusteluvalvontavaltuutetun nimittäminen. https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f8062504a Viitattu 15.5.2019.

YLEn uutinen 14.2.2019: ”Tiedustelulait lähetetään takaisin valiokuntien käsittelyyn – Risikko: ”Emme jätä mitään kiviä kääntämättä” https://yle.fi/uutiset/3-10646032 Viitattu 23.2.2020

Sisäministeriön internetsivut: Ministeriö: Laillisuusvalvonta. https://intermin.fi/ministerio/laillisuusvalvonta Viitattu 14.3.2020.

Centrum för Rättvisa v. Sweden: The Applicant’s Further Written Observations on Admissibility and Merits.
Saatavilla https://centrumforrattvisa.se/fra-lagen-provas-av-europadomstolen/ : “Läs Centrum för rättvisas yttrande till Europadomstolen den 3 maj 2019.” Viitattu 15.3.2020.

Oikeustapausluettelo

Euroopan ihmisoikeustuomioistuin

Suuren jaoston tuomiot merkitty lyhenteellä SJ

Amann v. Switzerland (Application no. 27798/95) 16.2.2000. **(SJ)**

Big Brother Watch and Others v. The United Kingdom (Applications nos. 58170/13, 62322/14 and 24960/15) 13.9.2018.

Centrum för Rättvisa v. Sweden (Application no. 35252/08) 19.7.2018.

Giacomelli v. Italy (Application no. 59909/00) 2.11.2006.

Gillow v. The United Kingdom (Application no. 9063/80) 24.11.1986.

Handyside v. The United Kingdom (Application no. 5493/72) 7.12.1976.

Huvig v. France (Application no. 11105/84) 24.4.1990.

Kennedy v. The United Kingdom (Application no. 26839/05) 18.5.2010.

Klass and Others v. Germany (Application no. 5029/71) 6.9.1978.

Liberty and Others v. The United Kingdom (Application no. 58243/00) 1.7.2008.

Malone vs. The United Kingdom (Application no. 8691/79) 2.8.1984.

Mustafa Sezgin Tanrıkulu v. Turkey (Application no. 27473/06), 18.7.2017.

Roman Zakharov v. Russia (Application no. 47143/06) 4.12.2015. **(SJ)**

Szabó and Vissy v. Hungary (Application no. 37138/14) 12.1.2016.

The Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (Application no. 62540/00) 28.6.2007.

Van der Heijden v. the Netherlands (Application no. 42857/05) 3.4.2012. **(SJ)**

Weber and Saravia v. Germany (Application no. 54934/00) 29.6.2006.

Euroopan unionin tuomioistuin

Åkerberg Fransson (C-617/10) 23.2.2013.

1. Johdanto

1.1. Tutkimuksen aihepiiri ja tutkimuksen kulku

1.1.1. Tutkimuksen aihe ja tausta

Suomen turvallisuusympäristö on ollut viime vuosina muutoksessa. Sisäistä ja ulkoista turvallisuutta uhkaavia tekijöitä on vaikea erottaa toisistaan, ja muutoksia ovat tuoneet lisäksi viestintäteknologian ja tietotekniikan kehitys. Kehitys helpottaa uhkaa aiheuttavien tekijöiden kommunikointia valtionrajojen yli ja haitallisten tekojen toteuttaminen entistä nopeammin on helpottunut. Kansallista turvallisuutta uhkaavat tahot ovat nykypäivänä useimmiten kansainvälisiä tai niillä on yhteyksiä Suomen ulkopuolisiin tekijöihin. Turvallisuusympäristön muutokset sekä lainsäädännön puutteellisuus reagoida tähän loivat tarpeen kehittää uutta lainsäädäntöä, jonka tarkoituksena oli parantaa turvallisuusviranomaisten tiedonhankintaa.[1]

Joulukuussa 2013 puolustusministeriön asettama tiedonhankintalakityöryhmä ryhtyi kehittämään turvallisuusviranomaisten, erityisesti puolustusvoimien ja suojelupoliisin, tiedonhankintakykyä parantavaa lainsäädäntöä. Työryhmän tehtävänä oli kehittää lainsäädäntöä koskien eritoten tietoverkossa esiintyviä uhkia ja niiden torjuntaa. Vuoden 2015 alussa työryhmä luovutti puolustusministeriölle mietinnön ”Suomalaisen tiedustelulainsäädännön suuntaviivoja”. Mietinnössä sen aikainen tilanne nähtiin epätyydyttävänä ottaen huomioon kansainvälisessä turvallisuusympäristössä tapahtuneet muutokset. Tarkasteltaessa turvallisuusviranomaisten tiedonhankintatoimivaltuuksia suhteessa toiminnan yhteiskunnalliseen merkittävyyteen tai vertailussa muihin valtioihin, olivat ne mietinnön mukaan puutteelliset.[2] Mietinnössä esitettiin toimialakohtaisesti valmisteltavien tiedustelua koskevien lainsäädäntöhankkeiden käynnistämistä.[3]

Saman aikaisesti tiedonhankintalakityöryhmän kanssa sisäministeriön asettama työryhmä selvitti suojelupoliisin hallinnollista asemaa, tulosohjausta ja valvonnan kehittämistä. Johtopäätöksissään työryhmä ehdotti suojelupoliisille säädettäväksi uusia tiedustelutoimivaltuuksia, joiden avulla se kykenisi vastaamaan sen toimintaympäristössä tapahtuneisiin muutoksiin. Uudet toimivaltuudet mahdollistaisivat esimerkiksi tiedon

[1] HE 202/2017 vp, s. 6.
[2] Suomalaisen tiedustelulainsäädännön suuntaviivoja 2015, s. 14.
[3] Suomalaisen tiedustelulainsäädännön suuntaviivoja 2015, s. 81.

hankkimisen turvallisuutta uhkaavista hankkeista jo nykyistä aikaisemmin sekä tiedonhankinnan ulkomailta. Tiedustelullisten toimivaltuuksien laajenemisen vastapainoksi esitettiin, että suojelupoliisin esitutkintatehtäviä tulisi rajoittaa oikeudenmukaisen oikeudenkäynnin turvaamiseksi. Toimintaympäristön muutoksesta ei kuitenkaan raportin mukaan noussut tarvetta perustaa Suomeen erillistä siviilitiedusteluviranomaista suorittamaan tietojen hankintaa ulkomailta, sillä suojelupoliisin toiminta sisälsi jo tämän kaltaisia elementtejä. Ulkomaantiedustelua koskevien toimivaltuuksien laajetessa tulisi siviili- ja sotilastiedustelun tehtävien ohjauksen, sääntelyn ja valvonnan kehittämisen ottaa toisensa huomioon. [4]

Näiden pohjalta hallitus antoi tammikuussa 2018 eduskunnan käsittelyyn tiedustelulakikokonaisuuden, joka koostui neljästä esityksestä: oikeusministeriö valmisteli esityksen Suomen perustuslain 10 §:n muuttamisesta (HE 198/2017 vp) sekä esityksen laista koskien tiedustelutoiminnan valvontaa (HE 199/2017 vp). Puolustusministeriö valmisteli esityksen laiksi koskien sotilastiedustelua (HE 203/2017 vp) ja sisäministeriö esityksen siviilitiedustelua koskevaksi lainsäädännöksi (HE 202/2017 vp), jossa mm. esitettiin poliisilakiin sisällytettäväksi uusi, siviilitiedustelua koskeva 5 a luku sekä säädettäväksi uusi laki tietoliikennetiedustelusta siviilitiedustelussa.[5] Perustuslain (731/1999) 10 §:n muutokset astuivat voimaan 15.10.2018 ja laki tiedustelutoiminnan valvonnasta (121/2019) 1.2.2019. Siviili- ja sotilastiedustelua koskevat lait ja niistä johtuvat lakimuutokset astuivat voimaan 1.6.2019. Näistä keskeisin tämän tutkimuksen kannalta on laki tietoliikennetiedustelusta siviilitiedustelussa (582/2019).

Tämän tutkimuksen kohteena on siviilitiedustelussa suoritettavan tietoliikennetiedustelun ennakollinen lupamenettely. Tutkimus kohdistuu nimenomaisesti siviilitiedustelussa tapahtuvaan tietoliikennetiedusteluun rajaten täten tutkimuksen ulkopuolelle sotilastiedusteluun liittyvän lainsäädännön. Rajauksen perusteena on sotilastiedustelun kohteet – sotilastiedustelutoiminta kohdistuu lähinnä valtiollisiin toimijoihin ja sotilasorganisaatioihin, kun taas tässä tutkimuksessa näkökulma painottuu perus- ja ihmisoikeuksiin [6]. Tutkimuskohteen rajaaminen tietoliikennetiedusteluun muiden

[4] Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittäneen työryhmän loppuraportti 2014, s. 57-58.
[5] Sisäministeriön verkkosivut: ”Tiedustelulakikokonaisuus eteni eduskunnan käsiteltäväksi”. Uutinen 5/2018. Viitattu 3.12.2018.
[6] Laissa sotilastiedustelusta säädetään kuitenkin myös siviilitiedustelussa tehtävän tietoliikennetiedustelun teknisestä toteuttamisesta, joten siltä osin myös sotilastiedustelulaki on tutkimuksessa oleellinen.

siviilitiedustelumenetelmien sijasta perustuu ennen kaikkea siihen, että siinä perus- ja ihmisoikeuksien suojan voidaan nähdä korostuvan erityisen paljon esimerkiksi sen vuoksi, että sivullisten tahaton joutuminen tiedustelun kohteeksi on todennäköistä tietoliikennetiedustelun käytössä.[7] Lisäksi tietoliikennetiedustelu on yksi täysin uusista tiedustelumenetelmistä, jolloin tutkimukselle on tarvetta. Tietoliikennetiedustelun yksittäisissä osissa riittänee jokaisessa tutkittavaa, mutta tässä tutkimuksessa painopiste on ennakollisessa lupamenettelyssä. Ennakollisen lupamenettely on ratkaisevassa asemassa perus- ja ihmisoikeuksien turvaamisessa, sillä siinä oikeudellinen taho määrittää, onko tietoliikennetiedustelun käytölle perusteita sekä millaisilla ehdoilla suojelupoliisi on oikeutettu toteuttamaan tiedustelua. Tuomioistuimen laatima lupapäätös rajoittaa tiedusteluviranomaisen toimivaltaa, sillä siinä määritellään ehdot sille, millä kriteereillä, kuinka laajasti ja miten pitkään tietoliikennetiedustelua voidaan yksittäisessä tapauksessa harjoittaa.

1.1.2. Lyhyesti siviilitiedustelusta

Yleisesti tarve tiedusteluun voidaan johtaa valtion velvollisuudesta suojella kansalaisiaan. Sotilastiedustelun avulla voidaan hankkia tietoa poliittisista ja sotilaallisista muutoksista niin läheltä kuin kaukaakin, kun taas siviilitiedustelulla voidaan saada tietoa sellaisista tekijöistä, jotka uhkaavat kansalaisten lisäksi demokratian rakenteita. Tällaisia ovat esimerkiksi väkivaltaiset ääriliikkeet tai terrorismi. Itsenäinen tiedonhankinta on osa valtion suvereniteettia, osoitus valtiollisesta riippumattomuudesta. Valtion velvollisuutta suojella kansalaisiaan ei voi ulkoistaa muille tahoille eikä sitä voi perustaa pelkästään muilta saatavaan tietoon. Mahdollistaakseen riippumattoman päätöksenteon valtion tulee itse valita tiedustelun kohteensa perustuen omiin tarpeisiinsa ja arvioida kertynyttä tietoa omista lähtökohdistaan käsin.[8]

Toisen maailmansodan jälkeinen perus- ja ihmisoikeuskehitys on ollut suurin syy muutokseen tiedustelupalveluiden historiassa. Tiedusteluviranomaisten päämäärä on vuosisatojen aikana vaihtunut hallitsijan vallassa pysymisestä perus- ja ihmisoikeuksien toteutumiseen ja turvaamiseen.[9] Perus- ja ihmisoikeuksien turvaaminen näkyy Suomessa esimerkiksi poliisilain 1 luvussa, jossa määritellään ns. poliisioikeudelliset periaatteet. Periaatteet ohjaavat poliisin toimintaa erityisesti voimakeinojen ja salaisten tiedonhankintakeinojen käytön

[7] HE 202/2017 vp, s. 150.
[8] Porvali 2018, s. 11.
[9] Porvali 2018, s. 207.

yhteydessä.[10] Näitä poliisilaissa määriteltyjä periaatteita tulee suojelupoliisin soveltaa myös toteuttaessaan tietoliikennetiedustelua siviilitiedustelussa. Tiedustelutoiminnan avulla valtio suojelee kansalaisiaan sekä demokratiaa, mutta tämän toteuttaminen vaatii perus- ja ihmisoikeuksien keskinäistä punnintaa, jossa oikeus yksityisyyteen ja luottamukselliseen viestintään usein joutuu väistymään ”suuremman hyvän” tieltä.[11]

Siviilitiedustelua koskevassa hallituksen esityksessä ehdotettiin säädettäväksi uusi laki tietoliikennetiedustelusta siviilitiedustelussa sekä lisäämällä poliisilakiin uusi luku koskien siviilitiedustelumenetelmiä ja niiden käyttöä. Suomessa tiedonhankintaa kansallisen turvallisuuden tukemiseksi harjoittaa suojelupoliisi[12] , ja uusi siviilitiedustelulaki laajensi sen tiedonhankintatoimivaltuuksia. Uuden tiedustelua koskevan lainsäädännön myötä suojelupoliisin tehtävät laajenivat, ja poliisin hallinnosta annetun lain (110/1992) 10 §:n 1 momentin mukaan sen tehtäviin lukeutuu 1.6.2019 alkaen sisäministeriön ohjauksen mukaisesti tiedon hankkiminen kansallisen turvallisuuden suojaamiseksi sekä sellaisten toimintojen, hankkeiden ja rikoksien havaitseminen, estäminen ja paljastaminen, ”jotka voivat uhata valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä ja ulkoista turvallisuutta.” Suojelupoliisin tulee tämän lisäksi kehittää ja ylläpitää yleistä valmiutta estää ja havaita sellainen toiminta, joka uhkaa yhteiskunnan turvallisuutta.

Ennen uusia toimivaltuuksia suojelupoliisi sovelsi tehtäviensä toteuttamiseksi suorittamassaan kotimaan tiedonhankinnassaan poliisille säädettyjä toimivaltuuksia, joista säädetään poliisilain (872/2011) 5 luvussa.[13] Yhteistä kaikille poliisilain 5 luvun salaisille tiedonhankintakeinoille on, että ne määritellään rikos- ja henkilölähtöisesti. Tämä tarkoittaa, että keinoja voidaan käyttää vain sellaisessa tilanteessa, jossa on olemassa tiettyyn henkilöön kohdistuva rikostorjunnallinen peruste. Henkilön tulee siis perustellusti voida olettaa olevan syyllistynyt tai syyllistyvän tulevaisuudessa tietyn vakavuusasteen rikokseen tai sen valmisteluun. Jos suojelupoliisi halusi hankkia muuta tiedustelutietoa, tuli sen turvautua avointen lähteiden seurantaan. Avoimia lähteitä ovat poliisin yleisvalvonta sekä suojelupoliisin yhteistyöverkostonsa kautta saama tieto.[14] Suojelupoliisilla oli oikeus käyttää poliisilaissa määriteltyjä tiedonhankintakeinoja vain Suomen alueella, eikä suojelupoliisin valtion ulkopuolelle kohdistuvasta tiedonhankinnasta ollut säädetty. Tällöin ulkomaihin

[10] HE 202/2017 vp, s. 16.
[11] Porvali 2018, s. 209-210.
[12] HE 202/2017 vp, s.14
[13] Suomalaisen tiedustelulainsäädännön suuntaviivoja 2015, s. 28.
[14] HE 202/2017 vp, s. 19.

kohdistuva tiedonsaanti perustui avointen lähteiden seuraamiseen, kansainväliseen tiedusteluyhteistyöhön sekä suojelupoliisin omaan yhdysmiestoimintaan. [15]

Uuden siviilitiedustelua koskevan lainsäädännön myötä poliisilakiin lisättiin uusi 5 a luku, joka sisältää säännökset siviilitiedustelusta. Tietoliikennetiedustelusta säädetään erikseen laissa tietoliikennetiedustelusta siviilitiedustelussa. Siviilitiedustelu on suojelupoliisille säädetty uusi tehtävä, jolla poliisilain 5 a luvun 1 §:n mukaan tarkoitetaan ylimmän valtiojohdon päätöksenteon tukemiseksi, kansallisen turvallisuuden suojelemiseksi sekä muiden viranomaisten lakisääteisiä kansalliseen turvallisuuteen liittyviä tehtäviä varten harjoitettavaa tiedon hankkimista ja hyödyntämistä. Valtaosa poliisilaissa säädetyistä siviilitiedustelumenetelmistä perustuu menetelmällisesti aiempiin, poliisilain 5 luvussa esitettyihin salaisiin tiedonhankintakeinoihin. Täysin uusia siviilitiedustelumenetelmiä ovat tietoliikennetiedustelu, paikkatiedustelu, jäljentäminen, lähetyksen pysäyttäminen jäljentämistä varten sekä tietojen saaminen yksityiseltä yhteisöltä. Siviilitiedustelun kohteista säädetään niin ikään poliisilain 5 a luvun 3 §:ssä. Näitä ovat muun muassa terrorismi, ulkomainen tiedustelutoiminta, kansanvaltaista yhteiskuntajärjestystä uhkaava toiminta sekä kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi.[16]

Uudet tiedustelutoimivaltuudet irtautuivat rikos- ja henkilölähtöisyydestä, ja niiden erityiset edellytykset määritellään uhkaperusteisesti. Tämä mahdollistaa tiedustelutoiminnan harjoittamisen Suomen kansallista turvallisuutta vakavasti uhkaavan toiminnan kohdalla. Siinä missä salaisen tiedonhankinnan kohteet tulee lain mukaan pystyä yksilöimään esimerkiksi henkilön roolin tai tehtävän kautta, on tiedustelutoiminnalle tyypillistä, ettei henkilö ole tiedossa. Tiedustelutoiminnan tavoitteena on löytää henkilöitä, joiden toiminta on uhka kansalliselle turvallisuudelle. Tämän vuoksi siviilitiedustelua koskevassa lakiesityksessä esitettiin suojelupoliisin suorittamassa tiedustelutoiminnassa luovuttavaksi myös henkilölähtöisyydestä, jota poliisille säädetyissä salaisissa tiedonhankintakeinoissa sovelletaan.[17]

Uudet tiedustelulait vaativat vastapainokseen tehokkaan valvontajärjestelmän. Tiedustelutoiminnan laillisuusvalvontaa suorittamaan luotiin uusi viranomainen, tiedusteluvalvontavaltuutettu. Tiedusteluvalvontavaltuutetun tehtäviin kuuluu tiedustelutoiminnan valvonnasta annetun lain 7 §:n mukaan valvoa tiedustelumenetelmien,

[15] HE 202/2017 vp, s. 33.
[16] HE 202/2017 vp, s. 114-115. Siviilitiedustelun kohteista enemmän tämän tutkimuksen osiossa 5.3.
[17] HE 202/2017 vp, s. 74.

tiedustelutiedon käytön ja tiedustelutoiminnan laillisuutta sekä perus- ja ihmisoikeuksien toteutumista. Parlamentaarista valvontaa suorittamaan perustettiin puolestaan uusi eduskunnan tiedusteluvalvontavaliokunta, jonka tehtävänä on eduskunnan työjärjestyksen (40/2000) 31 b §:n 2 momentin mukaan tiedustelutoiminnan tarkoituksenmukaisuuden ja asianmukaisuuden valvonta, tiedustelutoiminnan painopisteiden arviointi ja seuranta sekä perus- ja ihmisoikeuksien toteutumisen seuranta ja edistäminen.

1.1.3. Tutkimuksen kulku

Tässä luvussa on tarkoitus kartoittaa tutkimuksen taustaa, siinä käytettäviä lähteitä sekä sovellettavaa metodia. Luvussa 2 käydään läpi tietoliikennetiedustelun käsitettä, sen toteuttamista ja siihen kohdistettavaa valvontaa. Luvun 2.1 tarkoituksena on tarjota kokonaiskuva tietoliikennetiedustelun käsitteestä ja sen toteuttamisesta. Erityisesti tietoliikennetiedustelun käytön sekä laissa käytettyjen termien avaaminen on keskeisessä asemassa, sillä myöhemmin lupa- ja päätösvaatimusta koskevissa osioissa käsitteitä käytetään laajasti. Luvun 2 jälkimmäisessä osiossa sivutaan tietoliikennetiedustelun valvontaa. Vaikka tässä tutkimuksessa keskeinen rooli onkin tietoliikennetiedusteluun kohdistuvalla ennakkovalvonnalla, on tärkeää tuoda esiin myös se, että ennakollinen valvonta on osa suurempaa valvontakokonaisuutta. Tämän vuoksi osiossa 2.2 esitellään lyhyesti tietoliikennetiedustelun, ja samalla yleisemmin tiedustelutoiminnan, valvontaelimet.

Tutkimuksen luvussa 3 käsitellään yksityisyyden suojaa perus- ja ihmisoikeutena. Yksityisyyden suoja ja erityisesti luottamuksellisen viestin suoja ovat perus- ja ihmisoikeuksia, joita tiedustelutoiminta erityisesti rajoittaa. Osiossa tarkastellaan yksityisyyden suojaa suhteessa tiedustelutoimintaan edellä mainittujen hallitusten esitysten sekä kansainvälisen oikeuskäytännön valossa kiinnittäen huomiota myös välttämättömyysvaatimukseen sekä ”vakava uhka kansalliselle turvallisuudelle” -käsitteeseen, jotka ovat samalla uusia, luottamuksellisen viestin salaisuuden suojan rajoitusperusteita sekä tietoliikennetiedustelun käytön yleisiä edellytyksiä. Tässä luvussa nostan esiin myös Euroopan ihmisoikeustuomioistuimen linjauksia yksityisyyden suojasta erityisesti salaisen tiedonhankinnan ja tiedustelutoiminnan näkökulmasta. Euroopan ihmisoikeustuomioistuimen oikeuskäytännöllä on keskeinen asema käsillä olevassa tutkimuksessa, joten tuomioistuimen käsitys yksityiselämän suojasta ja riittävästä oikeusturvasta on syytä avata jo tässä vaiheessa tutkimusta.

Luvussa 4 käsitellään lyhyesti tuomioistuimen ja suojelupoliisin roolia lupamenettelyssä. Vaikka suurin painopiste onkin jäljempänä luvussa 5 läpikäydyllä lupavaatimuksella ja -

päätöksellä, on kokonaisuuden kannalta tärkeää myös käydä läpi sitä kokoonpanoa, missä kyseiset asiakirjat laaditaan. Lisäksi luvussa käydään läpi lupamenettelyyn liittyvää vastuunjakoa näiden kahden viranomaisen välillä.

Luvussa 5 käsitellään tutkimuksen kannalta keskeisintä teemaa eli lupavaatimusta ja -päätöstä Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa. Lisäksi luvussa 5 sivutaan esittelynomaisesti niitä ongelmakohtia, joita Suomessa nousi esiin lainsäädäntövaiheessa. Näiden ongelmakohtien kautta on mahdollista nostaa esiin sellaisia seikkoja, joihin on syytä jatkossakin kiinnittää erityistä huomiota. Luvun tarkoitus on esitellä lupavaatimuksen- ja päätöksen sisältö yhteen osa-alueeseen kerrallaan keskittyen ja samalla kahteen edelliseen lukuun viitaten tarkastella näitä osa-alueita yksityisyyden ja luottamuksellisen viestin salaisuuden suojan rajoitusedellytysten näkökulmasta sekä sivuta sitä, mitä sekä suojelupoliisilta että tuomioistuimelta vaaditaan edellytysten täyttymiseksi.

Tutkimuksessa Suomen lainsäädäntöä peilataan Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön lähinnä neljän eri tapauksen ja järjestelmän kautta. Euroopan ihmisoikeustuomioistuin antoi vuonna 2018 kaksi keskeistä ratkaisua tiedusteluun liittyen: Centrum för Rättvisa v. Sweden (Application no. 35252/08, 19.7.2018). sekä Big Brother Watch and Others v. The United Kingdom (Applications nos. 58170/12, 62322/14 and 24960/15, 13.9.2018), jotka jo tuoreudesta johtuen ovat vertailun keskiössä[18]. Erityisesti Ruotsin lainsäädäntö nousee keskiöön, sillä se on käsillä olevista valtioista ainoa, jonka tiedusteluun liittyvän lainsäädännön tuomioistuin on kokonaisuudessaan nähnyt Euroopan ihmisoikeussopimuksen mukaisesti. Näiden lisäksi lähempään tarkasteluun nostetaan suuren jaoston tuomio Roman Zakharov v. Russia (Application no. 47143/06, 4.12.2015) sekä Szabó and Vissy v. Hungary (Application no. 37138/14, 12.1.2016). Zakharov-tapaus on tuoreehko esimerkki järjestelmästä, jossa tuomioistuinkontrolli jäi vajavaiseksi. Sekä Szabó and Vissy ja Big Brother Watch -tuomio ovat puolestaan esimerkkejä järjestelmistä, joissa tiedusteluun vaadittavaa lupaa ei myönnä tuomioistuin.

Tutkimuksen viimeisessä luvussa käydään läpi analyysin pohjalta syntyneet johtopäätökset ja vastataan näin seuraavassa osiossa esitettyihin tutkimuskysymyksiin.

[18] Sekä Ruotsin että Iso-Britannian tapaukset ovat tällä hetkellä vireillä Suuressa jaostossa. Molempiin tapauksiin liittyen pidettiin kuuleminen 10.7.2019.

1.2. Tutkimuskysymys ja aiempi tutkimus

Tämän tutkimuksen tarkoituksena on tarkastella siviilitiedustelussa suoritettavan tietoliikennetiedustelun ennakollista lupamenettelyä Euroopan ihmisoikeustuomioistuimen oikeuskäytännön valossa. Tutkimus kohdistuu nimenomaisesti lupavaatimukseen ja -päätökseen. Päämääränä on selvittää, miten lupavaatimuksella ja -päätöksellä voidaan Euroopan ihmisoikeustuomioistuimen oikeuskäytännön näkökulmasta taata todellinen ennakkovalvonta. Kun tietoliikennetiedustelulla puututaan erityisesti luottamuksellisen viestin salaisuuden suojaan ja tuomioistuinmenettelyn on tarkoitus varmistaa, että siihen puututaan mahdollisimman kohdennetusti ja rajoitetusti, muodostuu pääasialliseksi tutkimuskysymykseksi, *miten lupavaatimuksella ja -päätöksellä voidaan varmistaa, että perus- ja ihmisoikeuksien rajoituksia sovelletaan niin kuin on tarkoitettu*? Perus- ja ihmisoikeusrajoituksella viitataan tässä niin perustuslaista kuin Euroopan ihmisoikeussopimuksesta johtuviin rajoituksiin.

Tarkastelen kysymystä annettujen hallitusten esitysten, lausuntojen ja mietintöjen kautta sekä Euroopan ihmisoikeustuomioistuimen tekemien ratkaisujen näkökulmasta. Tutkimuskysymykseen pyrin vastaamaan apukysymyksien avulla. Apukysymyksiäni ovat *(1) mitä Suomessa säädetään ennakollisesta lupamenettelystä; (2) millaisia kriteerejä Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä voidaan löytää tuomioistuinmenettelyä koskien; sekä (3) miten Suomen lainsäädäntö näyttäytyy Euroopan ihmisoikeustuomioistuimen valossa?*

Tietoliikennetiedustelusta ja siviilitiedustelusta tässä merkityksessä säädetään Suomessa nyt ensimmäistä kertaa. Tuoreen aihepiirin lisäksi aihetta on tärkeää tutkia sen vuoksi, että uusi siviilitiedustelulaki rajoittaa kansalaisten perus- ja ihmisoikeuksia. Perus- ja ihmisoikeuksien rajoittaminen tulee olla tarkasti perusteltua ja on tärkeää valvoa, että tätä ei tapahdu perusteettomasti. Tutkimuskohteena oleva ennakollinen lupamenettely tapahtuu tiedustelun kohteelta salassa, joten on erittäin tärkeää, että menettelyllä itsessään pystytään takaamaan yksilön perus- ja ihmisoikeuksien toteutuminen viranomaisessa. Yksilön täytyy pystyä luottamaan siihen, ettei hänen perus- ja ihmisoikeuksiaan rajoiteta ilman hyväksyttävää perustetta.

Tärkeän osan tutkimuksen analyysiä muodostaa kansainvälinen näkökulma, jota vasten Suomeen esitettyä mallia on mahdollista verrata. Tällöin asian käsittelyä ei tarvitse jättää

pelkästään teoreettiselle tasolle, vaan käsiteltävien Euroopan ihmisoikeustuomioistuimen ratkaisujen kautta voidaan löytää konkreettisia esimerkkejä koskien tietoliikennetiedustelua.

Euroopan ihmisoikeussopimus (SopS 63/1999), jonka soveltamisesta ja tulkinnasta Euroopan ihmisoikeustuomioistuin vastaa, on Suomessa lisäpöytäkirjoineen saman tasoinen säädös kuin eduskuntalait. Tästä seuraa, että sitä sovelletaan kuten eduskuntalakia tuomioistuimissa ja viranomaistoiminnassa. Euroopan ihmisoikeussopimuksessa turvatut ihmisoikeudet luovat minimitason, jota huonompaa suojaa valtio ei voi kansalaisilleen antaa. Kyseinen minimistandardi on huomioitava myös perusoikeussäännöksiä tulkittaessa ja usein Euroopan ihmisoikeussopimuksen vaatimukset huomioidaan jo lainvalmisteluvaiheessa.[19]

Jokaisen valtion tiedustelujärjestelmä ja lainsäädäntö ovat yksilöllisiä eivätkä tutkimuksessa käytetyt esimerkkitapaukset ole suoraan verrattavissa Suomen kansalliseen lainsäädäntöön. Euroopan ihmisoikeustuomioistuin on kuitenkin vuosikymmenien ajan käsitellyt tapauksia liittyen salaiseen tiedonhankintaan ja tiedusteluun suhteessa ihmisoikeuksiin ja sen oikeuskäytännöstä on löydettävissä vakiintuneita linjauksia, joiden valossa Suomen tietoliikennetiedustelun ennakollista lupamenettelyä on mahdollista tarkastella. Kansainvälisen näkökulman merkityksestä kertoo myös se, että hallituksen esityksissä sekä perustuslakivaliokunnan lausunnoissa ja mietinnöissä on johdonmukaisesti korostettu, että uusien lakien tulee olla yhdenmukaiset Suomea koskevien kansainvälisten ihmisoikeusvelvoitteiden kanssa, ja yksi perusoikeuksien yleisistä rajoitusedellytyksistä on vaatimus rajoituksen yhteensopivuudesta kansainvälisten sopimusten kanssa.

Aiempaa tutkimusta aiheeseen liittyen on ehtinyt ilmestyä jonkin verran. Lapin yliopistossa valmistui syksyllä 2018 Sami Pekolan pro gradu –tutkielma aiheena ”Tiedustelu oikeusvaltiossa: tiedustelutoimivaltuuksien laajentaminen tiedustelun valvonnan näkökulmasta”. Pekola tarkastelee työssään sitä, miten tiedustelun toimivaltuudet ja niiden käyttämisen valvonta tulisi järjestää demokraattisessa oikeusvaltiossa perus- ja ihmisoikeuksien näkökulmasta. Hän tutkii aihetta informaatio-oikeudellisesta näkökulmasta, jolloin keskiössä on oikeus tietää ja oikeus tietoon. Hän havaitsee työssään, että yksityiselämän suojaan liittyvissä kysymyksissä oikeusturva, yksilön oikeudet ja laajempi tiedustelutoiminnan yhteiskunnallinen hyväksyttävyys ovat yhteydessä toisiinsa: tiedustelutoiminnan tulee nauttia yleistä hyväksyntää, jotta perus- ja ihmisoikeuksiin voidaan

[19] Pellonpää et al. 2018, s. 64-66.

oikeusvaltiossa puuttua. Jotta tiedustelutoiminta voi olla yleisesti hyväksyttyä, sen taas tulee olla oikeusvaltion periaatteiden mukainen.[20]

Helsingin yliopistossa on julkaistu Petra Tokoin pro gradu aiheena ”Yksityiselämän suoja perusoikeutena ja tietoliikennetiedustelun toteuttaminen kansallisessa lainsäädännössä”. Tokoin gradu julkaistiin vuonna 2016. Tokoin työ on lainopillinen ja siinä hyödynnetään osaksi de lege ferenda –näkökulmaa. Hän tarkastelee työssään tiedonhankintalakityöryhmän mietintöä sekä siihen liittyviä asiakirjoja perusoikeusnäkökulmasta. Hänen tutkimuskysymyksiään on, onko uudelle massaluontoiselle tietoliikennetiedustelulle olemassa perusteita vai onko poliisilla ja muilla viranomaisilla jo nykyisellään pakkokeinolainsäädäntöön perustuen riittävät oikeudet saada tietoa terrorismin ja muun rikollisuuden torjumiseen. Hänen mukaansa pakkokeinolainsäädäntöä tulisi kehittää nykypäivän uhkia vastaaviksi mutta samalla välttää kohdentamatonta massavalvontaa, joka puuttuu yksityisyyden suojaan.[21]

Turun yliopiston oikeustieteellisestä tiedekunnasta valmistuneessa Mika Havulinnan sisältöanalyyttisessa pro gradu –tutkielmassa ”Kansallinen turvallisuus vs. perusoikeudet: Lainsäädäntötutkimus tiedustelulakihankkeesta” käsitellään tiedustelun suhdetta perus- ja ihmisoikeuksiin tiedustelulainsäädännöstä annettujen lausuntojen kehyksessä. Tutkimuksessa todettiin, että määrällisesti suurimmiksi ongelmiksi asiantuntijalausunnoissa nousivat väitteet tietoliikennetiedustelun tehottomuudesta sekä kohdentamattomuudesta, jotka Havulinna yhdistää vaatimukseen perusoikeuksien rajoituksen suhteellisuudesta, välttämättömyydestä sekä hyväksyttävyydestä. Tuloksissa nähtiin myös keskeiseksi, että perustuslain 10 §:n sanamuotoa tulisi muuttaa, jotta tietoliikennetiedustelun käytölle olisi hyväksyttävät perusteet. Havulinna peräänkuuluttaa tietoliikennetiedustelua koskevan lain tarkkarajaisuutta sekä vaatimusta lupamenettelystä ja riittävistä oikeussuojakeinoista.[22]

Katariina Kuhanen Helsingin yliopistosta keskittyy pro gradussaan Euroopan ihmisoikeustuomioistuimen kansallista turvallisuutta koskevaan oikeuskäytäntöön. Hän tutkii kansallista turvallisuutta yksityiselämän suojan rajoittajana erityisesti salaisen tiedonhankinnan valvonnalle asetettujen vaatimusten kautta. Tutkielmassa on tarkoitus selvittää, onko tuomioistuimen ratkaisukäytännössään antamat vaatimukset muuttuneet ja tarkentuneet ajan mittaan. Arvioinnissa keskitytään valvonta- ja tiedustelujärjestelmien

[20] Pekola 2018, s. 105.
[21] Tokoi 2016, tiivistelmä.
[22] Havulinna 2018, s. 93-97.

valvonnalle sekä oikeussuojakeinoille annettuihin vaatimuksiin ja edellytyksiin, sekä tuomioistuimen tulkintaperiaatteisiin ja niiden merkitykselle.[23]

Tanja Pietiläisen pro gradun aiheena on ”Yksityiselämän suoja tietoliikennetiedustelussa”. Myös tässä tutkimuksen keskiössä on uusi tietoliikennetiedustelua koskeva lainsäädäntö. Tutkielmassa Pietiläinen nostaa tärkeäksi yksityiselämän suojaamisen keinoksi ilmoitusvelvollisuuden, jonka avulla tiedustelutoimet voidaan saattaa riippumattoman viranomaisen arvioitavaksi. Ongelmalliseksi nähdään, että ilmoitusvelvollisuus ei koske sivullisia – positiiviseksi katsotaan kuitenkin, että kyseistä toimenpidettä on täydennetty mm. hävittämisvelvollisuudella. Kokonaisuutena tutkimuksessa katsotaan, että yksityiselämän suoja on huomioitu uudessa lainsäädännössä ja tietoliikennetiedustelun eri vaiheissa kattavasti. Vaikka yksityiselämän suojaan puututaan tiedustelun keinoin, se nähdään hyväksyttäväksi, koska tällä on mahdollista suojata kansallista ja kollektiivista turvallisuutta.[24]

Jokaisella yllä esitellyillä tutkimuksilla on liitäntäkohta omaan tutkimukseeni, mutta näidenkin jälkeen omalle pro gradulleni riittää vielä kysyntää. Kuhasen tutkielmaa lukuun ottamatta pro gradut on julkaistu ennen lakien voimaantuloa, ja esimerkiksi tietoliikennetiedustelulakia koskien keskustelua käytiin vielä helmikuussa 2019. Tietoliikennetiedusteluun liittyvään ennakolliseen valvontaan perus- ja ihmisoikeuksien turvaajana ei ole aiemmissa tutkimuksissa pureuduttu ja esimerkiksi Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään korostanut tiedustelutoiminnan käytön alistamista juridiselle valvonnalle ihmisoikeuksien toteutumisen turvaajana[25]. Tuomioistuinkontrollin todellisuutta peräänkuulutetaan myös perustuslakivaliokunnan lakiesityksestä antamassa lausunnossa[26]. Voidaan siis katsoa, että tuomioistuinmenettely muodostaa keskeisen osan perus- ja ihmisoikeuksien turvaamista tietoliikennetiedustelussa, eikä aiheeseen ole vielä tutkimuksissa tartuttu, jolloin käsillä olevalle tutkimukselle on tilaa.

[23] Kuhanen 2019, tiivistelmä.
[24] Pietiläinen 2018, tiivistelmä.
[25] Ks. esim. tuomioistuimen ratkaisu Centrum för Rättvisa (19.7.2018), kohta 133 lakiviittauksineen.
[26] PeVL 35/2018 vp, s. 29.

1.3. Metodiset valinnat ja lähdeaineisto

Metodilla tarkoitetaan tieteellistä tutkimusmenetelmää – se on väline, jonka avulla saadaan tietoa tutkimuksen kohteesta. Eri tieteenaloilla on käytössä erilaisia metodeja ja niiden valintaan vaikuttavat tutkimuksen kohde ja tutkimustehtävä. [27] Oikeustieteen tutkimuskohteena on oikeus, jolloin tutkimuksessa käytettävät metodit ovat erilaisia verrattuna esimerkiksi luonnontieteisiin, jossa tutkimuksen tarkoituksena on selittää ilmiöitä; oikeustiede tulkitsee selittämisen sijaan.[28] Käsite ”oikeus” pitää sisällään kaikki oikeudelliset ilmiöt, eikä rajoitu pelkästään voimassa olevaan oikeuteen[29].

Tässä tutkimuksessa tutkimusmetodina sovelletaan lainoppia eli oikeusdogmatiikkaa. Oikeusdogmatiikka on yksi oikeustieteen keskeisistä ja merkittävimmistä osa-alueista[30]. Oikeusdogmatiikan tutkimuskohteena on voimassa oleva oikeusjärjestys ja sen keskeisenä tehtävänä on selvittää voimassaolevan oikeuden sisältö kulloinkin käsiteltävänä olevassa oikeusongelmassa eli etsiä vastaus siihen, kuinka voimassa olevan oikeusjärjestyksen mukaan tulee toimia todellisessa tilanteessa. Sen avulla voidaan tutkia, tulkita ja systematisoida oikeusjärjestykseen kuuluvia sääntöjä.[31] Tämän lisäksi voidaan tutkia, mikä merkitys laista sekä muista oikeuslähteistä löytyvällä materiaalilla on[32].

Tehtäviensä perusteella oikeusdogmatiikka voidaan jakaa tulkintalainoppiin ja teoreettiseen lainoppiin. Tulkintalainoppi hoitaa oikeusdogmatiikan tulkitsevaa tehtävää, jolloin kohteena on oikeuden pintataso eli säädökset, tuomioistuinratkaisut sekä oikeustieteellinen tutkimus. Teoreettinen lainoppi puolestaan painottaa oikeusdogmatiikan systematisoivaa osaa. Systematisoinnin tarkoituksena on muotoilla eri oikeudenalojen yleisiä oikeusperiaatteita ja -käsityksiä, jolloin sen kohteena on oikeuskulttuuri.[33]

Lainoppia voidaan jaotella edelleen sen tutkimuskohteen mukaan. Edellä kuvattiin lainopin perinteistä, sääntökeskeistä näkökulmaa, jossa säädöksiä tulkitsemalla saadaan informaatiota oikeusnormien sisällöstä. Sääntökeskeisen näkökulman ohella toinen mahdollinen muoto on

---

[27] Hirvonen 2011, s. 4
[28] Aarnio 2006, s. 238. Aarnio näkee oikeustieteellisessä tutkimuksessa sovellettavan harkinnan niin voimakkaana, että esittää oikeustieteen metodin olevan luonteeltaan enemmänkin näkökulma verrattuna esimerkiksi luonnontieteen metodeihin. Tässä tutkimuksessa puhutaan kuitenkin oikeusdogmatiikasta yhtenä tutkimusmetodina muiden joukossa.
[29] Hirvonen 2011, s. 21.
[30] Ks. esim. Husa et al. 2008, s.19 sekä Aarnio 2011, s.1.
[31] Husa et al. 2008, s. 19-20.
[32] Hirvonen 2011, s. 23-24.
[33] Tuori 2000, s. 303. Ks. myös Aarnio 2006, s. 238.

tapauskeskeinen oikeustutkimus, jota sovelletaan suurelta osin vain common law -maissa. Suomalaisessa järjestelmässä tapauskeskeistä oikeustutkimusta lähinnä ovat oikeudellisissa julkaisuissa ilmestyvät, ylimpien oikeuksien ratkaisuja koskevat kommentaarit.[34]

Oikeusdogmatiikan avulla käsillä olevassa tutkimuksessa pyritään selvittämään, millainen on tietoliikennetiedustelua koskevien säädösten sisältö ja miten niiden sisältämiä oikeusnormeja voidaan tulkita. Tutkimuksessa painottuu vahvasti siis oikeusdogmatiikan tulkinnallinen tehtävä ja sääntökeskeinen näkökulma. Tulkitsemistehtävässä apuna toimivat erilaiset oikeuslähteet. Tärkeän osan tutkimuksen lähdeaineistoa muodostavat tietoliikennetiedustelulain valmisteluaineisto eli lain esityöt. Näihin kuuluvat jo alussa mainitut hallituksen esitykset sekä valiokuntien, erityisesti perustuslakivaliokunnan, lausunnot ja mietinnöt sekä valiokunnille, erityisesti perustuslakivaliokunnalle annetut asiantuntijalausunnot.

Tutkimuksellisesti lain esityöt ovat merkittäviä sen vuoksi, että ne avaavat lainsäätäjän tahtoa. Aarniolaisen oikeuslähdeopin mukaan lain esityöt luetaan heikosti velvoittaviin oikeuslähteisiin, eli ne eivät velvoita tuomiovaltaa soveltamaan niitä laintulkinnassa, mutta niiden käyttö on sallittua. Toisin kuin vahvasti velvoittavan oikeuslähteen, ei heikosti velvoittavan oikeuslähteen soveltamatta jättäminen johda virkavirheeseen. Aarnio kuitenkin pitää heikosti velvoittavia oikeuslähteitä sellaisina, joiden sivuuttaminen tulee perustella. Mitä lähempänä eduskunnan päätöksentekoa esityö on, sitä suurempi voidaan katsoa sen painoarvon olevan laintulkinnassa. Hallituksen esityksellä voidaan katsoa olevan suuri painoarvo, jos lakiesitystä ei ole muutettu[35]. Käsiteltävänä oleva lakiesitys ja -esitykset kävivät läpi monia vaiheita, joissa niistä muokattiin perustuslain mukaisia säädöksiä. Näiden keskustelujen esiin tuominen on keskeinen osa tutkimusta, sillä niiden kautta on mahdollista tunnistaa lain ns. kipukohdat ja näin nostaa esiin se, mitä lakia säädettäessä on pidetty tärkeänä ja keskeisenä osana perus- ja ihmisoikeuksien toteutumista.

Esitöiden suureen määrään ja niiden käyttämiseen tulkinnan apuna on otettu kantaa myös perustuslakivaliokunnalle annetuissa lausunnoissa. Valtiosääntöoikeuden professori Tuomas Ojasen mukaan esitöitä voidaan käyttää apuna lakeja tulkittaessa, mutta tarkastelussa olevaa lakiesitystä arvioitaessa on syytä muistaa, että hallituksen esittämiin lakiehdotuksiin tuli eduskunnan käsittelyssä huomattavia muutoksia, jolloin hallituksen esityksen merkityksen

[34] Aarnio 2011, s. 13 ss.
[35] Aarnio 1989, s. 226-227.

tulkintaa ja soveltamista ohjaavana esityönä voidaan katsoa heikentyneen. Ojanen katsoo, että perinteisen pelkän hallituksen esityksen lisäksi ja sen sijasta käsillä olevan lainsäädännön tulkinnassa ja soveltamisessa tulisi ottaa lain esitöinä huomioon valiokuntien, erityisesti perustuslakivaliokunnan, lausunnot ja mietinnöt.[36]

Toinen hyvin keskeinen oikeuslähde on Euroopan ihmisoikeustuomioistuimen antamat, aiheeseen liittyvät tuomiot. Kansainvälisen näkökulman mukaan tuominen tutkimukseen perustuu ennen kaikkea siihen, että Suomen lainsäädännön on oltava sopusoinnussa Suomea sitovien kansainvälisten sopimusten kanssa. Euroopan ihmisoikeussopimuksen lisäksi Suomea sitoo kuitenkin myös Euroopan unionin perusoikeuskirja sekä YK:n Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (SopS 8/1976), jotka kuitenkin on rajattu tämän tutkimuksen ulkopuolelle. Kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen täytäntöönpanoa valvova ihmisoikeuskomitea ei ole käsitellyt sähköisen viestintään tai tietoverkkoturvallisuuteen liittyviä asioita, vaikka niistä on tehty valituksia 17 artiklan perusteella[37], minkä vuoksi myös kyseinen sopimus rajautuu ulos tästä tutkimuksesta.

Euroopan unionin perusoikeuskirja ja unionin tuomioistuimen oikeuskäytäntö on rajattu tutkimuksen ulkopuolelle siksi, että pelkästään perusoikeuskirjassa määritellyt oikeudet eivät anna Euroopan unionin tuomioistuimelle toimivaltaa, toisin kuin Euroopan ihmisoikeussopimuksessa turvatut ihmisoikeudet Euroopan ihmisoikeustuomioistuimelle. Euroopan unionin perusoikeuskirjaa sovelletaan silloin, kun jäsenvaltio soveltaa Euroopan unionin oikeutta, ja Euroopan unionin tuomioistuin ei ole toimivaltainen sellaisissa tilanteissa, joissa on kyse vain perusoikeuskirjan alaan kuuluvasta oikeudellisesta ongelmasta, sillä yksin perusoikeuskirja ei luo tuomioistuimelle toimivaltaa. Oikeudellisen tilanteen tulee liittyä sellaiseen lainkäyttöalueeseen, johon tuomioistuimella on toimivalta, ja tällöin tulee arvioitavaksi myös perusoikeuskirjassa turvatut oikeudet.[38]

Koska tutkimuksen on tarkoitus keskittyä nimenomaan perus- ja ihmisoikeuksiin, on Euroopan unionin tuomioistuimen oikeuskäytäntö sekä perusoikeuskirja rajattu tutkimuksen ulkopuolelle. Tuomioistuin on kuitenkin käsitellyt huomionarvoisia tapauksia koskien

[36] Ojanen 20.2.2019, s. 6-7.
[37] HE 202/2017 vp, s. 51.
[38] Ks. esim. suuren jaoston tuomio Åkerberg Fransson (26.2.2013), kohdat 21-22.

sähköiseen viestintään ja yksityisyydensuojaan, jotka on myös huomioitu Suomen tiedustelulain valmisteluissa. [39]

[39] HE 202/2017 vp, s. 66. Aihealueeseen liittyviä tuomioita esim. Tele2 Sverige AB ja Secretary of State for the Home Department (yhdistetyt asiat C-203/15 ja C-698/15), Digitals Rights Ireland ja Kärntner Landesregierung. (yhdistetyt asiat C-293/12 ja C-594/12) ja Schrems (C-362/14).

2. Tietoliikennetiedustelu

2.1. Tietoliikennetiedustelun käsite ja toteutus

Tietoliikennetiedustelu on yksi täysin uusista siviilitiedustelun tiedustelumenetelmistä. Tietoliikennetiedustelua käytetään menetelmänä myös sotilastiedustelussa, mutta tässä tutkimuksessa viitataan kyseisellä termillä yksinomaan siviilitiedustelussa suoritettavaan tietoliikennetiedusteluun. Tietoliikennetiedustelusta säädetään laissa tietoliikennetiedustelusta siviilitiedustelussa (jäljempänä tietoliikennetiedustelulaki) ja muista siviilitiedustelussa käytettävistä tiedustelumenetelmistä säädetään poliisilain 5 a luvussa. Tietoliikennetiedustelun käyttäjänä toimii siviilitiedusteluviranomainen eli suojelupoliisi. Tietoliikennetiedustelulain 3 §:ssä luetellaan kokonaisuudessaan tietoliikennetiedustelun perusteuhat eli ne vakavasti kansallista turvallisuutta uhkaavat toimet, joista tietoliikennetiedustelulla saa hankkia tietoa. Perusteuhat ovat kaikissa siviilitiedustelussa sovellettavissa tiedustelumenetelmissä samat, mikä mahdollistaa tarvittaessa sujuvan siirtymisen menetelmästä toiseen. [40]

Tietoliikennetiedustelun keskeisille käsitteille on annettu määritelmät tietoliikennetiedustelulain 2 §:ssä. Tietoliikennetiedustelu on Suomen rajat viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa tiedonhankintaa, jota toteutetaan automatisoidun erottelun avulla. Tietoliikennetiedusteluun sisältyy myös hankitun tiedon käsitteleminen. Tietoliikennetiedustelulla hankitaan tietoja pelkästään valtion rajat ylittävästä tietoliikenteestä, eli sellaisesta, joka siirtyy suomalaisesta viestintäverkosta ulkomaiseen tai päinvastoin. Viestintäverkko määritellään toisiinsa liitetyistä johtimista ja laitteista muodostuvaksi järjestelmäksi, jolla on tarkoitus siirtää tai jakaa viestejä ”[…] johtimella, radioaalloilla, optisesti tai muulla sähkömagneettisella tavalla.” Termin määritelmässä keskeistä on vaatimus siitä, että tiedonsiirto tapahtuu sähkömagneettisesti. Muilta osin käsite on luonteeltaan teknologianeutraali. Suurin osa tietoliikennetiedustelun kohteena olevasta tietoliikenteestä liikkuu kaapeleiden välityksellä, mutta viestintäverkon teknologianeutraaliuden tarkoituksena on varmistaa lain soveltuvuus myös viestintäteknologian muuttuessa sekä muissa teknisissä ympäristöissä.[41] Tämän lisäksi termin määritelmässä on keskeistä, että viestintäverkon käyttötarkoitukseksi on määritelty viestien

[40] HE 202/2017 vp, s. 122. Tietoliikennetiedustelun kohteista ks. tutkimuksen osio 5.3.
[41] HE 202/2017 vp, s. 122.

siirto tai jakelu. Tällöin tietoliikennetiedustelulla on mahdollista hankkia viestintäverkosta myös sellaista tietoa, jota ei välttämättä pidetä viestintänä. [42]

Suuri osa suomalaisesta tietoliikenteestä on rajattu tietoliikennetiedustelun ulkopuolelle säätämällä tietoliikennetiedustelun kohdistumisesta vain rajat ylittävään tietoliikenteeseen. Kuitenkaan pelkästään se, että tietoliikenne ylittää Suomen rajat ei tarkoita, että se on kansainvälistä tietoliikennettä: Suomen sisäiseksi tarkoitettu tietoliikenne voi satunnaisesti kulkea ulkomaisen viestintäverkon kautta, ja voi tällöin joutua tietoliikennetiedustelun kohteeksi. Tämän vuoksi on tarpeellista säätää erikseen kotimaiseen viestintään kohdistuvasta tiedustelukiellosta. Tietoliikennetiedustelulain 12 §:ssä säädetään erikseen, että kotimaiseen viestintään ei saa kohdistaa tiedustelua ja jos tällainen viestintä joutuu tietoliikennetiedustelun kohteeksi, 15 §:ssä säädetään velvollisuudesta hävittää tällaisesta viestinnästä saatu tieto viipymättä.[43]

Suomen sisäinen viestintä on rajattu pois tietoliikennetiedustelun kohteista, koska kyseisellä menetelmällä on tarkoitus hankkia tietoa vain niistä uhista, jotka kohdistuvat kansalliseen turvallisuuteen ulkoa päin. Tämä ei kuitenkaan tarkoita, etteikö myös Suomen sisällä tapahtuva osapuolten välinen viestintä sisältäisi sellaista tiedustelun kannalta merkityksellistä tietoa. Kotimaisten viestien sisällöllä voidaan kuitenkin arvioida olevan kansainvälistä viestintää pienempi merkitys, kun hankitaan tietoa niistä uhista, joihin tietoliikennetiedustelua saa lain mukaan kohdistaa. Tällöin voidaan pitää perusteltuna, että kotimaisen viestinnän selvittäminen perustuu muihin poliisilain 5 a luvussa lueteltuihin siviilitiedustelumenetelmiin tietoliikennetiedustelun sijasta.[44]

Tietoliikennetiedustelua toteutetaan tietoliikenteen automatisoidulla erottelulla. Tiedon hankkimiseksi tietoliikennettä suodatetaan automaattisin menetelmin siitä kohdasta viestintäverkkoa, jossa tiedustelun kohteena olevaan uhkaan liittyvää tietoa voidaan olettaa kulkevan. Suodattaminen tapahtuu vertaamalla valittua tietoliikennevirtaa ennakolta asetettuihin kriteereihin eli hakuehtoihin. Suodattamisen avulla uhkaan liittyvä viestintä havaitaan ja sen taustalla olevat osapuolet tunnistetaan ja paikallistetaan. Suodattamisen piiriin ei kuulu kaikki viestintäverkoissa Suomen rajan ylittävä tietoliikenne, vaan tietoliikennetiedustelun käyttäminen vaatii suojelupoliisin epäilyksen tai tiedon jonkin laissa määritellyn perusteuhan todellisesta olemassaolosta ja siihen liittyvistä tosiasioista. Se, missä

[42] HE 202/2017 vp, s. 235. Viestintäverkosta laajemmin tutkimuksen osiossa 5.6.
[43] HE 202/2017 vp, s. 234.
[44] HE 202/2017 vp, s. 251.

viestintäverkon osassa uhkaan liittyvän viestinnän voidaan olettaa kulkevan rajan yli, riippuu uhan luonteesta ja tiedossa olevista tosiseikoista [45]

Tietoliikennetiedustelun teknisestä toteutuksesta vastaa puolustusvoimien tiedustelulaitos suojelupoliisin toimeksiannosta. Tietoliikennetiedustelun teknisestä toteuttamisesta säädetään tarkemmin sotilastiedustelua koskevan lain (590/2019) 73 §:n 1 momentin 2 kohdassa. Päätös teknisen toteuttamisen keskittämisestä yhdelle viranomaiselle perustuu tiedonhankintalakityöryhmän raporttiin: Sen sijaan, että sekä siviili- että sotilastiedusteluviranomaiset toteuttaisivat omaa tietoliikennetiedusteluaan, keskittämisellä voidaan vastata vaatimuksiin toiminnan yhdenmukaisuudesta ja salassa pidettävästä luonteesta, tarvittavasta erikoistumisesta ja teknisestä osaamisesta sekä lainmukaisuuden valvontaan liittyviin näkökulmiin. Puolustusvoimien tiedustelulaitoksen valintaa tehtävää suorittavaksi viranomaiseksi puolsivat sen omaama tekninen osaaminen sekä kansainväliset yhteistyösuhteet, joita molempia tehtävässä edellytetään.[46]

Teknisessä toteuttamisessa keskeistä on, että puolustusvoimien tiedustelulaitos toteuttaa suojelupoliisin puolesta tietoliikenteen automaattisen erottelun, eli viestintäverkon osassa kulkevan tiedon suodattamisen hakuehtoihin vertaamalla. Suojelupoliisi toimittaa tiedustelulaitokselle tietoliikennetiedustelua koskevan lupapäätöksen, josta ilmenee mm. käytettävät hakuehdot sekä se osa viestintäverkkoa, johon suodatus saa kohdistua. Kytkennästä vastaava taho eli Suomen Erillisverkot Oy luovuttaa puolustusvoimien tiedustelulaitokselle sen tietoliikenteen, joka liikkuu luvassa määritellyssä viestintäverkon osassa. Tietoliikenne peilataan virtaamaan tiedustelulaitoksen hallinnoiman teknisen tiedustelujärjestelmän läpi, jonne on ennakolta syötetty lupapäätöksessä mainitut hakuehdot. Tällä tavalla eroteltu tietoliikenne toimitetaan toimeksiantajalle eli suojelupoliisille, joka vastaa myös täysin erotellun materiaalin jatkokäsittelystä.[47]

Automatisoidun erottelun avulla suodatettu tietoliikenne ohjautuu jatkokäsittelyyn, josta vastaa suojelupoliisi. Tietoliikennetiedustelulain 6 §:n mukaan jatkokäsittelyyn ohjautunutta tietoliikennettä saa käsitellä sekä automaattisesti että manuaalisesti. Jatkokäsittelyssä saadaan selvittää viestin sisältö sekä muita luottamuksellisia tietoja, kuten viestinnän tunnistamistietoja sekä sijainti- ja välitystietoja. Automaattisella käsittelyllä tarkoitetaan jatkokäsittelyyn ohjautuneeseen tietoliikenteeseen kohdistettavaa, teknisen tietojärjestelmän

[45] HE 202/2017 vp, s.122.
[46] HE 202/2017 vp, s. 128. Ks. myös Suomalaisen tiedustelulainsäädännön suuntaviivoja 2015, s. 66.
[47] HE 202/2017 vp, s. 128.

avulla tehtävää analyysia. Automaattisessa käsittelyssä kerättyyn tietoon kohdistetaan esimerkiksi hakuja, jolla voidaan vähentää manuaalisesti käsiteltävän tiedon määrää. Manuaalinen käsittely puolestaan on luonnollisen henkilön suorittamaa, erotellun tiedon tarkastelua. Manuaaliseen käsittelyyn sisältyy esimerkiksi viestin tekstisisällön tai viestiin sisältyvän kuvien ja äänien havainnoimista suojelupoliisin palveluksessa olevan virkamiehen toimesta. [48]

Tietoliikennetiedustelun käytölle on säädetty lain 4 §:ssä yleiset edellytykset. Yleisenä edellytyksenä 1 momentin mukaan tietoliikennetiedustelulle on, että se on välttämätöntä tärkeiden tietojen saamiseksi tiedustelun kohteena olevasta, kansallista turvallisuutta vakavasti uhkaavasta toiminnasta. Tietoliikennetiedustelun käyttö edellyttää myös, että tietoja ei pystytä hankkimaan muilla tiedustelumenetelmillä. [49] Välttämättömyysedellytys on perusoikeussuojan kattavuudesta johtuen väljempi, jos tietoliikennetiedustelu kohdistuu pelkästään valtiollisen toimijan tai sellaiseen rinnastuvan tahon tietoliikenteeseen. Tällöin 4 §:n 2 momentin mukaan vaatimuksena on ns. tarpeellisuusedellytys, jolloin tietoliikennetiedustelun soveltamisen tulee olla tarpeen tietojen saamiseksi tiedustelun kohteena olevasta, kansallista turvallisuutta vakavasti uhkaavasta toiminnasta[50].

Tietoliikennetiedustelun kohteena voivat olla vain ne toiminnat ja tahot, jotka lain 3 §:ssä on määritelty tietoliikennetiedustelun kohteiksi. Näitä ovat esimerkiksi terrorismi, kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi sekä kansainvaltaista yhteiskuntajärjestystä vakavasti uhkaava toiminta. Tietoliikennetiedustelua koskevan lain 1 §:n 3 momentin mukaan henkilö ei ilman hyväksyttävää syytä voi joutua tietoliikennetiedustelun kohteeksi perustuen syrjiviin, henkilöön liittyviin ominaisuuksiin kuten ikään, sukupuoleen, kansalaisuuteen tai poliittiseen mielipiteeseen. Vaikka tietoliikennetiedustelussa tulee 1 §:n 2 momentin mukaan soveltaa poliisilaissa säädettyä perus- ja ihmisoikeuksien kunnioitusta, erillisellä syrjintäkiellolla pyritään vielä vahvemmin estämään tietoliikennetiedustelulle mahdollinen profilointi.[51]

Tietoliikennetiedustelulle on tietoliikennetiedustelulain 1 §:n 4 momentissa säädetty erillinen kielto kohdentamattomasta ja yleisestä tietoliikenteen seuraamisesta. Momentin tarkoituksena on estää ns. massavalvonta, jossa tiedustelun kohteeksi voi joutua periaatteessa kuka tahansa. Perustuslain 10 §:n 4 momentti, jossa säädetään luottamuksellisen viestin salaisuuden

[48] HE 202/2017 vp, s. 241.
[49] HaVM 36/2018 vp, s. 96-97.
[50] HE 202/2017 vp, s. 236.
[51] PeVL 35/2018 vp, s. 15.

rajoittamisesta, ei perustuslakivaliokunnan mukaan mahdollista massavalvonnan kaltaista yleistä ja kohdentamatonta tietoliikenteen seurantaa[52]. Tietoliikennetiedustelun kohdistaminen on mahdollista edellä kuvatulla, hakuehtojen käyttöön perustuvalla automatisoidun erottelun menetelmällä: jos tiedustelujärjestelmän läpi virtaava tietoliikenne ei vastaa ennakkoon syötettyjä ja hyväksyttyjä hakuehtoja, se ei ohjaudu jatkokäsittelyyn eikä tällaista tietoliikennettä voi myöskään palauttaa tarkasteluun myöhemmin.[53]

Sen lisäksi, että tietoliikennetiedustelulain 12 §:ssä säädetään Suomen sisäiseen viestintään kohdistuvasta tiedustelukiellosta, ei tietoliikennetiedustelua saa myöskään kohdistaa sellaiseen viestintään, josta viestinnän osapuolilla tai tiedon tallentajalla on velvollisuus tai oikeus kieltäytyä todistamasta nojautuen oikeudenkäymiskaaren 17 luvun 13-14, 16 ja 20 §:ään tai 22 §:n 2 momenttiin. Tällöin tiedustelukielto kattaa esimerkiksi oikeudenkäyntiasiamiehen ja asiakkaan tai lääkärin ja asiakkaan välisen viestinnän. Tiedustelukielloista huolimatta on kuitenkin mahdollista, että tietoliikennetiedustelulla kerätään sen piiriin kuuluvaa tietoa: esimerkiksi hakuehtoja ei hallituksen esityksen mukaan ole mahdollista määritellä siten, että ne tunnistaisivat tiedustelukiellon piiriin kuuluvan viestin eikä tällainen ohjautuisi jatkokäsittelyyn. Tästä syystä tietoliikennetiedustelulain 15 §:ssä säädetään velvollisuudesta hävittää tiedustelukiellon alainen tietoliikennetiedustelulla saatu viestintä viipymättä. Nopeaa viestin käsittelyä ja mahdollisten tiedustelukiellon alaisen viestinnän nopeaa hävittämistä edistämään on lain 13 §:ssä säädetty, että tiedustelulla haltuun saatu viestintä on tarkastettava ilman aiheetonta viivytystä[54]. Lisäksi siinä tapauksessa, että tietoliikennetiedustelun aikana Suomessa olleen henkilön viestin tai tallennetun tiedon sisältö taikka viestin tunnistamistieto on selvitetty manuaalisesti, tulee henkilölle tietoliikennetiedustelulain 20 §:n perusteella ilmoittaa häneen kohdistuneesta tietoliikennetiedustelusta.

Hävitysvelvollisuus koskee 15 §:n mukaan sellaista tietoliikennetiedustelulla saatua tietoa, joka kuuluu tiedustelukiellon piiriin tai jota ei tarvita kansallisen turvallisuuden suojaamiseksi. Suomen sisäistä tai oikeudenkäymiskaaren nojalla suojattua viestintää koskevasta kiellosta ei ole sallittua poiketa missään tilanteessa. Sellainen pykälän 3 momentissa tarkoitettu tieto, jota ei tarvita kansallisen turvallisuuden suojaamiseksi, on

[52] PeVM 4/2018 vp, s. 8.
[53] HE 202/2017 vp, s. 238.
[54] HE 202/2017 vp, s. 254.

kuitenkin mahdollista luovuttaa tietyin edellytyksin rikostorjuntaan sekä tallentaa ja säilyttää henkilötietojen käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin. [55]

Vaatimuksella hävittää edellä mainitut tiedot pyritään varmistamaan, ettei tiedusteluviranomaiset voi käyttää tietoja hyödyksi toiminnassaan. Myös hävitetyistä viesteistä jää kuitenkin tietoja asiakirjoihin, jolloin laillisuusvalvonnan ja oikeusturvan kannalta on tärkeää, että jokainen viestin hävittäminen ja syy sille dokumentoidaan. Hävittämisestä vastaa tietoliikennetiedustelun tekninen toteuttaja eli puolustusvoimien tiedustelulaitos tai toimeksiantaja eli suojelupoliisi siinä tapauksessa, että tiedot on ehditty sille toimittaa. Tiedustelukiellon alainen tieto on usein huomattavissa vasta viestin sisältöä selvitettäessä, jolloin on oletettavaa, että hävittämisestä huolehtii pääsääntöisesti suojelupoliisi.[56]

Tiedustelun kohteelle tulee ilmoittaa kirjallisesti viimeistään vuoden kuluttua tiedustelun loppumisesta, ellei tuomioistuin myönnä suojelupoliisin päällystöön kuuluvan virkamiehen pyynnöstä ilmoittamiselle lykkäystä esimerkiksi kansallisen turvallisuuden nojalla. Lykkäystä on mahdollista myöntää enintään kaksi vuotta kerrallaan. Tuomioistuimen on myös mahdollista päättää ilmoituksen tekemättä jättämisestä, jos se nähdään välttämättömäksi kansallisen tai valtion turvallisuuden varmistamiseksi tai terveyden ja hengen suojaamiseksi. Jos tieto on hävitetty kuten tietoliikennetiedustelulain 9 §:ssä tai 15 §:ssä säädetään, ei velvollisuutta ilmoittamiselle ole. Ilmoittamisvelvollisuus ei myöskään perusoikeussuojan kattavuudesta johtuen koske vierasta valtiota tai sellaiseen rinnastuvaa tahoa.[57]

Tietoliikennetiedustelu on tiedustelumenetelmänä Suomessa täysin uusi. Erikoisuutena verrattuna muihin sähköiseen viestintään kohdistuviin tiedustelumenetelmiin, kuten televalvontaan ja –kuunteluun, on, ettei se kohdistu sellaiseen laitteeseen, joka on mahdollista yksilöidä ennakolta. Tämä nostaa riskiä sivullisten mahdollisuudesta joutua tahattomaksi tietoliikennetiedustelun kohteeksi. Perus- ja ihmisoikeuksien suojan kannalta keskeistä on, millaisia valvontakeinoja tiedustelumenetelmiin ja niitä toteuttaviin tahoihin kohdistuu: tiedustelutoimivaltuuksien laajetessa on tarpeellista huolehtia myös riittävän tehokkaista ja riippumattomista valvontaelimistä. Asianmukaisen valvonnan vaatimus johtuu niin kansallisesta perusoikeussysteemistä kuin kansainvälisistä ihmisoikeussopimuksista.

[55] HE 202/2017 vp, s. 256. Tässä tarkoitetuista edellytyksistä säädetään poliisilain 5 a luvun 44 §:ssä sekä 45 §:n 1 momentissa.
[56] HE 202/2017 vp, s. 256
[57] HE 202/2017 vp, s. 259-260.

Luottamuksellisen viestin suojaan on mahdollista puuttua uusilla toimivaltuuksilla entistä syvemmin, joten vaatimus tarpeellisista oikeussuojakeinoista ja oikeusturvasta korostuu. Tiedustelutoiminnan ulkoista valvontaa hoitamaan perustettiin uudet viranomaiset, sillä Suomessa ei ollut erillistä tahoa, jonka tehtävänä oli yksinomaan valvoa tiedustelutoimintaa siinä muodossa, missä sitä harjoitettiin.[58]

2.2. Tiedustelutoiminnan valvonta

2.2.1. Tiedusteluvalvontavaltuutettu

Tiedusteluvalvontavaltuutettu [59] vastaa omalta osaltaan tiedustelutoiminnan ulkoisesta laillisuusvalvonnasta sekä suojelupoliisin muun toiminnan valvonnasta. Tiedusteluvalvontavaltuutettu on itsenäinen ja riippumaton valvontaelin, joka toimii tietosuojavaltuutetun toimiston yhteydessä. Tiedusteluvalvontavaltuutetun virassa on kyse laillisuusvalvontatehtävästä, joka edellyttää oikeudellista asiantuntemusta, ja täten tiedusteluvalvontavaltuutetun tulee tiedustelutoiminnan valvonnasta annetun lain (jäljempänä valvontalaki) 6 §:n 2 momentin mukaan olla suorittanut oikeustieteen ylempi korkeakoulututkinto muulta oikeustieteen alalta kuin kansainvälisestä tai vertailevasta oikeustieteestä. Lisäksi tiedusteluvalvontavaltuutetulta edellytetään perehtyneisyyttä tehtäväalaan ja hänellä tulee olla erityistehtävän hoitamiseen tarvittavaa asiantuntemusta ja osaamista, kuten perus- ja ihmisoikeusjuridiikan sekä laillisuusvalvonnan vahvaa osaamista. Tehtävässä edellytetään myös käytännössä osoitettua johtamistaitoa. [60] Perustuslakivaliokunta pitää tärkeänä, että tiedusteluvalvontavaltuutettu on myös henkilöllisesti riippumaton tiedusteluorganisaatioista[61], mistä johtuen tehtävään voidaan valvontalain 6 §:n 3 momentin mukaan nimittää vain sellainen henkilö, jolla ei ole valvontatehtävän asianmukaista ja riippumatonta hoitamista vaarantavia sidonnaisuuksia.

Erityisvaltuutettujen sekä ylimpien laillisuusvalvojien tehtäväkenttä ei kapene tiedusteluvalvontavaltuutetun viran myötä. Esimerkiksi eduskunnan oikeusasiamies valvoo

[58] HE 199/2017 vp, s. 32
[59] Valtioneuvosto nimitti yleisistunnossa 17.4.2019 ensimmäiseksi tiedusteluvalvontavaltuutetuksi Kimmo Hakosen. Hakonen nimitettiin ajalle 1.5.2019-30.4.2024. Ks. Valtioneuvoston yleisistunto 17.4.2019: Tiedusteluvalvontavaltuutetun nimittäminen,
[60] HE 199/2017 vp, s. 47; PeVM 9/2018 vp, s. 7.
[61] PeVM 9/2018 vp, s. 7.

salaista tiedonhankintaa ja salaisia pakkokeinoja kuten ennenkin, ja valvoo tiedusteluvalvontavaltuutetun toimintaa samalla tavalla kuin muitakin erityisvaltuutettuja.[62]

Tiedusteluvalvontavaltuutetun tehtävänä on valvontalain 7 §:n 1 ja 2 kohdan mukaan valvoa tiedustelumenetelmien, tiedustelutiedon ja muun tiedustelutoiminnan käytön laillisuutta sekä perus- ja ihmisoikeuksien toteutumista. Tiedusteluvalvontavaltuutetulla on siis oikeus valvoa myös muuta tiedustelutoimintaa kuin sitä, mistä siviili- ja sotilastiedustelulaeissa tiedustelumenetelmistä säädetään. Valvonnan alaan kuuluu täten esimerkiksi avointen lähteiden tiedustelu sekä sen tiedon valvonta, minkä varassa tiedustelua lähdetään toteuttamaan, mihin tiedustelua saatua tietoa käytetään ja miten tiedusteluoperaatio päättyy. Tiedusteluvalvontavaltuutetun tulee myös 7 §:n 4 kohtaan perustuen seurata ja arvioida oman toimialansa lainsäädännön toimivuutta ja antaa kehittämisehdotuksia niillä aihealueilla, missä kokee tarpeelliseksi. Uudessa tiedustelulakipaketissa säädettiin monista uusista toimivaltuuksista sekä kokonaan uutta lainsäädäntöä, joten toimivuuden tarkastelu ja kehittäminen on tärkeää. [63]

Tiedusteluvalvontavaltuutetulle on valvontalain 15 §:ssä säädetty oikeus keskeyttää tai lopettaa tiedustelumenetelmän käyttö. Tiedusteluvalvontavaltuutetulla on oikeus määrätä tiedustelumenetelmän käyttö keskeytettäväksi tai lopetettavaksi jos tiedusteluviranomainen on tiedusteluvalvontavaltuutetun näkökulmasta menetellyt lainvastaisesti tiedustelutoiminnassa. Keskeytys- ja lopettamisoikeus on erityisen vahva toimivaltuus laillisuusvalvonnan kentässä ja ne on tarkoitettu viimesijaisiksi keinoiksi. Valtuutetun tulee siis ensin pyrkiä muiden hänelle säädettyjen toimivaltuuksien avulla lainvastaisen menettelyn lopettamiseen tai keskeyttämiseen. Oikeus määrätä tiedustelumenetelmä lopetettavaksi tai keskeytettäväksi koskee kaikkia tiedustelumenetelmiä, mutta tuomioistuinluvan vaatineen tiedustelumenetelmän käyttöä koskeva määräys on väliaikainen ja se käsitellään loppuun tuomioistuimessa. Muussa tapauksessa, kuten esimerkiksi suojelupoliisin päällikön myöntämään lupaan perustuvassa tiedustelumenetelmässä, tiedusteluvalvontavaltuutetun päätös keskeyttämisestä tai lopettamisesta on itsenäinen.[64]

Jos tiedustelumenetelmän käyttö vaatii tuomioistuinluvan, kuten esimerkiksi tietoliikennetiedustelun käyttö, tiedusteluvalvontavaltuutetun antama keskeyttämismääräys ja lopettamismääräys ovat 15 §:n 2 momentin mukaan väliaikaisia, ja asia käsitellään loppuun

[62] HE 199/2017 vp, s. 37.
[63] HE 199/2017 vp, s. 48-49.
[64] HE 199/2017 vp, s. 59.

tuomioistuimessa. Tiedusteluvalvontavaltuutetun tai hänen määräämänsä virkamiehen on 3 momentin nojalla oltava tuomioistuinkäsittelyssä läsnä. Väliaikainen määräys voi tulla kyseeseen esimerkiksi tilanteessa, jossa lupa-asian käsittelyssä tuomioistuimelle on annettu väärää tietoa, tai tiedustelua harjoitetaan luvan vastaisesti.[65]

Tuomistuinluvan vaatineiden tiedustelumenetelmien keskeyttämisen tai lopettamisen käsittely tuomioistuimessa perustuu poikkeukselliseen vahvaan laillisuusvalvonnan muotoon, eikä tällä puututa tuomioistuimen toimivaltaan tai eduskunnan oikeusasiamiehen sekä valtioneuvoston oikeuskanslerin suorittamaan valvontaan. Tiedustelumenetelmän käytön keskeyttäminen tai lopettaminen ei merkitse sitä, että tiedusteluvalvontavaltuutettu arvioi tuomioistuimen myöntämää lupaa uudelleen tai että hänellä olisi toimivalta muuttaa tuomioistuimen ratkaisua. Tiedusteluvalvontavaltuutetun tehtävänä on nimenomaisesti valvoa myönnettyjen lupien noudattamista, ja tämän vuoksi tiedusteluviranomaisen tulee toimittaa tiedusteluvalvontavaltuutetulle tieto myönnetyistä luvista mahdollisimman pian sen jälkeen, kun tuomioistuin on tehnyt päätöksen.[66]

Harkinta koskien väliaikaisen määräyksen antamista ei voi olla sellaista tiedustelumenetelmän edellytyksiä tai niiden puutetta koskevaa arviointia, jota tuomioistuin on jo lupahakemusta käsitellessään tehnyt.[67] Vastaavasti tiedusteluvalvontavaltuutetun tiedonsaantioikeus ei ulotu suoraan tuomioistuimeen, vaan tiedusteluviranomaisella on velvollisuus ilmoittaa viranomaispäätöksistä ja tuomioistuinpäätöksistä koskien tiedustelumenetelmiä. Myöskään selvitys- ja tarkastusoikeus kohdistu tuomioistuimeen. [68] Tiedusteluvalvontavaltuutetulla on kuitenkin oikeus valvontalain 14 ja 15 §:n perusteella kannella tuomioistuimen päätöksestä hovioikeudelle. Kantelu voi koskea esimerkiksi tiedustelutoimenpiteitä, niiden johdosta tehtävän ilmoituksen lykkäämistä tai tekemättä jättämistä.[69]

Tiedusteluvalvontavaltuutetun tehtäviin kuuluu 7 §:n 3 kohdan mukaan oikeusturvan toteutumisen ja siihen liittyvien hyvien käytäntöjen edistäminen tiedustelutoiminnassa. Oikeusturvan edistämiseksi yksilön on mahdollista tehdä tiedusteluvalvontavaltuutetulle kanteluita tai tutkimispyyntöjä, joista säädetään lain 11 ja 12 §:ssä. [70] Kantelu- ja tutkimispyyntömenettelyillä on tarkoitus täydentää valtuutetun laillisuusvalvontaa sekä tuoda

[65] HE 199/2017 vp, s. 60.
[66] HE 199/2017 vp, s. 48.
[67] HE 199/2017 vp, s. 60.
[68] HE 199/2018 vp, s. 52-53.
[69] PeVM 9/2018 vp, s. 6.
[70] HE 199/2017 vp, s. 49.

tiedustelutoimeen tuomioistuimen ennakollisen lupamenettelyn ja suojelupoliisin sisäisen valvonnan rinnalle muita oikeusturvajärjestelyjä.[71]

Kantelun voi tehdä henkilö, joka näkee, että tiedustelutoimintaa harjoitettaessa hänen oikeuksiaan on rikottu tai muutoin toimittu lainvastaisesti. Tutkimispyynnön voi tehdä henkilö, joka on saanut ilmoituksen häneen kohdistuneesta tiedustelutoiminnasta tai epäilee, että häneen on kohdistunut tiedustelutoimintaa. Tiedusteluvalvontavaltuutettu ottaa kantelun käsittelyyn, jos hän katsoo asian kuuluvan hänen laillisuusvalvontansa alaan ja näkee tutkimisen muuten tarpeelliseksi. Valtuutettu arvioi tutkinnan tarpeen jokaisen kantelun kohdalla itsenäisesti ja tapauskohtaisesti. Vastaavaa menettelyä sovelletaan soveltuvin osin myös tutkimispyynnön kohdalla. Näiden toimien avulla tiedusteluvalvontavaltuutettu toteuttaa jälkikäteistä laillisuusvalvontaa. Ennen asian ratkaisua tiedusteluvalvontavaltuutetun tulee 13 §:ään perustuen varata valvottavalle taholle tilaisuus tulla kuulluksi.[72]

Tiedusteluvalvontavaltuutettu laatii vuosittain toiminnastaan salaiseen ja julkiseen osaan jakautuvan vuosikertomuksen, jonka hän antaa kokonaisuudessaan eduskunnalle, valtioneuvostolle sekä eduskunnan oikeusasiamiehelle. Kertomuksen julkisessa osassa tiedusteluvalvontavaltuutettu voi esimerkiksi yleisluontoisesti esittää kertomusvuoden toimintansa ja tuoda esiin perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa. Julkisessa osassa tiedusteluvalvontavaltuutettu voi myös nostaa esiin huomioituja kehittämistarpeita.[73]

2.2.2. Tiedusteluvalvontavaliokunta

Tiedusteluvalvontavaliokunta hoitaa tiedustelutoiminnan sekä suojelupoliisin muun toiminnan parlamentaarista valvontaa. Tiedusteluvalvontavaliokunta on yksi eduskunnan valiokunnista, mutta sillä on tehtävänsä vuoksi pienempi jäsenmäärä kuin muilla valiokunnilla. [74] Parlamentaarisen valvonnan on tarkoitus vahvistaa tiedustelutoiminnan hyväksyttävyyttä arvioimalla ja seuraamalla sitä, miten perus- ja ihmisoikeuksien kunnioittaminen, turvallisuusympäristön muutokset sekä yhteiskunnan kokonaisetu huomioidaan tiedustelutoiminnassa[75].

[71] HE 199/2017 vp, s. 38.
[72] HE 199/2017 vp, s. 54-55.
[73] HE 199/2017, s. 66.
[74] PNE 1/2018 vp, s. 20.
[75] PNE 1/2018 vp, s. 13.

Tiedusteluvalvontavaliokunnan tehtävistä säädetään eduskunnan työjärjestyksen 31 b §:ssä. Tehtäviin kuuluu pykälän 2 momentin 1 kohdan mukaan tiedustelutoiminnan painopisteiden seuraaminen ja arvioiminen, jota se toteuttaa saamiensa selvitysten sekä oman valvontatoimintansa pohjalta. Tiedusteluvalvontavaliokunta voi tarvittaessa antaa näkemyksensä painopisteiden asettamisesta valtioneuvoston tai asianomaisen ministeriön tietoon laatimalla lausunnon jostakin tietystä asiasta. Jos tilanne on erityisen merkityksellinen, voi valtiokunta laatia asiasta mietinnön. Tällöin tiedustelutoiminnan painopisteistä voidaan keskustella eduskunnan täysistunnossa ja tehdä päätös, esittääkö eduskunta mahdollisesti asiasta oman kannanottonsa. Momentin 2 kohdan mukaan tehtäviin kuuluu myös tiedustelutoiminnan asianmukaisuuden ja tarkoituksenmukaisuuden arviointi, jota tiedusteluvaliokunta voi harjoittaa esimerkiksi arvioimalla, miten tiedustelutoiminnalle asetetuttuja painopisteitä on huomioitu ja miten toiminnalle määritellyt tavoitteet on saavutettu. [76]

Momentin 3 kohdassa säädetään tiedusteluvalvontavaliokunnan tehtävästä ”seurata ja edistää perus- ja ihmisoikeuksien toteutumista tiedustelutoiminnassa”. Seuraamistehtäväänsä täyttäessään valiokunta toteuttaa ydintehtäväänsä, eli tiedustelutoiminnan hyväksyttävyyden ja suhteellisuuden valvontaa. Keskeistä on, että valiokunta pyrkii toiminnassaan arvioimaan perus- ja ihmisoikeuksiin puuttuvien toimien ja puuttumisen avulla torjuttavan uhan vakavauuden tai päämääränä olevan hyödyn tärkeyden ja tarpeellisuuden välistä oikeasuhtaisuutta. Perus- ja ihmisoikeuksien noudattamista tiedustelutoiminnassa valiokunta voi edistää esimerkiksi ”kiinnittämällä hallituksen tai asianomaisen ministeriön huomiota esimerkiksi tiedusteluhenkilöstön perus- ja ihmisoikeuskoulutuksen laatuun ja laajuuteen”.[77]

Jotta valvonnan kokonaisuus voidaan järjestää asianmukaisesti, tiedusteluvalvontavaliokunta osallistuu tiedusteluvalvontavaltuutetun valintaan. Perustuslakivaliokunta on mietinnössään korostanut, että valtuutetun virkaa täytettäessä valtioneuvoston tulee varata valiokunnalle tarpeeksi aikaa muodostaa mielipide, jotta se voi ottaa asiaan asianmukaisesti kantaa ja halutessaan esimerkiksi haastatella hakijoita. [78] Tiedusteluvalvontavaliokunnan sekä – valtuutetun yhteistyö on keskeisessä roolissa tarkasteltaessa valvonnan kokonaisuuden toimivuutta ja tehokkuutta. Tiedusteluvalvontavaliokunnalla ei ole tietojen ja selvitysten saamiseen käytössään samankaltaisia keinoja kuin tiedusteluvalvontavaltuutetulla, joten

[76] PNE 1/2018 vp, s. 33.
[77] PNE 1/2018 vp, s. 33-34.
[78] PeVM 10/2018 vp, s. 11.

tiedusteluvalvontavaltuutetun on tärkeää auttaa tällaisten tarvittavien selvitysten ja tietojen hankkimisessa. [79]

Tärkeä osa tiedusteluvalvontavaliokunnan työtä on momentin 4 kohdassa säädetty tiedusteluvalvontavaltuutetun kertomusten käsittely ja sen pohjalta mietinnön valmisteleminen täysistunnolle. Tiedusteluvalvontavaltuutettu voi antaa valiokunnalle vuosikertomusten lisäksi myös erilliskertomuksia ja lisäksi tuoda havaintojaan valiokunnan tietoon selvityksen ja raporttien kautta. Valiokunnan tehtäviin kuuluu lisäksi 5 momentin mukaan käsitellä ne valvontahavainnot, jotka tiedusteluvalvontavaltuutettu on katsonut tarpeen saattaa valiokunnan tietoon. Tiedusteluvalvontavaliokunta saa myös 31 b §:n 3 momentin perusteella ottaa oma-aloitteisesti käsiteltäväksi omaan toimialaansa kuuluva asia ja jos se katsoo asian laadun sitä vaativan, laatia asiasta mietintö täysistunnolle.[80]

2.2.3. Suojelupoliisin sisäinen valvonta

Suojelupoliisin suorittama sisäinen laillisuusvalvonta voidaan kohdistaa toimintaan, jota ulkopuolisen kontrollin on hankalampi tavoittaa sekä perus- ja ihmisoikeuksien toteutumiseen liittyviin seikkoihin ja sitä voi kohdentaa tarkemmin esimerkiksi jo havaittujen ongelmien perusteella. Laillisuusvalvonnassa havaituista asioista tehdään johdon toimesta tarvittavat johtopäätökset ja toimenpiteet. Laillisuusvalvonnan kohteiden käsittelyllä, virheiden myöntämisellä ja niistä syntyneillä toimenpiteillä lisätään viranomaisen toiminnan uskottavuutta. Tämänkaltaisen valvonnan päämäärä ei ole rangaista, mutta lainvastaiseen menettelyyn tulee aina puuttua ja asia on selvitettävä sen vaatimassa laajuudessa ja jos asian laatu sitä vaatii, on toiminta saatettava virkamies- tai rikosoikeudelliseen menettelyyn.[81]

Tiedusteluvalvontavaltuutetun virka ei muuta sisäministeriön tiedustelutoimintaan liittyvää roolia eikä sisä- ja puolustusministeriöin keskinäistä työnjakoa. Vaikka ulkoisen laillisuusvalvonnan ei ole tarkoitus toimia sisäisen laillisuusvalvonnan rajoittajana, voidaan niitä koordinoida keskinäisesti. Sisäisen laillisuusvalvojan on tarkoituksenmukaista saattaa tiedusteluvaltuutetun tietoon suunnittelemansa tarkastukset. [82] Suojelupoliisin organisaatio toimii sisäministeriön alaisuudessa, jolloin vastuu sen valvonnasta on sisäministeriöllä. [83] Siviilitiedustelu kuuluu suojelupoliisin tehtäviin, ja suojelupoliisin laillisuusvalvonnan

[79] HE 199/2017 vp, s. 49.
[80] PNE 1/2018 vp, s. 34.
[81] Sisäministeriön ja sen hallinnonalan laillisuusvalvontaohje 2016, s. 3. Laillisuusvalvontaohjeen voimassaoloaikaa on jatkettu 30.6.2020 saakka; ks. Sisäministeriön internetsivut: Ministeriö: Laillisuusvalvonta.
[82] HE 199/2017 vp, s. 37.
[83] HE 199/2017 vp, s. 10.

asianmukaisesta järjestämisestä sisäministeriössä vastaa sisäministeriön poliisiosasto. Suojelupoliisin päälliköllä on vastuu laillisuusvalvonnan järjestämisestä, resursoinnista ja kehittämisestä.[84]

Suojelupoliisin sisäiseen valvontaan kuuluu laillisuusvalvonta, laadunvalvonta sekä sisäinen tarkastus.[85] Sisäisellä laillisuusvalvonnalla toteutetaan hyvää hallintoa sekä edistetään perus- ja ihmisoikeuksien toteutumista. Sen tarkoituksena on lisäksi edistää sisäministeriölle ja sen hallinnonalalle asetettuja tavoitteita sekä ”ylläpitää ja parantaa viranomaistoiminnan laatua.” Sisäisellä laillisuusvalvonnalla valvotaan viranomaistoiminnan, virkavelvollisuuksien ja ohjeistuksen noudattamisen lainmukaisuutta ja sitä toteutetaan hallintokanteluiden, kansalaiskirjeiden ja omien aloitteiden käsittelyllä, laillisuusvalvontatarkastuksilla sekä valvomalla henkilötietojen käsittelyä. Sisäinen laillisuusvalvonta tuottaa ajantasaista ja riittävää tietoa viranomaisen toiminnan lainmukaisuudesta, jota käytetään viranomaisen johdossa päätöksenteon tukena. Sillä tulee pyrkiä estämään virheiden syntyminen ennakkoon ja paljastaa sekä saada asianmukaiseen menettelyyn lainvastainen tai virheellinen toiminta mahdollisimman aikaisin.[86]

Reaaliaikaisesti toteutettavan sisäisen valvonnan kohteena voi olla esimerkiksi se, käytetäänkö tiedustelumenetelmää juuri siihen kohteeseen, johon sitä on vaadittu käytettäväksi. Toinen valvonnan kohde on tiedustelumenetelmien yleiset ja erityiset edellytykset sekä se, miten tiedustelun yleisiä periaatteita noudatetaan. Sisäinen valvonta kohdistuu myös tiedustelumenetelmän käyttöä valvovaan virkamieheen. Tiedustelumenetelmän käytön edellytysten arvioinnin on jatkuttava koko sen käytön ajan, jolloin lupapäätöstä on tärkeää tarkistaa, jos tiedusteluun liittyvät olosuhteet muuttuvat. Tietoliikennetiedustelua koskien sisäinen valvonta voi kohdistua esimerkiksi siihen, että hakuehtoja noudatetaan. Tärkein tietoliikennetiedustelua koskeva sisäisen valvonnan kohde on massavalvonnan kiellon noudattaminen, jota myös perustuslakivaliokunta korostaa.[87]

Suojelupoliisin suorittamassa salaisessa tiedonhankinnassa se noudattaa tietyin täsmennyksin Poliisihallituksen määräystä koskien salaisen tiedonhankinnan järjestämistä, käytöstä ja valvontaa. Määräykseen perustuen suojelupoliisiin on muodostettu vastuuhenkilöjärjestelmä, jossa tehtävään nimetyt vastuuhenkilöt valvovat salaista tiedonhankintaa tarkastamalla

[84] Sisäministeriön ja sen hallinnonalan laillisuusvalvontaohje 2016, s. 16-17.
[85] HE 202/2017 vp, s. 37.
[86] Sisäministeriön ja sen hallinnonalan laillisuusvalvontaohje 2016, s. 3.
[87] Lohse & Viitanen 2018, s. 164. Ks. myös PeVL 35/2018 vp, s. 20; PeVM 4/2018 vp, s. 8.

esimerkiksi tiedonhankintakeinoista tehtyjä kirjauksia. Puolivuosittain suojelupoliisin laillisuusvalvoja tarkastaa kaikki salaiset tiedonhankintakeinot, jotka on hallinnoitu salaisten pakkokeinojen asianhallintajärjestelmän kautta.[88] Nämä järjestelyt ovat osoittautuneet toimiviksi ja on luultavaa, että niiden soveltaminen ulotetaan myös tiedustelumenetelmiin.[89]

[88] HE 199/2017 vp, s. 11.
[89] Lohse & Viitanen 2019, s. 158.

3. Yksityiselämän ja luottamuksellisen viestin salaisuuden suoja

3.1. Yksityiselämän suoja ja sen rajoittaminen

3.1.1. Yksityiselämän suojan ulottuvuus

Perustuslain 10 §:n 1 momentissa turvataan jokaiselle yksityiselämä, kunnia ja kotirauha. Lisäksi henkilötietojen suojasta säädetään erikseen [90]. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuuden loukkaamattomuudesta säädetään 10 §:n 2 momentissa. Yksityiselämän suojan perusta on ajatuksessa, että yksilöllä on oikeus elää elämänsä siten, ettei siihen mielivaltaisesti ja aiheettomasti puutu viranomaiset tai muut ulkopuoliset tahot. Yksityiselämän käsitteen voidaan nähdä kattavan henkilön koko yksityinen piiri, ja käsite pitää sisällään myös yksilön perhe-elämän, vaikka termiä ei ole säännöksessä erikseen mainittu.[91] Yksityiselämän piiriin kuuluvien asioiden määritteleminen ei ole yksiselitteistä, sillä säännöksen suojan kohteet ovat päällekkäisiä: esimerkiksi puuttuminen yksilön kotirauhan piiriin merkitsee usein myös puuttumista tämän yksityiselämään. [92]

Kuten edellä todettu, Suomi on sitoutunut Euroopan ihmisoikeussopimukseen ja täten yksilö saa turvaa myös siinä säädetyistä oikeuksista. Euroopan ihmisoikeussopimuksessa yksityis- ja perhe-elämän sekä kodin ja kirjeenvaihdon kunnioituksesta säädetään 8 artiklassa. Artikla antaa laajan suojan monelle eri elämän osa-alueelle, ja se ilmentää Euroopan tuomioistuimen oikeuskäytännön dynaamisuutta, sillä sen tulkinta on ollut ajan saatossa joustavaa ja kattavuus laajentunut merkittävästi. Artiklan keskeinen tarkoitus on turvata yksilön yksityis- ja perhe-elämä siten, ettei siihen viranomaisen toimesta puututa mielivaltaisesti. [93] Myöskään Euroopan ihmisoikeussopimuksen turvaamalle yksityiselämän suojalle ei voi antaa tyhjentävää sisältöä. Euroopan ihmisoikeussopimuksen turvaamaan yksityiselämän suojan piiriin kuuluu ainakin koskemattomuus ruumiillisessa ja psykologisessa tarkoituksessa; henkilön kuva, nimi ja maine; identiteetti; henkilökohtainen kehitys sekä sukupuolinen ja seksuaalinen suuntautuminen.[94] Käsite on kuitenkin Euroopan ihmisoikeustuomioistuimen

[90] Henkilötietojen suojasta säädetään tietosuojalaissa (1050/2018), jota sovelletaan rinnakkain Euroopan unionin tietosuoja-asetuksen (2016/679) kanssa. Henkilötietojen käsittelystä säädetään lisäksi esimerkiksi laissa henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018) ja laissa henkilötietojen käsittelystä poliisitoimessa (616/2019). Henkilötietojen suoja ei ole itsenäinen perusoikeus vaan se nähdään osana yksityisyyden suojaa. Ks. Neuvonen 2014, s. 41.
[91] HE 309/1993 vp, s. 52-53.
[92] Viljanen V-P II.
[93] Hirvelä & Heikkilä 2017, s. 628.
[94] Pellonpää et al. 2018, s. 785-786.

oikeuskäytännössä laaja ja kiinnittyy usein muihin 8 artiklassa turvattuihin oikeuksiin eli kirjeenvaihdon, kodin ja perhe-elämän kunnioitukseen eikä tuomioistuin ole aina nähnyt edes aiheelliseksi erottaa käsitteiden antaman suojan piiriä.[95]

Perustuslaissa turvattu yksityiselämän suoja on mahdollista mieltää enemmän immateriaaliseksi verrattuna esimerkiksi perustuslain 7 §:ään, jossa turvataan oikeus elämään ja henkilökohtaiseen vapauteen ja koskemattomuuteen.[96] Perusoikeusuudistuksessa yksityiselämän suojan käsite omaksuttiin Suomen perustuslakiin pitkälti Euroopan ihmisoikeussopimuksen 8 artiklan kautta. Käsitteen pohjautuessa ihmisoikeussopimukseen on aiheellista, että tulkittaessa kyseistä säännöstä nojataan keskimääräistä enemmän ihmisoikeussopimuksen soveltamiskäytäntöön. Tämän perusteella yksityiselämän suojan alaan voidaan katsoa kuuluvan myös henkilökohtainen identiteetti sekä moraalinen ja fyysinen koskemattomuus niiltä osin, kun ne eivät 7 §:ssä täysin toteudu.[97]

Yksilön kunnian suoja on yksi perustuslain 10 §:n 1 momentissa turvatuista, yksityiselämään sisältyvistä perusoikeuksista. Yksilön kunnian suoja toimii pitkälti toisten henkilöiden sekä joukkoviestinnän sananvapauden rajoittajana ja näyttäytyy täten rikoslain kautta. Se on oikeus, johon yksilö voi vedota silloin, kun kokee tätä oikeutta loukatun ja julkisella vallalla on velvollisuus selvittää, onko vaatimus perusteltu.[98] Yksilön kunnian suojaa ei erikseen mainita Euroopan ihmisoikeussopimuksessa, mutta kuten yllä todettiin, sisältyy artiklan turvaamiin oikeuksiin mm. yksilön maine.

Perhe-elämän suoja on jätetty mainitsematta perustuslain 10 §:n 1 momentissa ”perhe” käsitteen määrittelemisen hankaluuden vuoksi, mutta sen katsotaan kuitenkin sisältyvän yksityiselämän suojan piiriin[99]. Euroopan ihmisoikeussopimuksen 8 artiklan 1 kohdassa perhe-elämän suoja mainitaan erikseen artiklan suojan kohteena. Perhe-elämän suojan piiriin kuuluu Euroopan ihmisoikeustuomioistuimen tulkinnassa ensisijaisesti ydinperhe eli sellainen perhe, joka tosiasiassa elää yhdessä. Kuitenkaan, kuten yksityiselämän käsitteelle, ei perhe-elämän käsitteelle voi antaa tyhjentävää määritelmää, vaan perhe-elämän olemassaolo voi olla riippuvainen tapauksen olosuhteista. Käsitettä koskeva tulkinta on seurannut perhe-elämän

[95] Hirvelä & Heikkilä 2017, s. 630.
[96] Neuvonen 2014, s. 38.
[97] Neuvonen 2014, s. 38-39 viitaten Viljanen 2011, s. 393.
[98] Neuvonen 2014, s. 39.
[99] HE 309/1993 vp, s. 53.

muuttuneita käsityksiä ja laajentunut sisältämään myös muunlaisia parisuhteen ja perhe-elämän muotoja kuin perinteisen, avioliittoon pohjautuvan ydinperheen.[100]

Kotirauhan suojan ydinalueena on henkilön asunto[101], mutta kotirauhan suojan on tulkittu ulottuvan kaikkiin asumisen tiloihin kuten hotellihuoneisiin ja matkailuautoihin. Perustuslaissa määritelty kotirauha painottuu pysyvään asumiseen tarkoitettuihin tiloihin, ja täten eroaa laajuudeltaan esimerkiksi rikoslaissa tarkoitetusta kotirauhasta. [102] Euroopan ihmisoikeustuomioistuimen tulkinnassa ”koti” käsite viittaa yleensä henkilön vakituiseen asuntoon eli sellaiseen fyysisesti määriteltävän paikkaan, jossa vietetään perhe- ja yksityiselämää. Kodin määritelmä ei ole riippuvainen jäsenvaltion kansallisesta lainsäädännöstä, vaan tuomioistuin tulkitsee käsitettä sen autonomisen tulkinnan mukaisesti. Koti-käsitteen sisältöön vaikuttavat tosiasialliset olosuhteet sekä riittävät ja jatkuvat yhteydet tiettyyn paikkaan.[103]

Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuuden loukkaamattomuus on osa yksityiselämän suojan kokonaisuutta [104]. Tietoliikennetiedustelulla puututaan erityisesti luottamuksellisen viestin salaisuuteen, ja perustuslakivaliokunta katsoi lainsäädäntövaiheessa, että uutta lainsäädäntöä tulee arvioida erityisesti kyseisen momentin kannalta [105]. Uusi rajoituslauseke määrittää tulevaisuudessa rajoituksen sallittavuutta mahdollisesti myös muussa toiminnassa, jolloin on tärkeää, että luottamuksellisen viestin salaisuutta turvataan riittävästi liialta rajoittamiselta[106].

Euroopan ihmisoikeussopimuksen 8 artiklan turvaama kirjeenvaihdon kunnioitus kattaa perinteisen kirjeenvaihdon, puhelinliikenteen sekä tietoliikenteen välityksellä tapahtuvan kommunikoinnin, kuten sähköpostiviestien vaihdon. Kirjeenvaihdon suojan kunnioituksen päämääränä on taata yksilölle oikeus kommunikoida muiden kanssa ilman, että ulkopuoliset puuttuvat siihen tai sensuroivat sitä. [107]

---

[100] Hirvelä & Heikkilä 2017, s. 747. Perhe-elämän käsitteestä ks. esim. Van der Heijden v. the Netherlands (3.12.2012), kohta 50.
[101] HE 309/1993 vp, s. 53.
[102] Viljanen V-P II.
[103] Hirvelä & Heikkilä 2017, s. 814. Kodin määritelmästä ks. esim. Gillow v. the United Kingdom (24.11.1986), kohta 46 ja tosiasiallisten olosuhteiden vaikuttamisesta termin sisältöön esim. Giacomelli v. Italy (2.11.2006), kohta 76.
[104] HE 198/2017 vp, s. 4.
[105] PeVL 35/2018, s 4.
[106] PeVM 4/2018 vp, s. 4-5.
[107] Hirvelä & Heikkilä 2017, s. 835-836.

Perustuslain säännös koskien luottamuksellisen viestin salaisuutta turvaa yleisesti luottamuksellisen viestin salaisuuden riippumatta sen välitystavasta ja koskee niin viestin lähettäjää kuin sen vastaanottajaakin. Kuten Euroopan ihmisisoikeussopimuksessa, myös perustuslaissa pykälän keskeinen tarkoitus on ”[…]suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta”, mutta se antaa suojaa myös muille viestiä koskeville tiedoille, jotka voivat vaikuttaa viestin luottamuksellisuuden säilymiseen. Tällaisia tietoja ovat esimerkiksi puhelun tunnistamistiedot.[108]

Luottamuksellisen viestin salaisuuden suojan voidaankin katsoa jakaantuvan kahteen elementtiin: viestin sisältöön sekä tunnistamistietoihin, eli tietoon viestinnän tapahtumista ja osapuolista.[109] Viestin sisällön on nähty muodostavan luottamuksellisen viestin suojan ydinalue, ja tunnistamistietojen katsotaan sijoittuvan kyseisen perusoikeuden ns. reuna-alueelle. Luottamuksellisen viestin salaisuuden suoja kattaa siis myös tunnistamistiedot, mutta niiden paljastumisen ei ole perinteisesti katsottu olevan niin syvällistä puuttumista luottamuksellisen viestin salaisuuteen kuin viestin sisällön paljastumisen.[110]

Viestin sisällön ja tunnistamistietojen jaottelu ydin- ja reuna-alueeseen ei ole kuitenkaan absoluuttista, vaan siinä tulee ottaa huomioon myös rajoituksen merkittävyys. Esimerkiksi edellä luvussa 2.1. kuvatun ilmoitusvelvollisuuden suunniteltiin hallituksen esityksessä koskevan vain tilanteita, joissa viestin sisältö on selvitetty manuaalisesti rajaten tunnistamistietojen käsittelyn ilmoitusvelvollisuuden ulkopuolelle. Tätä arvioidessaan perustuslakivaliokunta näki tämän kuitenkin tärkeäksi osaksi yksilön oikeussuojaa ja totesi, että mahdollisuus tunnistamistietojen kokoamiseen ja yhdistämiseen voi olla yksityiselämän suojan näkökulmasta ongelmallista, sillä niiden avulla on mahdollista selvittää suojan ydinalueelle kuuluvia tietoja. Tästä syystä perustuslakivaliokunta katsoi, että edellä mainittu jaottelu ei ole mielekästä, vaan ilmoitusvelvollisuuden tulee kattaa myös tunnistamistiedot.[111] Myös Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä viestin sisällön ja tunnistamistietojen välistä jaottelua ei ole nähty mielekkääksi[112].

[108] HE 309/1993 vp, s. 53.
[109] Neuvonen 2014. s. 41-42.
[110] Viljanen V-P II.
[111] PeVL 35/2018 vp, s. 24.
[112] Ks. esimerkiksi tuomio Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 356.

3.1.2. Yksityiselämän suojan rajoittaminen

Suomen perustuslaissa säädettyjä perusoikeuksia ei ole tarkoitettu sellaisiksi ehdottomiksi oikeuksiksi, ettei niitä voisi millään edellytyksellä tai missään laajuudessa rajoittaa. Yksilölle turvattuja perusoikeuksia voi rajoittaa muiden ihmisten perusoikeudet, mutta myös painavat, yhteiskunnalliset intressit voivat toimia perustuslaissa taattujen oikeuksien rajoittajina.[113]

Uudet tiedusteluvaltuudet merkitsevät perustavanlaatuista puuttumista yksityiselämän ja henkilötietojen suojaan sekä luottamuksellisen viestin salaisuuden suojaan.[114] Lakimuutosten myötä luottamuksellisen viestin salaisuuteen puuttumiseen säädettiin uusia edellytyksiä, mutta sovellettaessa tietoliikennetiedustelua tulee perustuslain 10 §:n 4 momentin lakivarauksen lisäksi kiinnittää huomiota myös yleisiin rajoitusperusteisiin[115]. Perusoikeuksille on määritelty yleisiä rajoitusedellytyksiä, joita ovat[116]:

1. Lailla säätämisen vaatimus: Rajoituksen tulee perustua eduskunnan säätämään lakiin, eikä perusoikeuksia rajoittavaa toimivaltaa voi täten siirtää alemmalle säädöstasolle.
2. Täsmällisyys- ja tarkkarajaisuusvaatimus: Perusoikeuksien rajoitukset tulee määritellä riittävän täsmällisesti ja oltava tarkkarajaisia.
3. Hyväksyttävyysvaatimus: Rajoitusten tulee olla hyväksyttäviä suhteessa perusoikeusjärjestelmään ja vastata painavaan yhteiskunnalliseen tarpeeseen.
4. Ydinalueen koskemattomuuden vaatimus: Tavallisella lailla ei voida säätää sellaisesta rajoituksesta, joka ulottuu perusoikeuden ydinalueeseen.
5. Suhteellisuusvaatimus: Rajoitusten tulee olla välttämättömiä, jotta voidaan saavuttaa haluttu tavoite sekä olla laajuudeltaan oikeassa suhteessa perusoikeuksien suojaaman oikeushyvän ja rajoituksen perusteena toimivan yhteiskunnallisen intressin välillä.
6. Oikeusturvavaatimus: Oikeusturvajärjestelyjen tulee olla riittäviä perusoikeuksia rajoitettaessa.
7. Ihmisoikeusvelvoitteiden noudattamisen vaatimus: Perusoikeuksien rajoitusten tulee olla yhdenmukaisia Suomea koskevien ihmisoikeusvelvoitteiden kanssa.

Keskeistä perusoikeuksia rajoitettaessa on yksilön oikeusturva. Oikeusturvavaatimuksesta johtuen rajoitettaessa perusoikeuksia tulee huolehtia riittävistä valvonta- ja oikeusturvajärjestelyistä. Tiedustelutoimintaan ei ole sen luonteesta johtuen mahdollista liittää muutoksenhakumahdollisuutta, mutta sitä korvaamaan on luotu muita oikeusturvajärjestelyjä[117], kuten velvollisuus ilmoittaa tiedonhankinnan kohteelle häneen kohdistuneesta tiedustelutoiminnasta sekä yksilön oikeus tehdä kantelu- ja tutkintapyyntö tiedusteluvalvontavaltuutetulle. Edellä osiossa 2.2. käsitellyllä valvontajärjestelmällä,

[113] Viljanen V-P I.
[114] PeVL 35/2018 vp, s. 3.
[115] PeVM 4/2018 vp, s. 8.
[116] PeVM 25/1994 vp, s. 5. Ks. lisäksi Viljanen V-P I.
[117] HE 198/2017 vp, s. 38.

erityisesti tiedusteluvalvontavaltuutetun suorittamalla laillisuusvalvonnalla ja tiedusteluvalvontavaliokunnan parlamentaarisella valvonnalla, onkin kokonaisuudessaan oikeusturvan kannalta keskeinen merkitys[118].

Lisäksi viranomaisen harkintavaltaa rajoittamaan ja täten oikeusturvajärjestelyjä parantamaan on tiettyjen tiedustelumenetelmien, kuten tietoliikennetiedustelun, käyttö alistettu tuomioistuimen myöntämän luvan varaiseksi. Tärkeäksi oikeusturvatakeeksi on määritelty myös asianosaisjulkisuus, joka koskee kaikkia tiedustelumenetelmiä ja on voimassa siitä hetkestä lähtien, kun henkilölle on ilmoitettu häntä koskevasta tiedustelusta. [119]

Perusoikeuksia voi yleisten rajoitusedellytysten lisäksi rajoittaa säännöksen yhteyteen kirjatulla lakivarauksella eli lausekkeella, joka oikeuttaa kyseisen perusoikeuden rajoittamisen ja käytön sääntelemisen vain lailla tai lain nojalla. Lakivaraus voi olla esimerkiksi sääntelyvaraus, jolla ei niinkään rajoiteta perusoikeutta vaan annetaan lainsäätäjän tehtäväksi antaa perusoikeuden käyttöön liittyviä tarkempia säännöksiä.[120] Perusoikeussäännökseen voi sisältyä myös kvalifioitu lakivaraus eli rajoituslauseke, jolla rajoitetaan edelleen lainsäätäjän harkintavaltaa kytkemällä rajoitusvaltuus johonkin tiettyyn tarkoitukseen tai edellytykseen.[121]

Jotta uudet tiedustelutoimivaltuudet voitiin säätää tavallisessa lainsäätämisjärjestyksessä, tuli perustuslain 10 §:ää muuttaa tietyin osin. Aiempi 3 momentin viimeisen lause siirrettiin sisällöltään tarkastettuna 4 momenttiin[122], jolloin kotirauhan suojan rajoittamisesta säädetään nyt 3 §:ssä ja luottamuksellisen viestin salaisuuden rajoituksista 4 §:ssä. Uusi 4 §:ssä säädetty hyväksyttävä peruste luottamuksellisen viestin salaisuuden suojan rajoittamiseksi on tiedon hankinta sotilaallisesta tai muusta vakavasti kansallista turvallisuutta uhkaavasta toiminnasta. Perustuslain 10 §:ssä säädetyt kvalifioidut lakivaraukset kuuluvat siis seuraavasti:

> Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä.
>
> 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.

---

[118] HaVM 30/2016 vp, s. 41.
[119] Laitinen 2018, s. 14-15.
[120] Viljanen V-P I, s.164-165.
[121] PeVM 25/1994 vp, s. 5.
[122] HE 198/2017 vp, s.34.

Perustuslakivaliokunta on kuitenkin lakimuutosta koskevassa mietinnössään korostanut, ettei muutosta tule ottaa vain sivutuotteena tarpeesta säätää tavallisia lakeja vaan sitä tulee arvioida aina itsenäisesti. Uusi, kansalliseen turvallisuuteen nojautuva rajoitusperuste irtautuu rikosperusteisesta toiminnasta ja mahdollistaa tiedonhankinnan sellaisista toimista, joihin ei voida tiedonhankintavaiheessa kohdistaa yksilöityä ja konkreettista rikosepäilyä. Rajoituslauseke voi määrittää luottamuksellisen viestin rajoittamista mahdollisesti myös muissa tilanteissa kuin tiedustelussa, joten muutosesitystä arvioitaessa on pidetty olennaisena, että rajoituslauseke turvaa luottamuksellisen viestin salaisuutta edelleen riittävästi.[123]

Kvalifioidut lakivaraukset on perustuslakia uudistettaessa rinnastettu rakenteellisesti Euroopan ihmisoikeussopimuksen artikloihin sisältyviin rajoituslausekkeisiin.[124] Nyt uusia rajoitusperusteita säädettäessä kiinnitettiin lainvalmisteluvaiheessa myös huomiota siihen, että ne ovat Suomena sitovien kansainvälisten ihmisoikeussopimusten mukaiset.[125] Vastaavasti on syytä muistaa jo edellä mainittu: jo perustuslakia uudistettaessa perustuslakivaliokunta nosti esiin rajoitusten yhteensopivuusvaatimuksen Suomea sitovien ihmisoikeusvelvoitteiden kanssa. Euroopan ihmisoikeussopimuksessa yksityisyyden suojan rajoittamisesta säädetään 8 artiklan 2 kohdassa. Säännöksessä on listattu ne asiantilat, joihin perustuen artiklassa turvattuja oikeuksia on mahdollista rajoittaa:

> 2. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Yksityis- ja perhe-elämän suojaan saa siis puuttua vain kansallisella lailla, puuttumisen perusteena on oltava edellä yksilöidyt tilanteet ja sen tulee olla välttämätöntä demokraattisessa yhteiskunnassa kyseisen päämäärän saavuttamiseksi[126]. Verrattaessa ihmisoikeussopimuksen ja perustuslain sisältämiä sallittuja rajoitusperusteita on niistä löydettävissä yhteisiä elementtejä. Molemmissa säännöksissä mainitaan kansallisen turvallisuus sallittuna rajoittavana tekijänä, ja molemmissa tapauksissa turvattujen oikeuksien rajoittamisen tulee olla sekä välttämätöntä että sallittua laissa.

Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä yksityiselämän suojan kattamaan alueeseen sisältyy monet erilaiset tilanteet ja täten myös siihen kohdistuva puuttuminen voi

[123] PeVM 4/2018 vp, s. 2-5.
[124] PeVM 25/1994 vp, s. 5
[125] HE 198/2017 vp, s. 38; PeVM 4/2018 vp, s. 9.
[126] Ks. esim. Roman Zakharov v. Russia (2015), kohta 227; Kennedy v. The United Kingdom (2010), kohta 130.

olla monenlaista. Tuomioistuimen ratkaisuissa usein keskeistä onkin, onko puuttuminen ollut kohtuullista ja oikeutettua sen sijaan, että argumentoidaan, onko puuttumista todellisuudessa tapahtunut vai ei.[127] Esimerkiksi arvioidessaan onko yksittäinen henkilö joutunut tiedustelun tai salaisen tiedonhankinnan kohteeksi ei tuomioistuimen näkökulmasta ole olennaista se, onko häneen kohdistunutta tiedustelua todellisuudessa tapahtunut – pelkkä tällaisen tapahtuman todellinen mahdollisuus on riittävä syy, että tuomioistuin ottaa asian tutkittavaksi. Keskeistä ei siis ole se, onko valittajan 8 artiklassa taattuihin oikeuksiin tosiasiallisesti puututtu, vaan se, onko tähän olemassa kansallisen lainsäädännön perusteella mahdollisuus.[128]

3.2. Luottamuksellisen viestin salaisuuden suojan rajoittaminen

3.2.1. Rajoituksen lakiperusta

Perusoikeutta ei saa rajoittaa, jos rajoituksesta tai rajoitusvaltuudesta ole säädetty laissa. Laissa tarkoitetaan tässä yhteydessä eduskunnan säätämää lakia, ja tällöin rajoitusta perusoikeuteen ei voi määrätä esimerkiksi asetuksella. Lainsäätäjä ei saa tästä vaatimuksesta johtuen myöskään tavallisella lailla siirtää valtaa perusoikeuksien rajoituksien säätämisestä sellaiselle taholle, joka antaa asetuksia tai muita lakia alempiasteisia normeja. Tuomioistuin ei niin ikään saa soveltaa sellaista lakia alempiasteista säädöstä, joka rajoittaisi perusoikeuksia. Vaatimusta siitä, että perusoikeuksien rajoituksen tulee kirjata lakiin, voidaan tarkastella myös rajoitusten kontrolloinnin näkökulmasta – lakeja säädettäessä rajoitusten hyväksyttävyyttä voidaan arvioida avoimesti. Kun rajoitukset on kirjattu kaikkien ulottuvilla olevaan julkiseen säädöskokoelmaan, voi yksilö ennakoida niiden vaikutusta omaan toimintaansa.[129]

Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä vaatimus rajoituksen perustumisesta kansalliseen lakiin puolestaan pitää sisällään laatuvaatimuksia. Laillisuusvaatimus koostuu kolmesta erillisestä vaatimuksesta: 1) oikeuksiin puuttumiselle tulee olla perusta kansallisessa lainsäädännössä; 2) rajoituksen sallivan lainsäädännön tulee olla oikeusvaltioperiaatteen (rule

[127] Hirvelä & Heikkilä 2017, s. 632.
[128] Hirvelä & Heikkilä 2017, s. 838.
[129] Viljanen V-P 2001, s. 67-69.

of law) mukainen ja sen on oltava saatavilla sekä 3) yksilön on pystyttävä ennakoimaan lainsäädännön seuraamukset hänen kohdallaan.[130]

Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä vaatimuksen rajoituksen perustumisesta kansalliseen lakiin on katsottu korostuvan erityisesti silloin, kun oikeuksiin puuttuminen tapahtuu kohteelta salassa, kuten tiedustelutoiminnassa. Riittävän selkeiden, laissa määriteltyjen harkintavallan rajojen ja soveltamistapojen päämääränä on vahvistaa yksilön suojaa mielivaltaista oikeuksiinsa puuttumista vastaan. [131] Ennakoitavuus salaisen tiedonhankinnan kohdalla ei vaadi valtioita nimeämään lainsäädännössä tyhjentävästi niitä yksittäisiä rikkomuksia, joiden perusteella tiedustelun kohteeksi voi joutua, kunhan laissa tehdään riittävän yksityiskohtaisesti selvää tällaisten rikkomusten laadusta (nature of the offences in question).[132]

Tuomioistuin on oikeuskäytännössään jo vuosikymmenien ajan painottanut vallan väärinkäytön mahdollisuutta erilaisissa tiedustelujärjestelmissä. Mahdollisuus väärinkäyttöön kasvaa, jos kansallisessa laissa ei selvästi määritellä viranomaisten tiedusteluvaltuuksien todellista laajuutta. [133] Väärinkäytön estämiseksi Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään kehittänyt kuusi minimivaatimusta (minimum safeguards), jotka kansallisesta laista koskien tiedustelutoimintaa tulisi käydä ilmi. Minimivaatimukset ovat kuvaus niiden rikkomusten luonteesta, joiden pohjalta tiedustelua voidaan suorittaa; niiden ihmisryhmien määrittely, joiden viestintä voi joutua tiedustelun kohteeksi; tiedustelutoiminnan keston rajat; saadun tiedon tutkintaan, säilöntään ja hävittämiseen sovellettavat menettelyt; sovellettavat varokeinot kun dataa välitetään toisille osapuolille sekä ne tilanteet, joissa saatu tieto voidaan tai täytyy poistaa tai tuhota. Tuomioistuimen luoma kriteeristö on mainittu jo vuonna 1990 tapauksessa Huvig v. France ja sen jälkeen tuomioistuin on viitannut vaatimuksiin useissa tiedustelutoimintaa koskevissa ratkaisuissaan aivan nykypäivään asti. [134]

---

[130] Hirvelä & Heikkilä 2017, s. 841. Katso lisäksi esim. Kennedy v. The United Kingdom (18.5.2010), kohdat 151-154. Oikeusvaltioperiaate kansallisessa lainsäädännössä perustuu perustuslain 2 §:n 3 momenttiin: "Julkisen vallan käytön tulee perustua lakiin. Kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia."

[131] Ks. esim. Euroopan ihmisoikeustuomioistuimen ratkaisu Malone v. The United Kingdom (4.8.1984) kohdat 67 ja 68.

[132] Esimerkiksi Roman Zakharov v. Russia (4.12.2015), kohta 244.

[133] Ks. esim. Huvig v. France (24.4.1990) kohta 29; Weber and Saravia v. Germany (29.6.2006) kohta 93; Roman Zakharov v. Russia (4.12.2015) kohta 229; Centrum för Rättvisa v. Sweden (19.6.2018) kohta 113.

[134] "[…]a description of the nature of offences which may give rise to an interception order; a definition of the categories of people liable to have their communications intercepted; a limit on the duration of the measures; the procedure to be followed for examining, using and storing the data obtained; the precautions to be taken when

Suomessa kansallisella tasolla on niin ikään vaadittu, että laissa tulee määritellä tiedustelutoiminnan käytön kesto ja edellytykset, tiedustelun kohteena olevat ihmiset tai ihmisryhmät, tietojen hävittäminen sekä tiedustelun raportointiin käytettävä menetelmä[135].

3.2.2. Välttämättömyys ja vakava uhka kansalliselle turvallisuudelle

Perustuslain 10 §:n 4 momentissa säädetään, että luottamuksellisen viestin salaisuuden välttämättömistä rajoituksista voidaan säätää lailla. Välttämättömyysvaatimuksella tarkoitetaan perustuslain 10 §:ssä sitä, että luottamuksellisen viestin salaisuuteen saadaan puuttua vain, jos tiedonhankintaa ei voida suorittaa vähemmin puuttuvilla keinoilla ja luottamuksellisen viestin salaisuuteen puututaan tiedonhankintatoiminnassa mahdollisimman kohdennetusti ja rajoitetusti. Välttämättömyysvaatimus perustuslain luottamuksellisen viestin salaisuuden suojaa koskevassa säännöksessä ei salli rajoittamatonta puuttumista perusoikeuteen, ja täten sääntelyllä ei sallita kohdentamatonta, yleistä ja kaiken kattavaa tietoliikenteen seurantaa. [136]

Perustuslakivaliokunta korostaa, että välttämättömyysvaatimuksen täyttymiseksi ei kuitenkaan voida katsoa pelkästään se, että luottamuksellisen viestin salaisuuteen puuttuminen edistää kansallista turvallisuutta. Kussakin yksittäistapauksessa tulee osoittaa, että tiedon hankkiminen ja siitä johtuvat, yksilökohtaiset rajoitukset perusoikeuksiin ovat välttämättömiä ja tehokkaita tapoja hankkia tietoa kansallista turvallisuuta vakavasti uhkaavasta toiminnasta käsiteltävänä olevassa tilanteessa.[137]

Välttämättömyyttä ja yhteiskunnallisen tarpeen pakottavuutta arvioitaessa jäsenvaltiolle on myönnetty ensisijainen vastuu [138] . Välttämättömyyden vaatimuksen voidaan tiedustelutoimivaltuuksien kohdalla nähdä merkitsevän vaatimusta suppeasta tulkinnasta. [139] Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään korostanut, että koska 8 artiklan 2 momentissa sallitut päämäärät asettavat rajoituksia ihmisoikeussopimuksessa turvatuille oikeuksille, tulee kyseistä säännöstä tulkita kapeasti. Kansalaisiin kohdistuva salainen

---

communicating the data to other parties; and the circumstances in which recordings may or must be erased or destroyed[…]". Ks. Huvig v. France (24.4.1990) kohta 34, lisäksi esim. Amann v. Switzerland (2000) kohta 76; Weber and Saravia v. Germany (29.6.2006), kohta 95; Roman Zakharov v. Russia (4.12.2015) kohta 231; Big Brother Watch and Others vs. The United Kingdom (13.9.2018) kohta 307; Centrum för Rättvisa v. Sweden (19.6.2018), kohta 103.

[135] PeVL 35/2018 vp, s. 7.

[136] HE 198/2017 vp, s. 37-38. Ks. myös PeVM 4/2018 vp, s. 7.

[137] PeVM 4/2018 vp, s. 8-9

[138] Valtion harkintamarginaalista ja suhteellisuusperiaatteesta esim. Euroopan ihmisoikeustuomioistuimen ratkaisu Handyside v. The United Kingdom (7.12.1976), kohdat 48 ja 49.

[139] PeVL 35/2018 vp, s. 8.

tiedonhankinta on täten Euroopan ihmisoikeussopimuksen mukaan sallittua vain silloin, kun se on ehdottoman välttämätöntä (strictly necessary) demokraattisten instituutioiden suojaamiseksi.[140]

Vakava uhka kansalliselle turvallisuudelle on uusi hyväksyttävä luottamuksellisen viestin salaisuuden rajoitusperuste, jolla irrottaudutaan entisestä, rikosperusteisesta toiminnasta. Vakavan uhan kansalliselle turvallisuudelle perustuslain 10 §:n 4 momentin tarkoittamassa merkityksessä muodostaa sellainen väkivaltainen ulkoinen toiminta, joka välillisesti tai välittömästä uhkaa valtion oikeudenkäyttöpiirissä olevien ihmisten kollektiivista turvallisuutta. Yleensä tällaista on yleisvaarallinen toiminta tai siihen liittyvät teot, joka uhkaa suuren ja ennalta arvaamattoman, sattumanvaraisesti valitun ihmisjoukon henkeä tai terveyttä. Tyypillinen, kansalliselle turvallisuudelle vakavan uhan muodostava toiminta on esimerkiksi terrorismi. Keskeistä on, että toiminnalla on kytkentä Suomeen ja uhka kohdistuu Suomen kansalliseen turvallisuuteen, vaikka se maantieteellisesti tapahtuisikin valtionrajojen ulkopuolella. Säännöksessä ei edellytetä, että kansallisen turvallisuus olisi välittömästi uhattuna, vaan tiedonhankinta on sallittua silloin, jos toiminta jatkuessaan muodostaa vakavan uhan kansalliselle turvallisuudelle. Uhan aste ei kuitenkaan ole merkityksetön, vaan sen tulee olla laadultaan vakavaa. [141]

Ilmaisu ”kansallinen turvallisuus” pitää sisällään ajatuksen siitä, että sellainen uhkaava toiminta, johon säännöksessä viitataan, ei kohdistu kehenkään yksittäiseen henkilöön vaan yleisemmällä tasolla yhteiskuntaan ja sen koko ihmisyhteisöön. Toisaalta, jos yksittäiseen henkilöön kohdistuva väkivallanteko on laajuudeltaan tai merkitykseltään kansallisen turvallisuuden kannalta merkittävä tai voi muodostaa sitä vakavasti uhkaavan tilanteen, kattaa käsite myös tällaiset tapaukset. Vakavan uhan kansalliselle turvallisuudelle voi tällaisessa tapauksessa muodostaa esimerkiksi valtiojohtoon kohdistuva uhka. [142]

Perustuslakivaliokunta on jo perustuslain 10 §:ää muutettaessa kiinnittänyt huomiota 4 momenttiin sisältyvien käsitteiden ”kansallinen turvallisuus” ja ”vakava uhka” laaja-alaisuuteen. Näitä sovellettaessa on tärkeää huomioida ja noudattaa niitä lainsäädännälle asetettuja perusvaatimuksia, joita eurooppalainen oikeuskäytäntö asettaa. Eurooppalaisesta

[140] Szabó and Vissy v. Hungary (12.1.2016), kohta 54: “This provision [Art. 8.2], “since it provides for an exception to a right guaranteed by the Convention, is to be narrowly interpreted. Powers of secret surveillance of citizens, characterising as they do the police state, are tolerable under the Convention only in so far as strictly necessary for safeguarding the democratic institutions.”
[141] HE 198/2017 vp, s. 34-37.
[142] HE 198/2017 vp, s. 36.

oikeuskäytännöstä johdettuja vaatimuksia ovat esimerkiksi riippumaton valvonta, tietosuojan perusteiden noudattaminen ja toimivaltuuksien käytön ennakollinen hyväksyminen sekä oikeusturvan toteuttaminen tuomioistuimessa. Rajoitusperiaate on sikäli poikkeuksellinen, että sillä irrottaudutaan rikosperusteisesta toiminnasta. Tästä johtuen vahvat oikeusturvatakeet sekä laaja-alainen ja tehokas tiedusteluvaltuuksien käytön valvonta korostuvat. Perustuslakivaliokunta korostaa, että perustuslaista johtuen kansallisen turvallisuuden käsitettä on tulkittava suppeasti ja uhan vakavuusaste on asetettava korkeaksi. Se taho, joka vetoaa rajoitusperusteeseen, on velvollinen esittämään riittävät perustelut sille, että jostakin toiminnasta on mahdollisuus muodostua vakava uhka kansalliselle turvallisuudelle. [143]

Kansallisen turvallisuuden käsitteen laajuudesta johtuen on siihen lukeutuva toiminta jätettävä Euroopan ihmisoikeustuomioistuimen näkökulmasta ensisijaisesti valtion oman harkinnan varaan. Tuomiossaan Big Brother Watch and Others v. The United Kingdom tuomioistuin viittasi aiempaan tuomioonsa Kennedy v. The United Kingdom jossa se katsoi, että ilmaisua ”kansallinen turvallisuus” käytetään laajasti niin kansallisessa kuin kansainvälisessä lainsäädännössä. Lisäksi se on yksi niistä hyväksyttävistä rajoitusperusteista, jotka mainitaan Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdassa. Kansalliseen turvallisuuteen kohdistuvat uhat ovat luonteeltaan vaihtelevia ja niitä voi olla vaikea määritellä ennakolta. Tuomioistuimen ratkaisuista on kuitenkin nähtävissä, että sotilaallinen maanpuolustus sekä laittoman tiedustelutoiminnan ja terrorismin torjunta näyttävät kuuluvan kansallisen turvallisuuden käsitteen alle. Pelkkä ”kansallinen turvallisuus” ei kuitenkaan ole riittävä peruste 8 artiklan oikeuksiin puuttumiselle, vaan kansallisessa lainsäädännössä tulisi edes jollakin tarkkuudella yksilöidä eri tapahtumat ja tilanteet, jotka luovat uhan kansalliselle turvallisuudelle. Tällainen määrittely vahvistaa edellisessä kappaleessa käsiteltyä ennakoitavuutta, mutta tuomioistuin ei kuitenkaan vaadi, että lakiin sisällytettäisiin täydellisen tyhjentävää listausta.[144]

Luottamuksellisen viestin salaisuuden suoja ei ulotu vieraan valtion viranomaisorganisaation viestintään. Luottamuksellisen viestinnän salaisuuteen puuttuminen voi kuitenkin olla välttämätöntä, jotta tällainen viesti havaitaan; esimerkiksi tietoliikennetiedustelua varten tarvittavan, vieraan valtion viranomaisen käyttämän viestintäverkon osan yksilöinnissä

[143] PeVM 4/2018 vp, s. 8-9.
[144] Ks. esim. Kennedy v. The United Kingdom (18.5.2010), kohta 159 sekä Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 333.

voidaan joutua teknisesti puuttumaan myös muuhun viestintään.[145] Perustuslakivaliokunta on tässäkin korostanut rajoitusperusteen tulkitsemista suppeasti ja muistuttaa, että tiedon hankkiminen on sallittua vain sellaisesta sotilaallisesta toiminnasta, joka kohdistuu Suomeen tai on Suomen turvallisuusympäristön kannalta merkityksellisestä. [146]

Euroopan ihmisoikeustuomioistuin on toistuvasti oikeuskäytännössään korostanut, että valtioiden harkintamarginaali on laaja sen suhteen, minkä tavan ne katsovat parhaaksi suojaamaan kansallista turvallisuutta. Tuomioistuin on katsonut, ettei esimerkiksi laajamittainen tukkutiedustelukaan itsessään ole ihmisoikeussopimuksen vastainen, mutta muistuttaa, että vuosikymmenien aikana muotoutuneesta oikeuskäytännöstä on pääteltävissä, että minkä tahansa järjestelmän väärinkäyttö on mahdollista, etenkin jos viranomaisten todellista harkintavaltaa ei voida laista havaita. Tällöin, huolimatta laajasta harkintamarginaalista sovellettavan tiedustelujärjestelmän suhteen, harkintavallan tulee olla kapeampi tiedustelujärjestelmän käyttämisen sääntelyssä. [147]

[145] HE 198/2017 vp, s. 35.
[146] PeVM 4/2018 vp, s. 7.
[147] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 314-315. Ks. lisäksi esim. Weber and Saravia kohta 106; Szabó and Vissy v. Hungary (12.1.2016), kohta 57; Roman Zakharov v. Russia (4.12.2015), kohta 232.

4. Ennakollinen lupamenettely

4.1. Tuomioistuimen ja suojelupoliisin rooli ennakollisessa lupamenettelyssä

Tietoliikennetiedustelun käyttämiseksi on tiedusteluviranomaisen eli suojelupoliisin ensin haettava siihen lupa tuomioistuimelta. Tuomioistuinkontrollilla on keskeinen rooli tiedustelutoiminnan laillisuuden sekä perus- ja ihmisoikeuksien toteutumisen varmistajana. Siviilitiedustelulaista annetuissa lausunnoissa on korostettu perus- ja ihmisoikeuksien suojan tasoa suhteessa aiempiin salaisiin tiedonhankintamenetelmiin. Koska uusi siviilitiedustelulainsäädäntö irrottautuu rikos- ja henkilöperustaisuudesta, tulee lähtökohtana pitää vaatimusta perus- ja ihmisoikeuksien korkeammasta suojan tasosta. Ajatus korkeammasta suojan tasosta on merkityksellinen myös tarkastellessa ennakoivaa lupamenettelyä.[148]

Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään nähnyt, että salaisia tiedustelumenetelmiä voidaan valvoa kolmessa eri tiedustelutoiminnan vaiheessa: kun tiedustelutoiminnan aloittamisesta päätetään, tiedustelua toteutettaessa sekä tiedustelun lopettamisen jälkeen. Tiedustelutoiminnan luonteesta johtuen kaksi ensimmäistä vaihetta valvontamenettelyineen ei voi tulla yksilön tietoon eikä hän voi itse osallistua menettelyyn, jolloin menettelyn itse tulee turvata yksilön oikeudet.[149]

Vaikka tuomioistuimen roolia ennakollisena valvojana pidetään yleisesti parhaana oikeusturvatakeena Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä, ei tuomioistuin kuitenkaan suoranaisesti vaadi, että salaisen tiedonhankinnan oikeuttavan tahon tulee olla tuomioistuin. Keskeistä on, että luvan myöntävän tahon itsenäisyys voidaan taata toimeenpanevasta tasosta. Euroopan ihmisoikeustuomioistuin kuitenkin katsoo, että oikeusvaltioperiaatteeseen (rule of law) sisältyy vaatimus siitä, että toimeenpanevan viranomaisen puuttuminen yksilön oikeuksiin tulisi olla tehokkaan valvonnan alaista. Tuomioistuinkontrollin on tavallisesti nähty tarjoavan paras takuu itsenäisyydestä, puolueettomuudesta ja asiallisesta menettelystä, joten valvonnasta tulisi Euroopan ihmisoikeustuomioistuimen mukaan vähintään viimesijaisena keinona vastata tuomioistuin.[150]

---

[148] Melander 2018, s. 5.
[149] Esim. Roman Zakharov v. Russia (4.12.2015), kohta 233.
[150] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 133.

Suomessa tiedustelumenetelmiä koskevat lupa-asiat käsitellään keskitetysti Helsingin käräjäoikeudessa, sillä Helsingin käräjäoikeudella on nähty olevan salaisten tiedonhankinta- ja pakkokeinoasioiden käsittelyn osalta laajin kokemus. Keskittämisellä voidaan tämän lisäksi edistää tietoliikennetiedustelua koskevan erityisosaamisen saavutettavuutta kerryttämällä osaamista ja asiantuntemusta. [151] Helsingin käräjäoikeudessa käsiteltävä tietoliikennetiedusteluun vaadittava lupavaatimus tulee olla suojelupoliisin päällikön laatima. Lupavaatimuksen laatijana ollessa suojelupoliisin päällikkö tai virkamies, on sisäisellä valvonnalla myös mahdollista toteuttaa ennakollista valvontaa. Tiedustelumenetelmän käyttöön liittyviä valvontakohteita ovat esimerkiksi ne, onko vaatimuksen laatinut siihen oikeutettu virkamies ja vastaavasti onko päätöksen tehnyt siihen oikeutettu taho – esimerkiksi tietoliikennetiedustelussa lupavaatimuksen laatijana tulee lain mukaan olla suojelupoliisin päällikkö. Tärkeää on valvoa myös sitä, että lupaa ei haeta liian aikaisin, sillä luvasta päättävän tahon tulee pystyä varmistumaan siitä, että edellytykset menetelmän käytölle ovat edelleen olemassa silloin, kun menetelmän käyttö aloitetaan.[152]

Vaikka valtuuttavana tahona ei Euroopan ihmisoikeustuomioistuimen mukaan ole välttämätöntä olla tuomioistuin, on se ratkaisussaan Centrum för Rättvisa v. Sweden nähnyt kuitenkin, että luvan pyytäminen tuomioistuimelta jokaisessa tiedustelutapauksessa on merkittävä tekijä yksilön oikeuksien suojaamisessa. Lisäsuojana toimivallan väärinkäyttöä ja mielivaltaisuutta vastaan Euroopan ihmisoikeustuomioistuin näkee sen, että tiedustelutehtävän lainmukaisuuden ja suhteellisen arviointi on osoitettu elimelle, jonka jäsenet ovat tai ovat olleet tuomareita. Kokonaisuudessaan tuomioistuin on nähnyt Ruotsissa säädetyn ennakollisen lupamenettelyn tarjoavan tärkeitä takeita väärinkäyttöä vastaan.[153]

Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään käsitellyt myös sellaisia tiedustelujärjestelmiä, joissa tiedustelumenetelmän valtuuttavana tahona on jokin muu viranomainen kuin tuomioistuin. Tapauksessa Szabó and Vissy v. Hungary Unkarin lainsäädännössä kansallisen turvallisuuden vuoksi tehtävän tiedustelutoiminnan valtuutti oikeusministeri. Oikeusministerille lupahakemuksen toimitti tiedusteluviranomaisen eli TEK:n johtaja, ja TEK puolestaan on osa poliisivoimia toimien sisäministerin alaisuudessa. Tuomioistuin katsoi, että valtuutuksen mahdollinen poliittinen piirre oli omiaan lisäämään järjestelmän väärinkäytön riskiä. Järjestelmässä, jossa valtuuttava taho on muu kuin

[151] HaVM 36/2018 vp, s. 61. Ks. myös LaVL 27/2018 vp, s. 7.
[152] Lohse & Viitanen 2019, s. 162-163.
[153] Centrum för Rättvisa v. Sweden (19.7.2018), kohdat 139 ja 141.

oikeudellinen viranomainen, tulee tahon olla toimeenpanovallasta itsenäinen. Jos tahon itsenäisyyttä ei voida taata, tulee tuomarilla tai muulla itsenäisellä elimellä olla kontrolli luvan myöntävään tahoon – tällaisessa tapauksessa itsenäisen tahon, yleensä tuomarin, suorittama valvonta on sääntö ja vaihtoehtoiset tavat poikkeus. Tuomioistuimen näkökulmasta toimeenpanovallan sisällä toimivan, poliittisesti vastuussa olevan tahon suorittama valvonta ei tarjoa tarvittavia takuita väärinkäyttöä vastaan. [154] Tuomioistuimen näkökulmasta ennakollinen ja oikeudellinen lupamenettely voi toimia rajoituksena toimeenpanevan tason harkintavallalle esimerkiksi laajojen termien tulkinnassa. Se voi tarjota vakiintuneen tulkinnan oikeudellisille termeille tai vakiintuneen käytännön sen varmistamiseen, milloin yksilön viestintään puuttumiselle on perustelu syy yksittäisessä tilanteessa. [155]

Vertailukohtana voidaan tarkastella Iso-Britannian järjestelmää, jossa tiedustelutoiminnan valtuuttavana tahona toimii vastaava valtiosihteeri (Secretary of State). Tuomioistuin on viitannut Szabó and Vissy -tapauksessa tuomioonsa Kennedy v. The United Kingdom, jossa tarkastelun alla oli osittain sama järjestelmä kuin aiemmin käsitellyssä tapauksessa Big Brother Watch and Others v. The United Kingdom. Euroopan ihmisoikeustuomioistuin tarkasteli Iso-Britannian tiedustelujärjestelmää kokonaisuutena ja otti huomioon vallankäytön sekä vallan väärinkäytön välisen tasapainon (checks and balances), eikä nähnyt, että valtiosihteerin myöntämät luvat olisi myönnetty ilman asianmukaista harkintaa. Prosessiin kohdistui myös valvontaa itsenäisen valvontaelimen (Interception of Communications Commissioner) toimesta minkä lisäksi Iso-Britannian järjestelmässä oli hallinnosta itsenäinen tuomioistuin (the Investigatory Powers Tribunal), jolla oli toimivalta tutkia valituksia lainvastaisesta tiedustelutoiminnasta.[156] Ratkaisevaksi tekijäksi näissä kahdessa tapauksessa, jossa valtuuttaja ei ole oikeudellinen taho, muodostui siis luvan myöntäjään kohdistettu valvonta.

Myös niissä tapauksissa, joissa valtuuttavana tahona on tuomioistuin, Euroopan ihmisoikeustuomioistuin korostaa, että pelkän tuomioistuinkontrollin olemassaolo ei ole riittävä tae järjestelmän väärinkäyttöä vastaan, vaan kontrollin tulee olla todellista. Tapauksessa Roman Zakharov v. Russia Venäjän lainsäädännössä vaadittiin tuomioistuimen valtuutusta tiedustelutoimintaan, mutta ratkaisussa nähtiin, että kontrolli oli vajavaista. Tarkasteltaessa tiedustelun valtuuttavan viranomaisen, tässä tapauksessa tuomioistuimen,

[154] Szabó and Vissy v. Hungary (12.1.2016), kohdat 75 ja 77.
[155] Szabó and Vissy v. Hungary (12.1.2016), kohdat 72-73. Ks. myös Klass and Others v. Germany (6.9.1978), kohta 42.
[156] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 377-379.

arvioinnin laajuutta, tulee kansallisen tuomioistuimen pystyä vahvistamaan, onko todellisuudessa olemassa perusteltu epäilys tiedustelun kohdetta kohtaan. Vastaavasti tuomioistuimen tulee arvioida, täyttääkö vaadittu tiedustelutoiminta välttämättömyysvaatimuksen, joka pitää sisällään myös suhteellisuusvaatimuksen eli tarkastelun siitä, onko tieto mahdollista saavuttaa vähemmän puuttuvin keinoin. Euroopan ihmisoikeustuomioistuin katsoi, että kyseisessä tapauksessa tuomioistuinkontrolli ei ollut todellista, eikä täten täyttänyt Euroopan ihmisoikeussopimuksen asettamia vaatimuksia. Tiedustelun toimeenpanevan viraston tuli Venäjän lainsäädännön mukaan toimittaa tuomarille perustelu lupavaatimus, johon tuomari voi halutessaan pyytää lisäselvityksiä. Tuomioistuimelle ei annettu lupavaatimuksessa tietoa koskien peitetoimintaa suorittavia agentteja tai ilmiantajia eikä tietoa koskien tiedusteluoperaation organisointia tai taktiikkaa. Tällaisen tiedon puuttuminen kaventaa Euroopan ihmisoikeustuomioistuimen näkökulmasta tuomioistuimen arvioinnin kattavuutta, koska se ei tällaisen tiedon puuttuessa voi arvioida, onko tiedustelun kohteena olevan henkilön epäilyyn riittävää faktapohjaa. [157]

Lisäksi tuomioistuin kiinnitti huomiota siihen, että Venäjän kansallisessa, salaista tiedustelua koskevassa lainsäädännössä tuomareita ei ohjeistettu vahvistamaan perusteltua epäilystä tai testaamaan tarpeellisuus- ja suhteellisuusperiaatetta. Venäjän perustuslakituomioistuin oli lausunnossaan suositellut tuomioistuimia suorittamaan kyseiset testit niiden arvioidessa tiedustelun lupahakemuksia, mutta kansallinen laki ei suoranaisesti vaadi noudattamaan perustuslakituomioistuimen suosituksia, jos niitä ei ole julkaistu osana tuomiota. [158] Lupahakemuksen sisällön puutteista johtuen tuomioistuin myönsi ajoittain sellaisia lupia, joissa ei yksilöidä henkilöä tai puhelinnumeroa johon tiedonhankintaa kohdistetaan, vaan sallittiin tiedonhankinnan kohdistaminen kaikkeen puhelinviestintään sillä alueella, jossa rikos oli tapahtunut. Joissakin luvissa ei mainittu tiedonhankintatoimien sallittua kestoa. Tämänkaltaisia lupia ei selvästi kielletä tiedustelutoimintaa koskevassa OSAA-lainsäädännössä, ja ne sallivat Euroopan ihmisoikeustuomioistuimen näkökulmasta tiedonhankintaa suorittaville viranomaiselle laajan harkintavallan sen suhteen, mihin viestintään tiedonhankintaa kohdistetaan ja kuinka kauan sitä harjoitetaan.[159]

Euroopan ihmisoikeustuomioistuin kiinnitti huomiota lisäksi siihen, että tiedusteluviranomaiselta ei valittajien mukaan vaadittu, että lupahakemukseen sisällytetään

[157] Roman Zakharov v. Russia (4.12.2015), kohdat 259-261.
[158] Roman Zakharov v. Russia (4.12.2015), kohta 262-263.
[159] Roman Zakharov v. Russia (4.12.2015), kohta 265.

hakemusta tukevia materiaaleja. Tutkittuaan eri alueen käräjäoikeuksilta saamiansa raportteja tuomioistuin tuli johtopäätökseen, että useimmissa tapauksissa lupahakemukset eivät sisällä hakemusta tukevia materiaaleja eivätkä käräjätuomarit vastaavasti pyydä tiedusteluviranomaisilta kyseisiä tietoja. Käytännössä luvan myöntämiseen riitti, että hakemuksessa viitattiin tietoon sellaisen uhan olemassaolosta, joka kohdistuu Venäjän kansalliseen, sotilaalliseen, taloudelliseen tai ekologiseen turvallisuuteen. Hakemuksen hylkäämisen aiheutti vain se, jos hakemuksen allekirjoittaja ei ollut toimivaltainen henkilö, siinä ei yksilöity tiedustelun kohteena olevaa toimintaa tai, tiedustelun kohdistuessa rikokseen, kyseiseen rikokseen ei saanut kansallisen lain mukaan kohdistaa tiedustelua.[160]

Kyseinen näkökulma on Suomen tiedustelulainsäädännön kannalta keskeinen, sillä aiemmin salaisista pakkokeinoista päätettäessä tuomioistuinkontrolli on ollut osin vajavaista, mikä on nostettu esiin asiantuntijalausunnoissa perustuslakivaliokunnalle. Asiantuntijalausunnossaan Markku Fredman nosti esiin, että salaisia pakkokeinoja koskevien hakemusten tueksi ei pakkokeinoasioissa vaadittu kirjallisen materiaalin esittämistä ja riskinä on, että kyseinen käytäntö toistuu myös tiedusteluasioita koskevassa tuomioistuinkäytännössä.[161] Fredman on vuonna 2017 kirjoittamassa artikkelissaan tutkinut Helsingin käräjäoikeuden tekemiä päätöksiä koskien pakkokeinoasioita. Artikkelissa havaittiin, että hakemuksia hylättiin erittäin pieni osa. Helsingin käräjäoikeuden pakkokeinoasioita koskevista päätöksistä ei ollut havaittavissa oikeudellista harkintaa koskien esimerkiksi säädettyjen edellytysten ja välttämättömyyden arviointia. Vuoden 2015 alkupuolella ei ollut viitteitä siitä, että yksikään telepakkokeinoja koskeva hakemus olisi hylätty. Fredman tuli artikkelissa johtopäätökseen, että pakkokeinoille lupaa hakeva viranomainen saa pääsääntöisesti käräjäoikeudelta haluamansa ratkaisun, jolloin päätösvalta on käräjäoikeuden sijaan esitutkintaviranomaisella.[162]

Niklas Vainio on niin ikään asiantuntijalausunnossaan viitannut myös Oikeuspoliittisen tutkimuslaitoksen tutkimukseen käräjäoikeuksien telepakkokeinopäätöksistä. Tutkimuksesta ilmeni lupapäätösten perustelujen olevan tavallisesti kaavamaisia ja päätökset oli perustelu suppeasti, jos ollenkaan. Pelkistetyimmissä lupapäätöksissä käräjäoikeudet tutkimuksen mukaan vain toistivat pakkokeinolakiin kirjatut sanamuodot ja viittasivat hakemuksessa

[160] Roman Zakharov v. Russia (4.12.2015), kohdat 192-193 ja 263.
[161] Fredman 2018, s. 13.
[162] Fredman 2017, s. 366-367.

annettuihin perusteluihin eikä päätöksessä ollut kirjallista arviointia pakkokeinolupien edellytysten täyttymisestä.[163]

Oikeuspoliittisen tutkimuslaitoksen tutkimuksesta käy ilmi, että telepakkokeinoja koskevat käräjäoikeuden lupapäätökset olivat kaavamaisia. Tuomioistuimen päätösten lukeminen oli suurilta osin mielekästä vain yhdessä liitteenä olleen lupahakemuksen kanssa, jolloin pakkokeinon käyttämisen tarpeellisuus tuli ilmi. [164] Myös eduskunnan oikeusasiamies on useasti painottanut perustelun tärkeyttä niin suojelupoliisin hakemuksissa kuin tuomioistuimen päätöksissä koskien salaisia tiedonhankinta- ja pakkokeinoja. Jos tuomioistuin ei vaadi luvan hakijalta riittäviä perusteluja tiedonhankintamenetelmän käytölle tai vastaavasti itse laiminlyö riittävien perustelujen antamisen, on vaarana, että lupia myönnetään lainsäätäjän tarkoituksen vastaisesti.[165]

Tuomioistuimia ei tule hyödyntää tietoliikennetiedustelussa menetelmän ”hyväksyjänä”, vaan sen tulee toteuttaa sille tarkoitettua tehtävää eli aitoa laillisuuskontrollia. Kontrollin tavoitteena on, että tiedustelutoimintaa harjoitetaan lainmukaisesti siten, että huomioidaan tiedustelumenetelmien yleiset ja erityiset edellytykset sekä sääntelyyn sisältyvät periaatteet ja perus- ja ihmisoikeusvelvoitteet. Menettelyn asianmukaisuuden takaamiseksi tuomioistuimella tulee olla käytössään riittävästi tietoa käytettävistä sekä tiedustelumenetelmistä, niiden yleisestä ja erityisistä edellytyksistä että yksittäisen lupa-asian tosiseikoista. Tällöin korostuu taas tiedusteluviranomaisen velvollisuus toimittaa tuomioistuimelle lupavaatimuksessa tällaiset tiedot ja perustelut. [166]

Tuomioistuinkontrollin on tarkoitus toimia takeena siitä, että tiedustelua harjoitetaan lain mukaan ja siinä otetaan huomioon eri tiedustelumenetelmille säädetyt erityiset ja yleiset edellytykset. Tuomioistuinmenettelyn tulee myös varmistaa, että perus- ja ihmisoikeuksista johtuvat vaatimukset täyttyvät. Tiedustelumenetelmien käytöstä päättävän tuomioistuinkontrollin on oltava todellista ja perusteellista, sillä edellytys etukäteisestä luvasta on keskeinen takuu oikeusturvalle. Jotta tuomioistuin voi tehdä perusteellisen päätöksen ja kontrolli voi olla todellista, tulee tuomioistuimen saada riittävät tiedot, jotta se voi arvioida lupavaatimusta. Näyttövelvollisuus siitä, että niin yleiset ja erityiset edellytykset sekä tiedustelumenetelmien käytölle säädetyt yleiset periaatteet täyttyvät, on

[163] Vainio 2018, s. 11. Kts. myös de Gdozinsky & Niemi & 2009, s. 82.
[164] de Gdozinsky 2009 & Niemi, s. 83.
[165] Ks. esimerkiksi oikeusasiamiehen toimintakertomukset vuosilta 2015, s. 182; 2016, s.202; 2017, s. 180; 2018, s. 182.
[166] Melander 2018, s. 15.

tiedusteluviranomaisella. Niin ikään tiedusteluviranomaisella on velvollisuus antaa tuomioistuimelle tarpeelliset tiedot, jotta se voi arvioida lupavaatimusta riittävällä tasolla.[167]

4.2. Tuomioistuimen kokoonpano

Käräjäoikeus on poliisilain 5 a luvun 35 §:n mukaan on päätösvaltainen silloin, kun siinä on yksin puheenjohtaja. Lupamenettelyssä on lain mukaan oltava lisäksi paikalla suojelupoliisin päällystöön kuuluva virkamies. Käräjäoikeuden kokoonpanoa tulee kuitenkin oikeudenkäymiskaaren 2 luvun 11 §:n määrittämällä tavalla vahvistaa lainoppineella jäsenellä, ellei se ole ilmeisen perusteetonta ottaen huomioon asian laadun. Pääsääntöisesti kahden tuomarin kokoonpanoa vaadittaisiin esimerkiksi tilanteessa, jossa tuomioistuin käsittelee tiedusteluvalvontavaltuutetun määräystä tiedustelutoiminnan keskeyttämisestä tai lopettamisesta[168]. Perustuslakivaliokunta on kuitenkin lausunnoissaan nähnyt loogiseksi, että tiedustelumenetelmän käyttöön vaadittavan luvan myöntämistä ja tämän luvan perusteella suoritetun tiedustelun lopettamista tai keskeyttämistä käsiteltäisiin samanlaisissa kokoonpanoissa. Luvan myöntämisestä tehtävä päätös on myös keskeistä oikeusturvan toteutumisen kannalta, joten menettelyn toteuttamiseen on syytä kiinnittää erityistä huomiota.[169] Useamman tuomarin kokoonpanoa peräänkuulutettiin perustuslakivaliokunnalle annetuissa asiantuntijalausunnoissa. Useamman tuomarin kokoonpano nähdään perustelluksi, sillä tiedustelumenetelmät ja käyttöedellytykset ovat tuomareille uusia ja niihin liittyy huomattavia perus- ja ihmisoikeuskysymyksiä. Myös tiedusteluvalvontavaltuutetun läsnäoloa on etenkin alkuvaiheessa pidettävä pääsääntönä. [170]

Tiedusteluvalvontavaltuutetulla on tuomioistuinmenettelyssä mahdollisuus toteuttaa omalta osaltaan ennakollista valvontaa. Hänelle tai hänen määräämälleen virkamiehelle on valvontalain 14 §:ssä säädetty oikeus olla läsnä, kun tuomioistuin käsittelee tiedustelumenetelmää koskevaa lupa-asiaa. Tiedusteluvalvontavaltuutetun määräämän virkamiehen tulee olla asiantuntijavirkamies, joka toimii esittelijänä tai on muutoin asiaan perehtynyt. Tiedusteluvalvontavaltuutetulle tulee tiedusteluviranomaisen toimesta toimittaa tieto tuomioistuimelle annetusta lupahakemuksesta. Tieto lupahakemuksesta tulee toimittaa siten, että tiedusteluvalvontavaltuutetulla on ”mahdollisuus varautua osallistumaan kyseiseen

[167] HaVM 36/2018 vp, s. 61.
[168] HaVM 36/2018 vp, s. 63.
[169] PeVL 75/2018 vp, s. 3-4.
[170] Melander 2018, s. 14-15.

istuntoon”. Läsnäolo ei ole pakollista, vaan valtuutettu voi itse tapauskohtaisesti katsoa, näkeekö hän tarpeelliseksi käyttää läsnäolo- ja puheoikeuttaan. [171]

Tiedusteluvalvontavaltuutetun puheoikeudesta tuomioistuinkäsittelyssä säädetään poliisilain 5 a luvun 35 §:ssä, jossa säädetään siviilitiedustelussa sovellettavasta tuomioistuinmenettelystä. 35 §:n 2 momentin mukaan tiedusteluvalvontavaltuutetulle tai hänen määräämälleen virkamiehelle on varattava tilaisuus tulla kuulluksi ennen kuin lupa-asian käsittely päättyy. Puheoikeutta voi myös käyttää tiedusteluvalvontavaltuutetun määräämä virkamies. Perustuslakivaliokunta katsoi puheoikeudesta säätämisen edellytykseksi sille, että siviilitiedustelua koskeva laki voitiin käsitellä tavallisessa lain säätämisjärjestyksessä[172].

Kyseisellä oikeudella tiedusteluvalvontavaltuutetulle turvataan mahdollisuus saada reaaliaikaista tietoa tuomioistuinkäsittelyssä esillä olevista seikoista sekä niistä perusteista ja edellytyksistä, joita tiedustelumenetelmän käytölle esitetään. Lupahakemuksen perusteina käytettyjä seikkoja tullaan esittämään tuomioistuimelle myös suullisesti, jolloin tiedusteluvalvontavaltuutetun tiedonsaantioikeus täydentyy läsnäolo-oikeuden kautta. Valtuutetun läsnäolon nähdään myös ohjaavan lupavaatimuksen laatijaa esittämään riittävät perustelut tiedustelumenetelmän käyttölupaa koskevassa hakemuksessa.[173]

Tiedusteluvalvontavaltuutetulta vaadittua kokemusta ja oikeudellisesta sekä käytännön asiantuntemusta voidaan hyödyntää tuomioistuinkäsittelyssä juuri puhe- ja kyselyoikeuden kautta. Tiedusteluvalvontavaltuutetun mahdollisuus ilmaista näkemyksensä ja esittää kysymyksiä edistää omalta osaltaan tuomioistuimen mahdollisuutta toteuttaa tehokasta kontrollia ja toteuttaa oikeusturvaa: puhe- ja kyselyoikeus voi syventää ja monipuolistaa lupa-asian käsittelyä ja täten sillä voidaan varmistaa tuomioistuimen edellytykset arvioida tiedusteluviranomaiselta saatua informaatiota ja tehdä asianmukaisia päätöksiä. [174] Koska tiedusteluvalvontavaltuutetun läsnäolo- ja puheoikeus ovat oikeuksia, joiden käyttämisestä tiedusteluvalvontavaltuutettu päättää itse, ei tiedusteluvaltuutetun poissaolo tuomioistuinkäsittelystä viivästytä lupa-asian käsittelyä.[175]

Asiantuntijalausunnoissa on katsottu, että tuomioistuinkontrollin todellisuuden turvaamiseksi tulee tuomioistuimelle taata tarvittavat henkilö- ja aikaresurssit sekä koulutus. On myös

[171] HE 199/2018 vp, s. 58.
[172] PeVL 35/2018 vp, s. 29.
[173] HE 199/2017 vp, s. 58.
[174] LaVL 27/2018 vp, s. 7.
[175] HaVM 30/2018 vp, s. 62.

keskeistä, ettei tuomioistuin ole päätöstä tehdessään pelkästään lupavaatimuksen esittäjän antamien arvioiden varassa, vaan menettelyssä on mukana sellainen osapuoli, joka tarkastelee lupavaatimusta tiedustelun kohteena olevan henkilön tai henkilöiden perus- ja ihmisoikeuksien toteutumisen näkökulmasta, kuten tiedusteluvalvontavaltuutettu. [176] Tuomioistuimen asiantuntemuksen varmistamiseksi on asiantuntijalausunnoissa ehdotettu esimerkiksi ratkaisua, jossa tiedusteluasioita käsittelisivät vain laamannin erityisesti tähän tehtävään määräämät käräjätuomarit, jolloin koulutuksen kohdistaminen vain näihin tuomareihin olisi tehokasta.[177]

Esimerkiksi Ruotsissa luvan myöntämisestä huolehtii niin ikään tuomioistuin, mutta erona Suomen järjestelmään signaalitiedustelun lupa-asioita käsittelevä tuomioistuin (Försvarsunderrättelsedomstolen) on erityistuomioistuin, jonka kokoonpanona on puheenjohtaja, yksi tai kaksi varapuheenjohtajaa sekä kahdesta kuuteen muuta jäsentä. Puheenjohtajalta vaaditaan pysyvän tuomarin virkaa ja varatuomareilla on oltava oikeudellinen koulutus sekä aiempaa tuomarikokemusta. Muilla jäsenillä tulee olla tuomioistuimen toimintaan liittyvää relevanttia erityisasiantuntemusta.[178]

Lähtökohtaisesti olisi siis oikeusturvaa vahvistavana tekijänä pidettävä sitä, että ainakin aluksi tietoliikennetiedustelun lupa-asioista päätettäessä tuomioistuimen kokoonpanoa vahvistetaan lainoppineella jäsenellä. On toki huomioitava, että tiedusteluvalvontavaltuutetulle tai hänen määräämälleen virkamiehelle on poliisilain 5 a luvun 35 §:n 2 momentissa säädetty läsnä- ja puheoikeus tuomioistuimessa, kun käräjäoikeus päättää tiedustelumenetelmän käytöstä. Tiedusteluvalvontavaltuutettu tai hänen määräämänsä virkamies saa olla läsnä lupa-asian käsittelyssä sekä esittää näkemyksensä hakemuksesta ennen kuin tuomioistuin tekee asiasta päätöksen. Tiedusteluvalvontavaltuutettu kuitenkin päättää itse, käyttääkö hän läsnäolo- ja puheoikeuttaan, jolloin lupa-asian käsittely ei lykkäänny tai viivästy vaikka valtuutettu ei olisi paikalla.

Vaikka tiedusteluvalvontavaltuutetulle on määritelty perus- ja ihmisoikeuksien toteutumisen valvonnan tehtävä ja hänelle on varattu tuomioistuimessa puhe- ja kyselyoikeus sekä oikeus kannella päätöksestä hovioikeuteen, on huomattava, että läsnäolo on kuitenkin perimiltään vapaaehtoista. Lainsäädäntövaiheessa tiedusteluvalvontavaltuutetulle ehdotettiin vain läsnäolo-oikeutta tuomioistuinmenettelyssä, mutta asiantuntijalausunnoissa nostettiin

[176] Vainio 2018, s. 11
[177] Fredman 2018, s. 13.
[178] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 22.

toistuvasti esiin tarve myös puheoikeudelle[179]. Perustuslakivaliokunta huomioi lausunnot omassa lausunnossaan ja totesi puheoikeuden olevan edellytys sille, että lakiehdotus voitiin säätää tavallisessa lain säätämisjärjestyksessä. Perustuslakivaliokunta viittasi lausunnossaan tapaukseen Centrum för Rättvisa v. Sweden, jossa tuomioistuinmenettelyssä on mukana erityinen asiamies.[180]

Tuomiossaan Centrum för Rättvisa v. Sweden Euroopan ihmisoikeustuomioistuin katsoi läpinäkyvyyttä vahvistavaksi tekijäksi asiamiehen läsnäolon. Ruotsin tuomioistuinmenettelyssä on mukana erityinen asiamies (integritetsskyddsombud), jonka tehtävänä on puolustaa tiedustelun kohteena olevien yksityisyyttä. Asiamies ei edusta ketään yksittäistä henkilöä, vaan yksilöiden etua yleisellä tasolla. Tuomioistuin saa järjestää kuulemisen ja tehdä päätöksen ilman asiamiehen läsnäoloa vain silloin, jos kyse on erittäin aikaherkästä tilanteesta, jossa tiedustelusta saatava tieto kärsisi viivytyksestä. Asiamieheltä vaaditaan nykyistä tai aiempaa vakituisen tuomarin virkaa tai asianajajan koulutusta.[181] Asiamiehellä oli pääsy kaikkiin tapaukseen liittyviin asiakirjoihin ja hänellä on oikeus antaa lausuntoja. Vaikka asiamiehellä ei ole oikeutta kannella tuomioistuimen päätöksestä tai raportoida valvontaelimille epäsäännöllisyydestä, jo pelkästään hänen pakollinen läsnäolonsa istuntoihin oli ihmisoikeustuomioistuimen yksi salaista luonnetta kompensoiva osa.[182]

Ruotsin asiamies ei ole samankaltainen valvontalein kuin tiedusteluvalvontavaltuutettu. Jos kuitenkin verrataan Ruotsin yksilön oikeutta puolustavaa asiamiestä, jonka tuomioistuin katsoo kompensoivan tuomioistuimen lupaharkinnan salaista luonnetta, ja Suomen tiedusteluvalvontavaltuutettua, on löydettävissä niin yhtäläisyyksiä kuin perustavanlaatuisia erojakin. Ruotsin asiamieheltä vaaditaan tuomarin tai asianajajan työkokemusta, Suomessa tiedusteluvalvontavaltuutetulta vaaditaan valvontalain 6 §:n 3 momentissa oikeustieteen ylempää korkeakoulututkintoa muulta kuin kansainvälisen tai vertailevan oikeustieteen alalta. Tiedusteluvalvontavaltuutetulle on valvontalain 3 §:ssä säädetty oikeus saada tarvittavat tiedot valvontatehtäviensä hoitamiseksi, kuten asiamiehelläkin on oikeus saada kaikki tiedot yksittäistä tapausta kohden. Tiedusteluvalvontavaltuutetulla, kuten asiamiehelläkään, ei ole oikeutta valittaa tuomioistuimen päätöksestä. Tiedusteluvalvontavaltuutetulla on kuitenkin valvontalain 14 §:n 3 momentissa säädetty oikeus kannella hovioikeudelle tiedustelumenetelmästä. Keskeisin ero näiden kahden viranomaisen välillä on kuitenkin

[179] Esim. Fredman 2018, s. 5-6.
[180] PeVL 35/2018 vp, s. 29.
[181] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 22.
[182] Centrum för Rättvisa v. Sweden (19.7.2018), kohdat 137-138.

läsnäolo tuomioistuinkäsittelyssä. Suomen tiedusteluvalvontavaltuutetulle tai hänen määräämälleen virkamiehelle läsnäolo tiedustelumenetelmää koskevassa tuomioistuinkäsittelyssä on vapaaehtoista, kun taas Ruotsin lainsäädäntö vaatii asiamiehen läsnäoloa tuomioistuimessa[183].

Tiedusteluvalvontavaltuutetun läsnä- tai poissaolo ei itsessään liene sellainen tekijä, joka on ratkaiseva Euroopan ihmisoikeussopimuksen ja Suomen kansallisen lainsäädännön yhteensopivuuden kannalta. Varmaa kuitenkin lienee se, että itsenäisen ja riippumattoman valvontatahon läsnäolo ja oikeus puhua tuomioistuimessa ovat perus- ja ihmisoikeuksia vahvistavia tekijöitä ennakollisessa lupamenettelyssä. Tiedusteluvalvontavaltuutetun läsnä- ja puheoikeuden voidaan katsoa myös vähentävän riskiä edellä kuvatusta huolesta, että salaisten pakkokeinojen ja tiedonhankintakeinojen tuomioistuinkäsittelyssä tehdyt virheet toistuisivat myös siviilitiedustelumenettelyissä. Jos huolena on, että esimerkiksi tietoliikennetiedustelun käyttö sallitaan pääsääntöisesti aina eikä tuomioistuin todellisuudessa käytä sille säädettyä harkintaa asian suhteen, voi riippumattoman osapuolen läsnäolo vahvistaa yksityisyyden suojan turvaamista.

4.3. Kiiremenettely

Suojelupoliisin lupavaatimus on käsiteltävä tuomioistuimessa kiireellisesti, mutta jos asia ei kestä viivytystä, saa suojelupoliisin päällikkö tietoliikennetiedustelulain 9 §:n nojalla päättää tietoliikennetiedustelusta tuomioistuimen ratkaisuun asti. Tässäkin tapauksessa päätös tulee laatia kirjallisesti ja se on saatettava tuomioistuimen ratkaistavaksi 24 tunnin kuluessa tiedustelutoiminnan aloittamisesta. Tuomioistuin saa määrätä tietoliikennetiedustelun käytön lopetettavaksi ja siitä saadut aineistot sekä niistä luodut muistiinpanot hävitettäväksi, jos se katsoo, ettei sille ole tietoliikennetiedustelulain 4 §:n mukaan edellytyksiä tai kiirepäätöksestä ilmenee vakavuudeltaan 4 §:ään rinnastuvia virheitä. Tietoliikennetiedustelu voidaan määrätä tuomioistuimen toimesta myös osittain keskeytettäväksi. Tällaisissa tilanteissa esimerkiksi kiirepäätöksessä käytetty hakuehto on ollut liian epätarkka, jolloin kyseisen hakuehdon käyttö on lopetettava välittömästi ja sen avulla saatu tieto sekä muistiinpanot hävitettävä. Muilta osin tietoliikennetiedustelu voi tuomioistuimen päätöksen mukaan jatkua. [184] Tällä tavoin saatu tieto saadaan kuitenkin 9 §:n 2 momentin mukaan tallentaa ja säilyttää henkilötietojen

[183] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 22.
[184] HE 202/2017 vp, s. 247-248.

käsittelystä poliisitoimessa annetussa laissa tarkoitettuun rekisteriin niin kuin poliisilain 5 a luvun 46 §:n 1 momentissa on säädetty, eli jos voidaan olettaa, että on tehty sellainen rikos, josta voidaan ankarimmillaan tuomita vähintään kuusi vuotta vankeutta tai voidaan olettaa, että tällainen rikos on suunnitteilla ja se voitaisiin vielä estää.

Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään katsonut, että tilanteessa, jossa ulkoinen, oikeudellinen kontrolli voi hukata aikaa tiedustelutoiminnassa, tiedusteluviranomainen voi itse sallia tiedustelutoimen alkavaksi. Se kuitenkin korostaa, että menettelyn, jossa tiedustelun salliva taho on muu kuin oikeudellinen taho, tulee olla alisteinen jälkikäteiselle valvonnalle. Tapauksessa Szabó and Vissy v. Hungary Unkarin lainsäädännössä kansallisen turvallisuuspalvelun (National Security Services) johtajalla on oikeus antaa lupa tiedustelutoimintaan enintään 72 tunniksi, jos luvan hankkiminen lupaviranomaiselta, Unkarin tapauksessa oikeusministeriltä, vaarantaisi operaation. Euroopan ihmisoikeustuomioistuin kuitenkin muistuttaa, että tämänkaltaisessa käytännössä vaaditaan jälkikäteistä arviointia.[185]

Ratkaisussaan Centrum för Rättvisa v. Sweden tuomioistuin on aiempaan oikeuskäytäntöönsä nojautuen katsonut hyväksyttäväksi Ruotsissa sovelletun kiirepäätösmenettelyn, joka muistuttaa menettelyltään Suomeen säädettyä mallia. Ruotsissa tiedusteluviranomainen, FRA, saa itse myöntää luvan tiedusteluun, jos tuomioistuimelta haettu lupa voi viivyttää signaalitiedustelua tai muuten aiheuttaa tiedustelulle olennaista harmia. Tuomioistuin korostaa tällaisen menettelyn vastapainona oikeusturvakeinoja, joilla voidaan varmistaa, että menettelyä käytetään marginaalisesti ja perustellusti. EIT on nähnyt Ruotsin lainsäädännön kiirepäätösmenettelyn hyväksyttävänä, sillä Ruotsissa päätöksestä täytyy ilmoittaa viipymättä tuomioistuimelle, jonka tulee käsitellä asia nopeasti ja se voi määrätä tiedustelu keskeytettäväksi tai muutettavaksi.[186]

Tapauksessa Roman Zakharov v. Russia tuomioistuin puolestaan katsoi tämän kaltaisen menettelyn ihmisoikeussopimuksen vastaiseksi. Venäjän kansallinen lainsäädäntö sallii tiedonhankinnan aloittamisen ilman tuomioistuimen lupaa, jos on olemassa välitön uhka, että vakava tai hyvin vakava rikos toteutetaan. Kiiremenettely saa kestää enintään 48 tuntia ja tuomarille tulee ilmoittaa menettelyn käytöstä 24 tunnin sisällä sen aloittamisesta. Jos tiedusteluun ei ole saatu tuomarilta lupaa 48 tunnin kuluessa sen aloittamisesta,

[185] Szabó and Vissy v. Hungary (12.1.2016), kohta 81.
[186] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 140.

tiedustelutoiminta tulee keskeyttää välittömästi. Rikoksiin kohdistuvassa tiedonhankinnassa kiiremenettelyn käyttäminen vaatii välittömän uhan olemassaolon, mutta tätä ei lainsäädännössä vaadita tilanteissa, joissa kyse on uhasta kansalliselle, sotilaalliselle, taloudelliselle tai ekologiselle turvallisuudelle. Näissä tilanteissa riittää lain mukaan, että on olemassa tietoa näitä vaarantavista tekijöistä. Tästä seuraa Euroopan ihmisoikeustuomioistuimen mukaan se, että lainsäädäntö jättää tiedusteluviranomaisten oman harkinnan varaan, millaisissa tilanteissa kiiremenettelyä voidaan käyttää avaten mahdollisuuden järjestelmän väärinkäyttöön. Lisäksi, vaikka tiedusteluviranomainen on velvoitettu ilmoittamaan kiiremenettelyn käytöstä tuomarille, tuomarilla ei ole toimivaltaa arvioida kiiremenettelyn käytön oikeutusta tai päättää, tuleeko edeltävän 48 tunnin aikana kerätty materiaali tuhota vai säilyttää. Tuomarilla on toimivalta ainoastaan pidentää tiedustelumenetelmän käyttöä. Venäjän lainsäädäntö ei siis takaa tehokasta tuomioistuinkontrollia kiiremenettelyn käyttämiseen.[187]

Vertailukohtana tuomioistuin on edellä mainittua arvioidessaan käyttänyt tapausta Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria, jossa laissa tuotiin esiin, että ilman tuomioistuimen lupaa suoritettava kiiremenettely koskee vain sellaisia tilanteita, joissa on välitön riski vakavan, tahallinen teon toteuttamiseen tai välitön uhka kansalliselle turvallisuudelle. Tuomioistuimen lupa vaadittiin lisäksi viimeistään 24 tunnin kuluttua kiiremenettelyyn perustuvan tiedustelutoimen alkamisesta ja jos sitä ei saada, menetelmän käyttö tulee lopettaa. Tuomioistuimen päätöksestä kerätty materiaali saadaan joko säilyttää tai se tulee hävittää. Euroopan ihmisoikeustuomioistuin näki lainsäädännön rajaavan kiiremenettelyn käyttämisen siihen, että poikkeusmenettelyä tulee käyttää harkiten ja vain silloin kun se on oikeutettua.[188]

Suojelupoliisin päätöksen perustuva tietoliikennetiedustelun ei ole tarkoitus muodostua pääsäännöksi vaan jäädä marginaaliseksi. Tätä menettelyä voidaan soveltaa esimerkiksi tilanteessa, jossa tuomioistuimen lupapäätöksen odottaminen aiheuttaisi sellaisen materiaalin menetyksen, joka tiedustelutoiminnalla pyrittiin saamaan haltuun.[189] Kiiremenettelyssä näyttää siis korostuvan suojelupoliisin oma harkinta. Tärkeänä oikeussuojakeinona on kuitenkin pidettävä Euroopan ihmisoikeustuomioistuimen oikeuskäytännössäkin mainittu

[187] Roman Zakharov v. Russia (4.12.2015), kohdat 35 ja 266.
[188] Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria (28.6.2007), kohdat 16 ja 82.
[189] HE 202/2017 vp, s. 127.

jälkikäteinen, tuomioistuimen suorittama arviointi lupapäätöksen laillisuudesta ja mahdollisuus määrätä tällä tavoin saatu tieto hävitettäväksi.

Asiantuntijalausunnoissa perustuslakivaliokunnalle on kuitenkin kiinnitetty huomiota 9 §:n 2 momenttiin: vaikka on menetelty virheellisesti, lainvastaisesti saadun tiedon hyödyntäminen on tähän perustuen sallittua [190]. Menettelyn sallivassa säännöksessä on toki viitattu ankarimpiin rikostyyppeihin, mutta kuitenkin väärin perustein suoritetulla menettelyllä viranomaisen haltuun saatua tietoa on lain nojalla sallittua hyödyntää. Tässä voidaan perustellusti pohtia, avaako tällainen järjestely mahdollisuuden järjestelmään väärinkäyttöön. Toisaalta, tässäkin tapauksessa oikeus tiedon hyödyntämiseen on rajoitettu lailla vain tietyn typpisiin tilanteisiin eikä täten jätä väärin perustein hankitun tiedon säilyttämisestä päättämistä tiedusteluviranomaisen tai edes tuomioistuimen harkinnan varaan.

[190] Viljanen J. 2018, s. 7.

5. Lupavaatimus ja –päätös ennakollisessa lupamenettelyssä

5.1. Lupavaatimus ja -päätös

Kuten edellisessä osiossa todettiin, tietoliikennetiedustelua käyttääkseen tulee suojelupoliisin hakea siihen kussakin yksittäistapauksessa lupa tuomioistuimelta. Lupamenettely toimitetaan Helsingin käräjäoikeudessa. Lupavaatimus tulee tietoliikennetiedustelulain 7 §:n 1 momentin mukaan tehdä kirjallisessa muodossa ja sen laatijana on oltava suojelupoliisin päällikkö. Edellytys siitä, että vaatimuksen laatija on erityisen korkean virka-aseman haltija, johtuu tietoliikennetiedustelun erityisluonteesta verrattuna muihin tiedonhankinta- ja tiedustelumenetelmiin[191]. Tuomioistuimen suorittama ennakkovalvonta toimii suojelupoliisin harkintavallan rajoittajana, sillä lupapäätös määrittää rajat sille, millä ehdoilla tietoliikennetiedustelua toteutetaan.

Tietoliikennetiedustelua koskevassa lupavaatimuksesta ja vastaavasti tämän vaatimuksen johdosta tehtävässä tuomioistuimen päätöksessä on käytävä ilmi ne seikat, joista säädetään tietoliikennetiedustelulain 7 §:n 2 momentissa. Näitä ovat

1. tietoliikennetiedustelun kohteena oleva, lain 3 §:ssä tarkoitettu toiminta;
2. ne tosiseikat, jotka koskevat kohdassa 1 tarkoitettua toimintaa;
3. ne tosiseikat, joihin perustuvat tietoliikennetiedustelun käytön edellytykset ja tehokkuus;
4. tietoliikennetiedustelussa käytettävät hakuehdot tai hakuehtojen luokat perusteluineen;
5. se Suomen rajan ylittävä viestintäverkon osa, jonka sisässä liikkuvaan tietoliikenteeseen hakuehtoja käytetään perusteluineen;
6. luvan voimassaoloaika kellonajan tarkkuudella;
7. se tehtävään määrätty ja tiedustelumenetelmien käyttöön perehtynyt suojelupoliisin päällystöön kuuluva poliisimies, joka valvoo ja johtaa tietoliikennetiedustelua sekä
8. mahdolliset rajoitukset ja ehdot koskien tietoliikennetiedustelua.

Mietinnössään perustuslain 10 §:n muuttamisesta perustuslakivaliokunta korosti, että tiedustelutoimivaltuuksien käyttämiseen lupaa hakevan tahon on jokaisessa yksittäisessä tilanteessa esitettävä riittävät perustelut ja osoitettava, että tiedonhankinta ja perusoikeuksien rajoittaminen ovat välttämättömiä ja tehokkaita keinoja toteuttaa tiedonhankintaa. [192] Perustuslakivaliokunnalle siviilitiedustelulaista annetuista asiantuntijalausunnoissa kiinnitettiin huomiota edellä sanottuun ja katsottiin, että lakiesityksessä ei nimenomaisesti vaadittu tällaisten perusteiden sisällyttämistä lupavaatimukseen. Tällöin nähtiin tarpeelliseksi

[191] HE 202/2017 vp, s. 242.
[192] PeVM 4/2018 vp, s. 9.

lisätä listaan kohta, jossa vaaditaan esitettäväksi edellä esitettyyn perustuvat tosiseikat sekä se, että käytettävissä ei ole perusoikeuksiin vähemmän puuttuvia tapoja hankkia tietoa.[193]

Perustuslakivaliokunta viittasi vastaavasti tietoliikennetiedustelulaista antamassa lausunnossaan yllä mainittuun mietintöönsä ja muistutti, että tiedustelun yleisten periaatteiden ja tiedustelutoimenpiteen yhtenäisyyden osoittaminen on tiedusteluviranomaisen vastuulla. Perustuslakivaliokunta katsoi, että tästä velvollisuudesta tulee säätää laissa tarkemmin. Toimivallan käyttöä rajoittavat säännöt ja periaatteet nähtiin käsillä olevassa lainsäädännössä keskeiseksi ja niiden säätäminen niin tarkasti ja yksiselitteisesti kuin mahdollista luo edellytykset sille, että ne tosiasiassa myös toteutuvat.[194]

Perustuslakivaliokunnan lausunnosta johtuen 7 §:n 2 momentin 3 kohtaan lisättiin tietoliikennetiedustelun edellytyksiin liittyvien tosiseikkojen esittämisen lisäksi vaatimus niistä tosiseikoista, joihin perustuu tietoliikennetiedustelun käytön tehokkuus. Tämän lisäksi 3 kohtaan ei tehty muutoksia, ja hallintovaliokunta viittasikin perusteluissaan siihen, että tietoliikennetiedustelun yleisiksi edellytyksiksi on uuden muotoilun mukaan laissa määritelty välttämättömyys sekä tietoliikennetiedustelun viimesijaisuus suhteessa muihin tiedustelumenetelmiin. Tällöin 7 §:n 2 momentin 3 kohdassa tarkoitettuihin edellytyksiin sisältyy vaaditut tehokkuus, välttämättömyys ja viimesijaisuus.[195]

Lupavaatimuksen ja –päätöksen sisältö vastaa pitkälti sellaista mallia, jota Euroopan ihmisoikeustuomioistuin on pitänyt oikeuskäytännössään hyväksyttävänä. Tuoreessa ratkaisussaan Centrum för Rättvisa v. Sweden tuomioistuin arvioi Ruotsissa käytettävää televiestintään kohdistuvaa tukkutiedustelua (”bulk interception of electronic signals”), ja totesi järjestelmän kokonaisuudessaan yhteneväksi ihmisoikeussopimuksen 8 artiklan kanssa. Edellä esitetyssä luvan ja päätöksen sisältövaatimuksessa voidaan nähdä yhteys Ruotsin signaalitiedustelussa vaadittavaan lupaan. Ruotsin tiedustelulainsäädännön mukaan lupahakemuksessa tulee eritellä tiedusteluviranomaiselle (FRA) annettu toimeksianto, johon sisältyy tieto oleellisesta ja yksityiskohtaisesta toimintaohjeesta (information on the relevant detailed tasking directive[196]) sekä tiedustelun tarpeesta. Luvassa tulee myös yksilöidä ne kantoaallot (signal carriers), joihin tiedustelu kohdistuu, käytettävät hakuehdot tai niiden

[193] Lavapuro 2018, s. 7.
[194] PeVL 35/2018 vp, s. 16.
[195] HaVM 30/2018 vp, s. 96.
[196] Ruotsissa hallitus määrittelee ne toimet, johon signaalitiedustelua saa kohdistaa ja antaa vuosittain yleiset toimintaohjeet. Lisäksi hallitus määrittelee ne tahot, jotka voivat määrätä yksityiskohtaisempia toimintaohjeita (detailed tasking directives). Ks. Centrum för Rättvisa v. Sweden (19.7.2018, kohta 8).

luokat (search terms, categories of search terms) sekä tiedustelutoiminnan ajallinen kesto.[197] Luvan myöntämisestä myös Ruotsissa vastaa tuomioistuin, ja Euroopan ihmisoikeustuomioistuin on nähnyt sen valvonnan laajaksi esimerkiksi juuri sen vuoksi, että tuomioistuinvalvonnalle alistetaan hakuehdot sekä tiedustelun kohteena olevat kantoaallot. Tällöin tiedustelutoimintaan kohdistuva ennakollinen valvonta on erityisen tärkeä, sillä tulkitsemalla signaalitiedustelun toteuttamisen ja valtuuttamisen laajuutta se rajoittaa tiedusteluviranomaisen harkintavaltaa.[198]

Myös Ruotsin järjestelmässä tuomioistuimen tiedusteluviranomaisen vaatimuksesta myöntämä lupa on sisällöltään pääpiirteittäin sama kuin lupavaatimus. Myönteinen päätös luvasta voidaan tehdä, jos tiedustelutehtävä ja käytettävät hakuehdot tai niiden luokat ovat yhdenmukaiset lainsäädännön kanssa, tietoja ei voida hankkia vähemmin puuttuvin keinoin ja lupavaatimus ei koske pelkästään yksittäistä, luonnollista henkilöä. Lisäksi vaaditaan, että tiedustelulla voidaan olettaa saatavan sellaista tietoa, jonka arvo on suurempi kuin mahdollinen yksityisyyteen puuttuminen. Lupapäätökseen voidaan myös sisällyttää ehtoja ja rajoitteita koskien tiedustelutehtävää. [199] Suomen lainsäädännössä tuomioistuimen antama päätös voi sisältää niin ikään ehtoja ja rajoituksia tietoliikennetiedustelun käytölle. Lain esitöissä viitataan näiden määrittelyssä esimerkiksi hakuehtoja koskeviin rajoituksiin.[200]

Iso-Britanniassa luvan myöntämisestä vastaa tuomioistuimen sijaan valtiosihteeri. Tapauksessa Big Brother Watch and Others v. The United Kingdom valittajien mukaan tiedustelutiedon seulominen ei ollut yhteensopiva Euroopan ihmisoikeussopimuksen 8 artiklan kanssa. Luvan myöntävän valtiosihteerin tulee tiedustelutoiminnan sallivan luvan ohella laatia lupaa rajoittava todistus (certificate), ja siinä ei vaadittu mainittavaksi tiedustelulla saadun tiedon seulomiseen käytettäviä hakuehtoja (selectors) eikä niitä alistettu valvonnalle.[201] Valtiosihteerin myöntämän luvan oheen liitettävä todistus on asiakirja, jossa valtiosihteeri vahvistaa katsovansa, että tiedustelulla saadun materiaalin tutkiminen on välttämätöntä lainsäädännössä erikseen määritellyn päämäärän saavuttamiseksi. Sen tarkoituksena on varmistaa, että tiedustelulla saadun materiaalin suodatus tapahtuu siten, että luonnollisen henkilön suorittamaan tutkintaan päätyy vain todistuksessa kuvattu

[197] Centrum för Rättvisa v. Sweden (19.7.2018), kohdat 18 ja 19.
[198] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 139.
[199] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 20.
[200] HE 202/2017 vp, s. 246.
[201] Big Brother Watch and Others v. The United Kingdom (13.9.2018) kohta 274.

materiaali. [202] Arvioidessaan luvan oheen liitettävää todistusta Euroopan ihmisoikeustuomioistuin yhtyi parlamentin tiedustelu- ja turvallisuuskomitean (Intelligence and Security Committee of Parliament) vuonna 2015 laatimaan raporttiin. Raportissa kiinnitettiin huomiota siihen, että itse lupa oli erittäin lyhyt. Lisäksi lupaan liitettävässä todistuksessa ne kategoriat, joissa määriteltiin, millainen tietoliikenne voidaan ottaa tutkittavaksi, oli määritelty erittäin laajoin ilmauksin. Todistuksissa käytettiin ilmaisuja kuten ”materiaali, joka sisältää tietoa terrorismista sisältäen, mutta ei rajoitettu näihin: terroristijärjestöt, terroristit, aktiiviset kannattajat, iskun suunnittelu, varojen kerääminen”. Suuremmaksi ongelmaksi tuomioistuin kuitenkin näki sen, että kaapatun materiaalin seulomiseen käytettäviä valitsimia (selectors) ei alistettu itsenäiselle valvonnalle. [203]

Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään katsonut, että tiedustelutoimen sallivassa päätöksessä on mainittava se henkilö, johon tiedustelu kohdistuu tai ne edellytykset, joiden perusteella tiedustelua harjoitetaan. Päätöksessä tulee siis yksilöidä esimerkiksi nimi, osoite, puhelinnumero tai muu olennainen tieto. Tapauksessa Roman Zakharov v. Russia tuomioistuin arvioi Venäjän kansallista lakia koskien puhelinviestintään kohdistuvaa tiedustelua. Venäjän kansallisessa lainsäädännössä ei edellytetty, että tuomioistuimelle tehdyssä lupavaatimuksessa mainitaan se henkilö, kehen tiedustelutoiminta kohdistuu eikä tiedustelun kestoa. Tämä johti siihen, että tuomioistuimet saattoivat myöntää sellaisia lupia, joissa ei eritelty tiedustelun kohdehenkilöä tai –puhelinnumeroa, vaan sallivat puhelinviestinnän tarkkailun kokonaisilla alueilla. Euroopan ihmisoikeustuomioistuin katsoi tuomiossaan tämän olevan yksi syy siihen, että kyseisessä järjestelmässä tiedustelulupien myöntämiseen vaadittu prosessi ei pysty takaamaan, että lupia ei myönnetä umpimähkäisesti, epätasaisesti tai ilman asianmukaista harkintaa.[204]

Yllä olevista esimerkeistä voidaan siis nähdä, että Suomeen säädettyä, pitkälti Ruotsin lainsäädäntöä vastaavaa mallia voidaan ainakin Centrum för Rättvisa -tapaukseen nojautuen pitää yhdenmukaisena Euroopan ihmisoikeussopimuksen kanssa. Tärkeää kuitenkin lienee myös yksittäisten osien tarkempi tarkastelu, kuten Venäjän ja Iso-Britannian esimerkit osoittavat. Arvioidessaan lupavaatimuksen sisältöä tuomioistuin nojautuu täysin niiden tietojen varaan, jotka suojelupoliisi sille antaa. Siksi onkin tärkeää, että lupavaatimuksen sekä -päätöksen perusteluissa esitetään ne seikat, joihin niin luvan hakeminen kuin annettu päätös

[202] Big Brother Watch and Others v. The United Kingdom (13.9.2018) kohta 90, osa 6.14.
[203] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 342. Ks. myös kohta 156. Valitsimiin kohdistuvan valvonnan puutetta käsitellään laajemmin jäljempänä osiossa 5.5.
[204] Roman Zakharov v. Russia (4.12.2015), kohdat 264-265; 267.

perustuvat. Lisäksi lupapäätöksestä tulee käydä ilmi siihen käytetty oikeudellinen päättely. Käsittely, jossa perinteisen vastaaja-kantaja asettelun sijaan paikalla on lain mukaan oltava vain ratkaisun tekijä sekä suojelupoliisin virkamies, korostaa tuomarin aktiivisutta käyttää kyselyoikeuttaan sekä velvollisuutta selvittää käsiteltävään asiaan liittyvät tosiasiat.[205]

Vaikka tietoliikennetiedustelun käyttö on alisteinen tuomioistuimen luvalle, tulee lupavaatimusta laatiessa kiinnittää huomiota myös sisäisen laillisuusvalvonnan toimivuuteen. Sisäisen laillisuusvalvonnan kohteita ovat lupavaatimukseen ja -päätökseen sisällytettävät seikat. Kohdistamiseen sekä yleisten edellytysten arviointiin on syytä kiinnittää erityistä huomiota. Suojelupoliisin tulee lupavaatimusta muotoillessaan arvioida, onko tiedustelumenetelmän käytölle todellisuudessa riittävät perusteet ja jos näin ei ole, lupavaatimusta ei ole syytä saattaa tuomioistuimen arvioitavaksi.[206]

Lupavaatimusta ja -päätöstä arvioidessa on myös syytä ottaa huomioon tietoliikennetiedustelulain 1 §:n 2 momentti, joka pitää sisällään vaatimukset poliisilaissa säädettyjen yleisten poliisioikeudellisten periaatteiden noudattamisesta. Pykälän 2 momentissa vaaditaan tietoliikennetiedustelun käyttämisessä noudattamaan poliisilain 1 luvun 2-5 §:ssä säädettyjä periaatteita, joita ovat perus- ja ihmisoikeuksien kunnioittaminen, suhteellisuusperiaate, vähimmän haitan periaate sekä tarkoitussidonnaisuuden periaate. Vastaavasti tiedusteluviranomaista sitoo tietoliikennetiedustelulain 1 §:n 3 momentissa säädetty erillinen syrjintäkielto, joka velvoittaa kohdistamaan tietoliikennetiedustelun syrjimättömästi. Koska tietoliikennetiedustelua harjoitetaan myönteisen lupapäätöksen rajoissa, tulee tuomioistuimen varmistua siitä, että myös tämä edellytys täyttyy.

Kokonaisuutena se, että lupavaatimuksen ja -päätöksen sisällöstä säädetään laissa, voidaan katsoa edellä osiossa 3.2.1 käsitellyn laillisuusvaatimuksen eri osa-alueisiin liittyväksi. Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä laillisuusvaatimukseen sisältyy oikeusvaltioperiaate, joka Suomessa sisältyy perustuslain 2 §ään. Periaatteen mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa tulee noudattaa lakia. Kun lupavaatimukselle ja -päätökselle on määritelty laissa tarkat sisältövaatimukset, ja julkisen vallan tulee perustaa toimintansa lakiin ja noudattaa sen säännöksiä, rajoittaa lupapäätöksen sisällön määrittely omalta osaltaan suojelupoliisin harkintavaltaa suorittaa

[205] HE 202/2017 vp, s. 206.
[206] Lohse & Viitanen 2019, s. 164.

tietoliikennetiedustelua. Samalla se täyttää ennakoitavuusvaatimusta siltä osin, että yksittäisen kansalaisen saatavilla ovat ne raamit, joiden sisässä tietoliikennetiedustelua tulee harjoittaa.

5.2. Luvan voimassaolo

Luvan enimmäisvoimassaoloajaksi on tietoliikennetiedustelulain 7 §:n 3 momentissa määritelty kuusi kuukautta kerrallaan. Kuuden kuukauden enimmäisaika ei kuitenkaan tarkoita, että lupa olisi aina mahdollista hakea kuudeksi kuukaudeksi kerrallaan tai että tuomioistuimen tulisi myöntää aina enimmäisajan mukainen lupa. Poliisilain 3 §:n ja 4 §:n mukainen suhteellisuus- sekä vähemmän haitan periaate tulevat sovellettavaksi lupaa haettaessa ja myönnettäessä, jolloin tietoliikennetiedustelun käytön kestoa tulee harkita aina tapauskohtaisesti. Jos tietoliikennetiedustelulla haluttu lopputulos saavutetaan aikaisemmin tai tietoliikennetiedustelulle ei ole enää edellytyksiä ennen määräajan päättymistä, on tiedustelutoiminta lopetettava.[207] Asiantuntijalausunnoissa on esitetty, että luvan kesto tulee suhteuttaa myös tiedustelutoiminnan välttämättömyyteen.[208]

Euroopan ihmisoikeustuomioistuin on vuosien ajan oikeuskäytännössään linjannut, että oikeus luvan keston määrittelyyn on mahdollista myöntää luvan myöntämisestä ja uusimisesta päättävälle taholle, mutta tällöin vaaditaan riittävien oikeussuojakeinojen olemassaoloa. Kotimaisessa lainsäädännössä tulee selkeästi määritellä, minkä ajanjakson jälkeen lupa ei ole enää voimassa, missä olosuhteissa lupa on mahdollista uusia ja sekä ne olosuhteet, joissa lupa raukeaa.[209] Enintään kuuden kuukauden voimassaolon lisäksi Suomessa ei ole säädetty erikseen luvan uusimisesta koskevista tekijöistä, mikä käytännössä voi johtaa siihen, että lupa voidaan uusia rajattomasti. Tietoliikennetiedustelulain 7 §:n 4 momentissa on kuitenkin selkeästi ilmaistu, että tietoliikennetiedustelu tulee lopettaa ennen määräajan päättymistä, jos haluttu päämäärä on saavutettu tai sille ei ole enää perusteita. Lisäksi tiedusteluvalvontavaltuutetulle on valvontalain 15 §:ssä säädetty oikeus keskeyttää tai lopettaa tiedustelumenetelmän käyttö, jos viranomainen on toiminut lainvastaisesti. Luvan lopettamiseen vaadittujen olosuhteiden kirjaaminen lakiin on nähtävä oikeussuojakeinona: ratkaisussaan Big Brother Watch and Others v. The United Kingdom Euroopan ihmisoikeustuomioistuin viittasi ratkaisuunsa Kennedy v. The United Kingdom ja katsoi, että

[207] HE 202/2017 vp, s. 246.
[208] Vainio 24.10.2018, s. 10.
[209] Ks. esim. Kennedy v. The United Kingdom (18.5.2010), kohta 161; Klass and Others v. Germany (6.9.1978), kohta 52; Weber and Saravia v. Germany (29.6.2006), kohta 98; Roman Zakharov v. Russia (4.12.2015), kohta 250; Centrum för Rättvisa v. Sweden (19.6.2018), kohta 127.

valtiosihteerille säädetty oikeus keskeyttää tiedustelumenetelmän käyttö aiheutti käytännössä sen, että tiedustelua toteuttavan tahon oli jatkuvasti arvioitava lupiensa tarkoituksenmukaisuutta, mitä puolestaan on pidettävänä hyvänä oikeussuojakeinona järjestelmän väärinkäyttöä vastaan[210].

Tuomiossaan Roman Zakharov v. Russia Euroopan ihmisoikeustuomioistuin kiinnitti huomiota siihen, että lainsäädännössä määriteltiin selvästi aikaraja, jonka jälkeen tiedusteluun myönnetty lupa ei ollut enää voimassa ja lisäksi luvan uusimiseen vaaditut tekijät oli yksilöity lainsäädännössä: tuomioistuin voi myöntää luvan kuudeksi kuukaudeksi kerrallaan ja pidentää sen voimassaoloa kuudella kuukaudella tarkasteltuaan uudestaan siihen liittyviä, olennaisia materiaaleja. Ongelmallista kuitenkin oli, että laissa ei ollut säännelty siitä, missä olosuhteissa tiedustelumenetelmän käyttö tuli lopettaa. Venäjän kansallinen lainsäädäntö ei täten tarjonnut riittäviä oikeussuojakeinoja sen suhteen, milloin tiedustelu tulee lopettaa. Euroopan ihmisoikeustuomioistuin katsoi tämän olevan yksi syy siihen, että järjestelmä ei ollut yhteensopiva Euroopan ihmisoikeussopimuksen 8 artiklan kanssa.[211]

Ruotsin signaalitiedustelua koskevassa lainsäädännössä lupa voitiin vastaavasti myöntää enintään kuudeksi kuukaudeksi kerrallaan, ja lain mukaan sille voitiin myöntää jatkoaikaa uuden tarkastelun jälkeen niin ikään enintään kuudeksi kuukaudeksi. Myöskään Ruotsin lainsäädännössä ei ollut säännöksiä sille, missä olosuhteissa signaalitiedustelun käyttö tuli lopettaa. Tuomioistuin kuitenkin huomioi, että lupa oli voimassa enintään vain kuusi kuukautta ja luvan uusiminen edellyttää tosiasioiden uudelleen arviointia. Lisäksi ulkomaantiedustelun valvontaryhmällä (Foreign Intelligence Inspectorate) oli oikeus keskeyttää tiedustelutoiminta, jos sen suorittamassa tarkastuksessa havaitaan luvanvastaista tiedustelutoimintaa, mutta sillä ei kuitenkaan ollut velvollisuutta valvoa jokaista tiedustelutehtävää. Euroopan ihmisoikeustuomioistuimen mukaan tuli huomioida, että signaalitiedustelun kohteena olivat kansallista turvallisuutta uhkaavat tekijät eikä se kohdistunut rikoksista epäiltyihin yksittäisiin henkilöihin, missä tapauksessa luvan uusimiseen liittyvien säännösten tulisi olla selkeämmät. Lisäksi tuomioistuin viittasi tietosuojaviranomaisen (Data Protection Authority) raporttiin, josta kävi ilmi FRA:n jatkuvasti arvioivan tiedustelutoiminnalla saatujen henkilötietojen tarpeellisuutta signaalitiedustelutoimintaan. Kaiken kaikkiaan Euroopan ihmisoikeustuomioistuin oli

[210] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 360. Ks. myös Kennedy v. The United Kingdom (18.5.2010), kohta 161.
[211] Roman Zakharov v. Russia (4.12.2015), kohdat 251 ja 302.

vakuuttunut, että Ruotsin kansallinen lainsäädäntö koskien luvan pituutta, uusimista ja lopettamista sisältää riittävät oikeussuojakeinot.[212]

Tuomiossa Big Brother Watch and Others v. The United Kingdom valittajat nostivat esiin, että tiedusteluun tarkoitettu lupa voitiin lainsäädännön perusteella uusia käytännössä rajattomasti kuuden kuukauden välein. Euroopan ihmisoikeustuomioistuin kuitenkin katsoi, että Iso-Britannian lainsäädäntö tarjosi tarpeelliset oikeusturvakeinot. Lainsäädännössä määriteltiin lupien enimmäisvoimassaoloajaksi kuusi kuukautta, ja lupa oli mahdollista uusia missä tahansa vaiheessa voimassaoloajan puitteissa. Luvan uusimiseksi laadittavaan hakemukseen tuli sisällyttää samat tiedot kuin alkuperäiseen hakemukseen ja sen lisäksi siinä tuli arvioida siihen saakka saavutetun tiedustelutiedon arvo sekä tehdä selkoa siitä, miksi tiedustelun jatkaminen on välttämätöntä ja oikeasuhtaista. Lisäksi valtiosihteerillä oli velvollisuus peruuttaa lupa, jos hän katsoi, ettei tiedustelutoiminnalle ollut enää perusteita.[213]

Verrattaessa kolmea yllä esitettyä järjestelmää voidaan huomata, että tehokkaalla, tiedustelutoimintaan kohdistetulla ulkoisella valvonnalla näyttää olevan mahdollista kompensoida jopa Euroopan ihmisoikeustuomioistuimen vaatimia lain sisältövaatimuksia. Lisäksi erityisesti tiedustelutoiminnan tarpeellisuuden jatkuvan arvioinnin voidaan katsoa nousevan keskiöön. Jonkinlaista kompensaatiota voidaan Suomen tietoliikennetiedustelussa vaatia, sillä kuten edellä todettu, ei laissa tai sen esitöissä mainita erillisiä säännöksiä luvan uusimiseksi. Lupa on lain mukaan voimassa enintään kuusi kuukautta kerrallaan, josta on pääteltävissä, että tiedusteluviranomaisella on luvan uusimiseen mahdollisuus. Tapauksessa, jossa suojelupoliisi hakee jatkoaikaa tietoliikennetiedusteluun, tulisi etenkin välttämättömyysvaatimuksen arviointi suorittaa erittäin tarkasti niin tuomioistuimessa kuin jo suojelupoliisin sisäisessä valvonnassa. Esimerkiksi yllä esitetty Iso-Britannian lainsäädäntö koskien luvan uusimista sisälsi tiedusteluviranomaisen velvollisuuden esittää perusteet jatkoajalle sekä siihen asti saavutetun tiedustelutiedon merkittävyys. Tämänkaltainen järjestelmä voi vahvistaa Euroopan ihmisoikeustuomioistuimen hyvänä pitämää jatkuvaa

[212] Centrum för Rättvisa v. Sweden (19.6.2018), kohdat 23 ja 128-130. Tätä näkökulmaa kritisoitiin Centrum för Rättvisan toimesta Suuren jaoston kuulemisessa tapaukseen liittyen ja nostettiin esiin se, että Ruotsin sääntely ei täytä Roman Zakharov -tapauksessa nimettyä vaatimusta siitä, että luvan keskeyttämiseen johtavista olosuhteista tulee säätää laissa. Ks. Centrum för Rättvisa v. Sweden: The Applicant's Further Written Observations on Admissibility and Merits, 3.7.2019, kohdat 89-90.

[213] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 276 ja 358-359. Weber and Saravia -minimivaatimuksista ks. tämän tutkimuksen osio 3.2.1.

tiedustelutoiminnan tarkoituksellisuuden arviointia ja samalla se nostaisi kynnystä rasittaa tuomioistuinta perusteettomilla hakemuksilla.

Euroopan ihmisoikeustuomioistuimen määrittelemissä, laillisuusvaatimukseen liittyvissä minimivaatimuksissa (minimum safeguards) mainitaan, että kansallisessa lainsäädännössä tulee säätää tiedustelutoiminnan keston rajoista sekä olosuhteista, jolloin tiedustelutoiminta tulee lopettaa. Suomen kansallisessa lainsäädännössä molemmista säädetään tässä käsitellyn lainkohdan yhteydessä. Edellä käsitellyn perusteella voidaan katsoa, että Euroopan ihmisoikeustuomioistuin on linjannut, että kansallisessa laissa tulee luvan voimassaolon lisäksi säätää tiedustelun lopettamiseen johtavista olosuhteista sekä luvan uusimisesta. Oikeuskäytännöstä nähtiin, että Iso-Britannian tapauksessa lainsäädännössä vaadittiin jo saavutetun tiedon arviointia sekä perusteluja siitä, miksi lupa tulee uusia. Vastaavasti Ruotsin ja Venäjän tiedustelutoiminnassa luvan uusimiseen vaadittiin, että tiedustelutehtävää arvioidaan uudelleen.

Suomeen säädetyssä tietoliikennetiedustelulaissa luvan uusimisen olosuhteista ei ole säädetty. Lupa voi olla lain mukaan voimassa kuusi kuukautta kerrallaan, mikä aika on yllä esitetyssä oikeuskäytännössä katsottu hyväksyttäväksi. Kun asiaa kuitenkin arvioidaan laillisuusvaatimuksen kautta, voidaan nostaa esiin se, että uusimista rajoittavia säännöksiä ei ole laissa olemassa. Tällöin korostunee, kuten useassa muussakin jäljempänä käsiteltävässä kohdassa, sekä suojelupoliisin että tuomioistuimen oma arviointi ja harkinta. Erityisesti tässä voidaan kummankin tahon osalta pohtia luvan uusimisen välttämättömyyttä ja korostaa suojelupoliisin vastuuta suorittaa jatkuvaa arviointia tietoliikennetiedustelun käytön tarpeellisuudesta.

5.3. Tietoliikennetiedustelun kohde

Tietoliikennetiedustelun kohteet ovat samat kuin poliisilain 5 a luvun 3 §:ssä luetellut siviilitiedustelun kohteet, ja ne on lueteltu säännöksissä tyhjentävästi[214]. Siviilitiedustelun kohteena ovat:

1. terrorismi;
2. ulkomainen tiedustelutoiminta;
3. joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö;
4. kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö;

[214] HaVM 30/2018 vp, s. 48.

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, 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; sekä
11. kansanvaltaista yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus.

Lainsäädäntövaiheessa pykälän sanamuotoa tarkennettiin. Asiantuntijalausunnoissa kiinnitettiin huomiota siihen, että perustuslain 10 §:n 4 momenttia säädettäessä perustuslakivaliokunta on korostanut toimivaltuuksien kohdentumisen ja rajoituksen suppean tulkitsemisen lisäksi myös yleisten perusoikeuksien rajoitusedellytysten merkitystä. Kohdeluetteloa tarkasteltaessa tulee siis yllämainitun lisäksi kiinnittää huomiota erityisesti tarkkarajaisuuteen ja täsmällisyyteen. Kohteiden katsottiin olevan määritelty väljästi ja uhan vakavuusasteen puutteeseen kiinnitettiin huomiota. [215] Erityisesti 11 kohtaan esitettiin lisättäväksi rajoitus vakavasta uhasta, koska katsottiin, että nykyisessä muodossaan sen alle voi mahdollisesti lukeutua myös pienimuotoisempi toiminta, joka ei välttämättä ole luonteeltaan sellaista, johon perustuslain 10 §:n 4 momentin perusteella voidaan kohdistaa tiedustelutoimintaa. Vastaavasti 1 kohdassa mainittu ”terrorismi” nostettiin esiin laajuutensa vuoksi. Vaikka on selvää, miksi terrorismi on asetettu yhdeksi siviilitiedustelun kohteeksi, esitettiin sen täsmentämistä tarkkarajaisuuden ja täsmällisyyden näkökulmasta.[216]

Perustuslakivaliokunta otti lausunnot huomioon ja muistutti, että perustuslain 10 §:n 4 momentin uusia rajoituksia säädettäessä perustuslakivaliokunta korosti, että kansallisen turvallisuuden käsitettä tulee tulkita suppeasti ja uhan vakavuusaste asettaa korkealle. Rajoitusedellytyksestä johtuu, että tiedonhankinta on sallittua kohdistaa vain sellaiseen toimintaan, joka voi luonteensa vuoksi muodostua vakavaksi uhaksi kansalliselle turvallisuudelle. Lisäksi lailla ”tulee säätää tyhjentävästi toimivaltuuksien kohdentumisesta kansallista turvallisuutta vakavasti uhkaavasta toiminnasta.”[217] Perustuslakivaliokunta katsoi hallituksen esityksen mukaisen luettelon kohteiden olevan sellaisia, jotka voivat muodostaa vakavan uhan. Listaa ei kuitenkaan pidetty täysin ongelmattomana, sillä osassa kohteita

[215] Melander 2018, s. 6-7; Ojanen 2018, s. 10-11.
[216] Melander 2018, s. 7.
[217] PeVM 4/2018 vp, s. 8-9.

maininta uhan vakavuusasteesta puuttui[218], ja lausuntokierroksen jälkeen kohdeluettelon 5 ja 10 kohtiin lisättiin tarkennus uhan vakavuudesta.

Ruotsin lainsäädännössä signaalitiedustelun kohteet on lueteltu laissa ja niille on annettu seikkaperäisempiä määritelmiä lain esitöissä. Luettelossa nimettyjen kohteiden lisäksi tiedusteluviranomainen FRA saa kerätä elektronisia signaaleja tarkkaillakseen muutoksia kansainvälisessä signaaliympäristössä, teknisiä kehityksiä ja signaalien suojelua sekä kehittääkseen signaalitiedusteluun tarvittavaa teknologiaa. Näihin viitataan termillä kehitystoiminta (development activities), ja esitöiden mukaan niistä ei synny tiedusteluraportteja, mutta FRA voi jakaa teknisiin asioihin liittyvää tietoa muiden viranomaisten kanssa. Kehitystoimintaan ei liity yksilöiden välistä viestintää, mutta yksilön henkilöllisyyteen liittyvää tietoa saattaa joutua tiedustelun piiriin. [219] Euroopan ihmisoikeustuomioistuin katsoi tuomiossaan joidenkin luettelon kohteista olevan yleisluontoisesti määriteltyjä, mutta kiinnitti huomiota siihen, että niille annettiin tarkempi määritelmä lain esitöissä, joka on Ruotsin lainsäädännön keskeinen oikeuslähde. Tuomioistuin piti kahdeksan kohdan kohdelistausta riittävänä.[220]

Tuomiossaan Roman Zakharov v. Russia Euroopan ihmisoikeustuomioistuin käsitteli Venäjän kansallista tiedustelulainsäädäntöä, joka koostui kahdesta osasta: OSAA-lainsäädännön (Operational-Search Activities Act) nojalla viranomainen sai suorittaa viestintään kohdistuvaa tiedustelua koskien rikosprosesseja sekä muuta viestintää, ja CCrP-lainsäädäntöön (Code of Criminal Procedure) nojaten viranomaisella oli valtuudet suorittaa pelkästään rikosprosesseihin kohdistuvaa viestintätiedustelua. [221] Valittaja katsoi tuomioistuimen aiempaan oikeuskäytäntöön viitaten, että OSAA-lainsäädäntö ei täyttänyt Euroopan ihmisoikeussopimuksen ennakoitavuusvaatimusta. Valittaja ei katsonut vaatimuksen täyttyvän, koska viranomaisten oikeudellista harkintavaltaa määrätä yksityisen viestinnän tallentamista sisältävä operatiivinen koe (operational expertiment) ei ollut rajattu tiettyihin

[218] PeVL 35/2018 vp, s. 14-15.
[219] Centrum för Rättvisa v. Sweden (19.6.2018), kohdat 12-14. Signaalitiedustelun kohteita ovat "[…]1) external military threats to the country, 2) conditions for Swedish participation in international peacekeeping or humanitarian missions or threats to the safety of Swedish interests in the performance of such operations, 3) strategic circumstances concerning international terrorism or other serious cross-border crimes that may threaten essential national interests, 4) the development and proliferation of weapons of mass destruction, military equipment and other similar specified products, 5) serious external threats to society's infrastructure, 6) foreign conflicts with consequences for international security, 7) foreign intelligence operations against Swedish interests, and 8) the actions or intentions of a foreign power that are of substantial importance for Swedish foreign, security or defence policy (section 1(2))."
[220] Centrum för Rättvisa v. Sweden (19.6.2018), kohta 120.
[221] Roman Zakharov v. Russia (4.12.2015), kohta 25.

olosuhteisiin tai tilanteisiin, eikä sen toteuttamistapaa tai laajuutta ollut määritelty. Venäjän kansallisessa lainsäädännössä ei määritelty niitä henkilöitä, joihin tiedustelutoimintaa oli sallittua kohdistaa. Tiedonhankintaa ei ollut rajoitettu rikoksista epäiltyihin tai syytettyihin, vaan käytännössä jokainen henkilö, jolla oli tietoa rikoksesta, saattoi joutua tiedustelun kohteeksi. Tiedonhankintaa ei ollut myöskään rajattu vain vakaviin rikoksiin, vaan sitä voitiin harjoittaa jo esimerkiksi taskuvarkauteen liittyen.[222]

Tuomioistuin katsoi, että tiedustelutoiminnan aiheuttavien toimien luonne tuli laista esiin tarpeeksi selkeästi. Se kuitenkin huomautti, että Venäjän kansallinen laki salli tiedonhankinnan erittäin laajasta skaalasta rikoksia, eikä laissa tai oikeuskäytännössä myöskään määritelty, mitä käytännössä tarkoitetaan ilmaisuilla ”henkilö, jolla saattaa olla tietoa rikoksesta” ja ”henkilö, jolla saattaa olla rikoksen kannalta relevanttia tietoa”. Rikosten tunnistamisen ja estämisen lisäksi OSAA:n perusteella sai hankkia tietoa myös Venäjän kansallista, sotilaallista tai ekologista turvallisuutta vaarantavista toimista. Laissa ei määritelty, millaiset toimet katsotaan vaarantavan edellä mainittuja turvallisuusintressejä. Tuomioistuin katsoi, että lainsäädäntö antoi Venäjän viranomaisille lähes rajoittamattoman harkintavallan sen määrittelyyn, millaiset toimet aiheuttavat senkaltaisen uhan, että siihen voidaan kohdistaa salaista tiedustelua. Tällöin se jättää mahdollisuuden järjestelmän väärinkäytölle. Tuomioistuin kuitenkin nosti esiin, että tässä on keskeistä arvioida, toimiiko Venäjän laissa vaadittu ennakollinen tuomioistuimen suorittama valvonta viranomaisten harkintavallan rajoittajana. [223]

Toisessa tuoreessa ratkaisussaan Big Brother Watch and Others v. The United Kingdom Euroopan ihmisoikeustuomioistuin katsoi Iso-Britannian kohdentamattoman ulkomaantiedustelun kokonaisuudessaan ihmisoikeussopimuksen 8 artiklan vastaiseksi. Iso-Britannian lainsäädännön mukaan tiedustelutoimille voidaan myöntää lupa, jos se on tarpeen (1) maan kansallisen turvallisuuden vuoksi; (2) vakavan rikoksen estämiseksi tai paljastamiseksi tai (3) Iso-Britannian taloudellisen hyvinvoinnin turvaamiseksi. Lisäksi luvan sallima menettely tulee suhteuttaa haluttuun päämäärään. Arvioitaessa suhteellisuutta ja tarpeellisuutta tulee kiinnittää huomiota siihen, onko luvassa määritelty tieto kohtuullisesti hankittavissa jollakin muulla menetelmällä.[224]

---

[222] Roman Zakharov v. Russia (4.12.2015), kohta 182.
[223] Roman Zakharov v. Russia (4.12.2015), kohdat 244-246; 248-249.
[224] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 57.

Tapauksessa valittajat katsoivat, että Iso-Britannian rajojen ulkopuolella liikkuvaan tietoliikenteeseen kohdistuva tiedustelutoiminta ei täyttänyt Euroopan ihmisoikeustuomioistuimen ratkaisussa Weber and Saravia v. Germany määriteltyjä minimivaatimuksia. Esimerkiksi termejä ”kansallinen turvallisuus” ja ”Iso-Britannian taloudellinen hyvinvointi” kritisoitiin niiden laajuuden osalta. Lisäksi valittajat nostivat esiin, että termeille ulkoinen ja sisäinen viestintä ei ole annettu selkeää määritelmää, jolloin tiedustelun kohteeksi voi joutua kuka tahansa.[225]

Tuomioistuin muistutti edelleen tässä tapauksessa, että ennakoitavuusvaatimuksen merkitys on salaista tiedustelutoimintaa käsiteltäessä erilainen. Valtioilta ei vaadita, että lainsäädännössä nimetään tyhjentävästi ne yksittäiset rikkomukset, joiden perusteella tiedustelun kohteeksi voi joutua, kunhan laissa tehdään riittävän yksityiskohtaisesti selvää tällaisten rikkomusten laadusta (nature of the offences in question). Arvioidessaan termiä ”kansallinen turvallisuus” tuomioistuin viittasi aiempaan, Iso-Britannian tiedustelujärjestelmää koskevaan tuomioonsa Kennedy v. The United Kingdom. Kyseisessä ratkaisussa tuomioistuin näki, että ilmaisua ”kansallinen turvallisuus” käytetään laajasti niin kansallisessa kuin kansainvälisessä lainsäädännössä ja on yksi niistä hyväksyttävistä rajoitusperusteista, jotka mainitaan Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdassa. Kansalliseen turvallisuuteen kohdistuvat uhat ovat luonteeltaan vaihtelevia ja niitä voi olla vaikea määritellä ennakolta. Kennedy-tapauksessa tuomioistuin viittasi viestintään kohdistuvaa tiedustelua valvovan valtuutetun (Interception of Communications Commissionerin) raporttiin, jossa selvennettiin termin soveltamista käytännössä. Valtuutetun mukaan kansallisen turvallisuuteen nojautuva tiedustelu salli tiedustelun sellaisista toimista, jotka uhkasivat valtion turvallisuutta tai hyvinvointia tai joiden tarkoituksena oli poliittisin, teollisin tai väkivaltaisin keinoin horjuttaa tai kukistaa parlamentaarinen demokratia. Tuomioistuin näki täten, että termi kuvasi riittävän selkeällä tavalla rikkeitä, joiden johdosta henkilö voi joutua tiedustelun kohteeksi. Samaan lopputulokseen tuomioistuin tuli ilmaisun ”vakava rikos” kanssa. Iso-Britannian taloudellisen hyvinvoinnin turvaamiseen sovellettava tiedustelutoiminta puolestaan oli viestintään kohdistuvan tiedustelun käyttöä sääntelevän säännöstön (The Interception of Communication Code of Practice) mukaan rajoitettu sellaisiin tilanteisiin, jotka ovat merkityksellisiä kansallisen turvallisuuden kannalta. Kokonaisuudessaan tuomioistuin siis piti Iso-Britannian lainsäädäntöä 8 artiklan kanssa

[225] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 274. Minimivaatimuksista ks. tutkimuksen osio 3.2.1.

yhteensopivana siltä osin, kun kyse on niistä olosuhteista ja tilanteista, joiden perusteella tiedustelutoimintaan voidaan myöntää lupa. [226]

Tuomiossa Szabó and Vissy v. Hungary tuomioistuin arvioi Unkarin terrorismin vastaista lakia, joka sallii poliisin sisässä työskentelevälle terrorismin vastaiselle erikoisyksikölle (anti-terrorism taskforce, ”TEK”) salaisten tiedustelutoimien suorittamisen joko tietyn rikoksen selvittämisessä, johon vaaditaan tuomioistuimen lupa tai kansallisen turvallisuuden nojalla, johon vaaditaan oikeusministerin valtuutus. Kansallisen turvallisuuden nojalla harjoitettavaa, lakiin 7/E (3) perustuvaa tiedustelutoimintaa saa käyttää estämään terroristia toimia; Unkarin kansallisen turvallisuuden tueksi tai pelastamaan Unkarin kansalaisia ulkomaisilla sota-alueilla tai terroritekojen yhteydessä tapahtuneesta vangitsemisesta.[227]

Valittajat katsoivat, että heillä oli mahdollisuus joutua lain 7/E (3) nojalla epäoikeudenmukaisen ja suhteettoman tiedustelun kohteeksi etenkin oikeudellisen kontrollin puuttuessa. [228] Heidän mukaansa laista ei selkeästi käynyt ilmi ne edellytykset, joihin perustuen salaisia tiedustelumenetelmiä ja -keinoja käytettiin, joka puolestaan voi valittajien mukaan oikeudellisen kontrollin puuttuessa johtaa mielivaltaiseen päätöksentekoon. [229] Valittajat siis katsoivat, että Unkarin lainsäädäntö ei täyttänyt ennakoitavuusvaatimusta. Tuomioistuin oli kuitenkin asiasta eri mieltä ja katsoi Unkarin lainsäädännön olevan tältä osin riittävä. Tuomioistuin muistutti, että säännöksien sanamuodot eivät aina ole täsmällisesti muotoiltuja ja on väistämätöntä, että laissa käytetyt termit ovat epämääräisiä, jotta lainsäädännön on mahdollista välttää liikaa jäykkyyttä ja pysyä muuttuvien olosuhteiden mukana. Tuomioistuin katsoi, että viittaukset terroristisiin uhkiin tai pelastusoperaatioihin voidaan nähdä antavan yksilöille riittävän kuvan siitä, mihin perustuen tiedustelutoimia suoritetaan.[230]

Tuomioistuin kiinnitti kuitenkin huomiota siihen, että kansallinen lainsäädäntö mahdollisti käytännössä kenen tahansa joutumisen tiedustelun kohteeksi, eikä laissa yksilöity niitä ihmisryhmiä, joiden viestintään voidaan kohdistaa tiedonhankintaa. Euroopan ihmisoikeustuomioistuin huomioi, että vaatimus ihmisryhmien sekä edellä esitettyjen olosuhteiden selkeästä määrittelystä olivat osittain päällekkäiset: edellä kuvatut, tiedustelun

[226] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 332-335. Ks. myös Kennedy v. The United Kingdom (18.10.2010), kohta 159. Ks. myös tämä tutkimuksen osio 3.2.2.
[227] Szabó and Vissy v. Hungary (12.1.2016), kohdat 8 ja 11.
[228] Szabó and Vissy v. Hungary (12.1.2016), kohta 3.
[229] Szabó and Vissy v. Hungary (12.1.2016), kohta 47.
[230] Szabó and Vissy v. Hungary (12.1.2016), kohta 64.

oikeuttavat olosuhteet antoivat samalla jonkinlaisia viitteitä siitä, mihin ihmisryhmiin tiedonhankinta voi kohdistua. Lupahakemuksessa oli kuitenkin vaadittu yksilöitäväksi nimellä tai ihmisryhmänä (range of persons) henkilö tai henkilöt, jotka ovat tiedonhankinnan kohteena ja kaikki muu olennainen tieto heidän tunnistamiseensa liittyen. Huolestuttavaa tuomioistuimen näkökulmasta oli, että ilmaisu ”asianosaiset henkilöt […] henkilöryhminä” (“persons concerned identified ... as a range of persons”) voi pitää sisällään kenet tahansa. Tämä voi johtaa rajoittamattomaan, suureen joukkoon kohdistuvaan tiedonhankintaan. Kotimaisessa lainsäädännössä ei annettu selvennystä sille, miten tätä ilmaisua sovelletaan käytännössä. Tuomioistuin katsoi ilmaisun olevan liian laaja, sillä viranomaisilla ei ole velvollisuutta näyttää todeksi oletettua tai todellista yhteyttä henkilön tai henkilöryhmän ja terroristisen teon estämisen välillä. Luvan myöntävällä taholla ei täten ollut mahdollisuutta arvioida tiedonhankinnan ehdotonta välttämättömyyttä tavoiteltujen päämäärien ja käytettyjen menetelmien välillä, vaikka kyseinen välttämättömyyden arviointi oli laissa vaadittu: Unkarin kansallisen lain mukaan salaista tiedonhankintaa on sallittua suorittaa vain silloin, kun tietoja ei ole hankittavissa millään muulla keinolla.[231]

Euroopan ihmisoikeustuomioistuin on jo vuosien ajan linjannut salaista tiedonhankintaa koskevassa oikeuskäytännössään, että tiedustelun kohde voidaan luvassa sekä lupapäätöksessä yksilöidä esimerkiksi nimellä, osoitteella, puhelinnumerolla tai muulla aiheeseen liittyvällä, relevantilla tiedolla. [232] Suomessa tietoliikennetiedustelulaissa vaaditaan, että lupavaatimuksessa ja –päätöksessä on yksilöitävä, mikä tietoliikennetiedustelulain 3 §:ssä luetelluista kohteista on kyseessä siinä tietoliikennetiedustelutehtävässä, johon haetaan lupaa sekä siihen liittyvät tosiseikat. Lupavaatimuksessa tulee riittävän tarkasti ja konkreettisesti selventää tietoliikennetiedustelun kohteena olevan todellisen toiminnan luonne, esimerkiksi miten toiminnasta on saatu tieto, miten toiminta on tähän mennessä ilmennyt ja miten sen oletetaan kehittyvän. Suojelupoliisin vastuulla on osoittaa, että sen tiedossa olevien tosiseikkojen perusteella toiminta voidaan määrittää lain 3 §:ssä tarkoitetuksi uhaksi.[233]

Tiedustelun kohteiden sisällyttämisen lainsäädäntöön voidaan nähdä kiinnittyvän vahvasti edellä luvussa 3 kuvattuun Euroopan ihmisoikeustuomioistuimen laatuvaatimukseen lain ennakoitavuudesta: tieto siitä, mitkä asiantilat tai tekijät ovat laissa sallittuja tiedustelun kohteita, on avoimesti kaikkien saatavilla. Lisäksi lain esitöissä on määritelty 3 §:ssä

[231] Szabó and Vissy v. Hungary (12.1.2016), kohdat 66-67.
[232] Esim. Klass and Others v. Germany (6.9.1978) kohta 51; Liberty and Others v. The United Kingdom (1.7.2008) kohdat 64-65; Mustafa Sezgin Tankrikulu v. Turkey (18.7.2017) kohta 56.
[233] HE 202/2017 vp, s. 242.

käytettyjä käsitteitä laajemmin[234], jolloin niiden merkityssisältö ei jää tyhjäksi. Tällöin yksittäiselle ihmiselle on olemassa avoimesti saatavilla olevaa tietoa siitä, millaista tietoa tietoliikennetiedustelulla on sallittua hankkia ja mitä erilaisia tilanteita voi sisältyä yllä esitettyjen käsitteiden alaan.

Vaikka edellä on useasti todettu, ettei Euroopan ihmisoikeustuomioistuimen ennakoitavuusvaatimus velvoita valtiota listaamaan tiedustelun kohteita tyhjentävästi, on tuomioistuin ratkaisussaan Centrum för Rättvisa v. Sweden pitänyt tämänkaltaista listausta riittävänä ja kiinnittänyt huomiota nimenomaisesti siihen, että käsitteitä avattiin lain esitöissä. Toisaalta ratkaisussaan Roman Zakharov v. Russia Euroopan ihmisoikeustuomioistuin piti laissa annettuja kohdemääritelmiä itsessään selkeinä, mutta totesi niiden antavan tiedusteluviranomaisille hyvin laajat valtuudet. Tätä on mahdollista tuomioistuimen mukaan kompensoida tehokkaalla tuomioistuinvalvonnalla, joka kyseisessä ratkaisussa todettiin tehottomaksi. Vastaavasti ratkaisussaan Szabo and Vissy v. Hungary tuomioistuin piti Unkarin laissa säädettyä kohdelistausta riittävänä, mutta katsoi että lainsäädäntö ei yksilöinyt ihmisryhmiä, joihin tiedustelua voitiin kohdistaa. Henkilöryhmät kuitenkin vaadittiin nimettäväksi lupavaatimuksessa, mutta tiedusteluviranomaisella ei ollut velvollisuutta osoittaa yhteyttä tiedustelua aiheuttavan toiminnan sekä henkilöryhmien välillä. Tämä esti luvan myöntävän tahon arvioinnin tiedustelun välttämättömyydestä.

Lainsäädäntövaiheessa tietoliikennetiedustelulain 3 §:ään jäi edelleen sellaisia kohtia, joissa vaatimusta uhan vakavuusasteesta ei ole tarkennettu. Tällöin lienee edellä esitettyyn perustuslakivaliokunnan lausuntoon perustuen syytä olettaa, että näissä uhan itsessään katsotaan olevan sellainen, että se täyttää vaaditut edellytykset ilman erillistä mainintaa sen vakavuudesta kansallisen turvallisuuden uhkaamisessa. Esimerkiksi terrorismin voidaan tällä perusteella katsoa muodostavan sellaisen vakavan uhan kansalliselle turvallisuudelle, joka sallii tietoliikennetiedustelun käyttämisen sen selvittämiseksi. Pykälässä käytetään suhteellisen abstrakteja ilmaisuja, eikä jokaiseen tilanteeseen olekaan olemassa tyhjentävää listausta sen sisältämistä tilanteista. Kohteen osalta lupavaatimuksessa korostunee siis suojelupoliisin perustelut ja tuomioistuimen arvio siitä, täyttyykö vaaditut edellytykset yksittäisen tiedustelutehtävän kohdalla.

Suomen kansallinen lainsäädäntö muistuttaa kohdeluetteloltaan pitkälti Ruotsin lainsäädäntöä, jota Euroopan ihmisoikeustuomioistuin on pitänyt kattavana. Suomen

[234] Käsitteiden määritelmistä ks. HE 202/2017 vp, s. 172-176.

lainsäädäntö siis sallii tietoliikennetiedustelun yllä mainittuihin kohteisiin, mutta rajaa lisäksi ulos tietoliikennetiedustelulain 12 §:ssä sellaisen viestinnän, jonka lähettäjä ja vastaanottaja ovat Suomessa. Tällöin tiedustelun kohteeksi voi siis joutua sellainen henkilö tai ihmisryhmä, joiden viestintäliikenne kulkee Suomen rajojen ulkopuolella ja on oleellista liittyen edellä esitettyihin tietoliikennetiedustelun kohteisiin. Tietoliikennetiedustelun kohteiden lisäksi tulee arvioinnissa ottaa huomioon tietoliikennetiedustelulle säädetyt yleiset edellytykset.

5.4. Tietoliikennetiedustelun käytön yleiset edellytykset ja tehokkuus

Tietoliikennetiedustelun käytön yleisiksi edellytyksiksi on lain 4 §:ssä määritelty, että sen käyttäminen on välttämätöntä, jotta saadaan tärkeitä tietoja vakavasti kansallista turvallisuutta uhkaavasta, tietoliikennetiedustelun kohteena olevasta toiminnasta. Tosiseikat koskien tietoliikennetiedustelun käytön edellytyksiä ja tehokkuutta pitävät sisällään edellytykset siitä, että tietoliikennetiedustelun käyttö on välttämätöntä tärkeiden tietojen saamiseksi vakavasti kansallista turvallisuutta uhkaavasta, tiedustelun kohteena olevasta toiminnasta eikä näitä tietoja ole mahdollista saada muilla keinoin. Lupavaatimuksessa ja päätöksessä tulee siis tältä osin tuoda ilmi tietoliikennetiedusteluun liittyvä viimesijaisuus, tehokkuus ja välttämättömyys. [235]

Välttämättömyysedellytys on voimassa vain silloin, kun tietoliikennetiedustelu kohdistuu muuhun kuin valtiolliseen toimijaan tai siihen rinnastuvaan tahoon. Tietoliikennetiedustelulain 2 §:n 1 momentin 6 kohdan mukaan valtiollisella toimijalla tarkoitetaan sellaista tahoa, joka on tunnistettu vieraan valtion viranomaiseksi tai siihen rinnastuvaksi toimijaksi sekä tällaisen tahon ”[…]palveluksessa olevaa tai sen määräyksessä ja ohjauksessa toimivaa tahoa.” Tietoliikennetiedustelun kohdistuessa tällaiseen tahoon sen ei tarvitse olla välttämätöntä, vaan sen ”tulee olla tarpeen”. Tiedustelulla saatavilta tiedoilta ei myöskään vaadita oletettua tärkeyttä, mutta tietoliikennetiedustelun kohteena olevan toiminnan tulee edelleen olla vakavasti kansallista turvallisuutta uhkaavaa.

Lakia säädettäessä kiinnitettiin eri vaiheissa vahvasti huomiota välttämättömyyden sääntelemiseen. Hallituksen esityksessä tietoliikennetiedustelun käyttö edellytti 4 §:n mukaan, että tietoliikennetiedustelulla voidaan ”perustellusti olettaa saatavan tietoja” sen kohteena olevasta, vakavasti kansallista turvallisuutta uhkaavasta toiminnasta. Tällöin kaikelle tietoliikennetiedustelulle olisi ollut edellytyksenä perusteltu tuloksellisuusodotus. Jos

[235] HaVM 36/2018 vp, s. 97.

tietoliikennetiedustelun hakuehdot koskisivat myös sellaista tietoliikennettä, joka ei ole valtiollisen toimijan tai siihen rinnastuvan tahon tietoliikennettä, olisi sovellettavaksi tullut lisäksi välttämättömyysedellytys. Välttämättömyysedellytyksen mukaan tietoliikennetiedustelun käytön ”voidaan olettaa olevan välttämätöntä” edellä mainittujen tietojen saamiseksi. Välttämättömyys merkitsi tässä tietoliikennetiedustelun käytön välttämättömyyttä eli viimesijaisuutta suhteessa muihin siviilitiedustelumenetelmiin. Tämä tarkoittaa, että tietoliikennetiedustelua olisi ollut sallittua käyttää vain sellaisissa tapauksissa, joissa tietoja ei ole mahdollista hankkia muilla siviilitiedustelumenetelmillä, joista säädetään poliisilain 5 a luvussa.[236]

Lakiesityksestä perustuslakivaliokunnalle annetuissa asiantuntijalausunnoissa nostettiin esiin Euroopan ihmisoikeustuomioistuimen välttämättömyysvaatimus, ja esitettiin tietoliikennetiedustelulle asetettavan tämän mukainen edellytys ehdottomasta välttämättömyydestä. Tiedustelutoiminnassa irrottaudutaan perinteisten salaisten tiedonhankinta- ja pakkokeinojen rikosperustaisuudesta. jolloin on perustelua odottaa perus- ja ihmisoikeussuojan tason olevan korkeampi[237]. Alkuperäisen lakiesityksen ei katsottu täyttävän myöskään perustuslain 10 §:n 4 momentista johtuvaa välttämättömyysvaatimusta. Välttämättömyyttä arvioitaessa ei riitä, että se kytkettäisiin hallituksen esityksen mukaisesti pelkästään siviilitiedustelun kohteiden tyhjentävään listaukseen[238], vaan sitä tulee arvioida myös tiedustelumenetelmien käytölle säädettyjen edellytysten näkökulmasta sellaisena tekijänä, joka asettaa niille lain tasolla yleisen edellytyksen ja vaikuttaisi myös tiedustelumenetelmän käyttöön yksittäistapauksia arvioitaessa. Lisäksi siviilitiedustelun keinoilla puututaan perus- ja ihmisoikeuksiin ilman konkreettista rikosepäilyä, jolloin yleisiä edellytyksiä tuli tarkentaa siten, että välttämättömyysvaatimus tulee laista selkeämmin ilmi esimerkiksi lisäämällä vaatimus saatavien tietojen tärkeydestä ja välttämättömyydestä lakitekstiin.[239]

Perustuslakivaliokunta katsoi omassa lausunnossaan välttämättömyysedellytyksen heijastavan tiedustelutoimivaltuuksille asetettuja vaatimuksia niiden käytön oikeasuhtaisuudesta sekä tiedustelutoiminnan irtautumista rikosperusteisuudesta. Valiokunta esitti tietoliikennetiedustelun käytön edellytyksiin lisättävän myös maininnan menetelmällä oletettavasti saatavan tiedon tärkeydestä. Tällä voidaan edistää tietoliikennetiedustelun käytön

[236] HE 202/2017 vp, s. 236-237.
[237] Melander 2018, s. 5.
[238] HE 2017 vp, s. 273
[239] Melander 2018 vp, s. 9.

asianmukaisuutta ja kohdentumista, joka on tarpeellista tiedustelutoiminnan erityisluonteen sekä sääntelyn laajuuden vuoksi.[240]

Ensimmäisellä lausuntokierroksella perustuslakivaliokunta kiinnitti huomiota hallituksen lausumaan siitä, että ”perusteltu tuloksellisuusodotus” toimisi kaiken tietoliikennetiedustelun edellytyksenä. Perustuslakivaliokunta korosti luottamuksellisen viestin salaisuuden suojalle määriteltyä välttämättömyysedellytystä, jonka mukaan suojaan saa puuttua vain, jos tiedonhankintaa ei ole mahdollista suorittaa vähemmin puuttuvin keinoin. Tästä johtuen perustuslakivaliokunta katsoi, että välttämättömyys tulee asettaa tiedustelutoiminnan yleiseksi edellytykseksi niin poliisilain 5 a luvun 4 §:ään kuin tietoliikennetiedustelulain 4 §:ään, jotta lakiehdotukset voidaan käsitellä tavallisessa lain säätämisjärjestyksessä. [241] Valiokunta kehotti lisäksi lisäämään edellytyksen tietoliikennetiedustelun viimesijaisuudesta myös itse säännökseen. Tätä ei kuitenkaan pidetty säätämisjärjestykselle olennaisena muutoksena. [242]

Hallintovaliokunta huomioi mietinnössään perustuslakivaliokunnan ehdotukset lisäämällä niin poliisilain 5 a luvun 4 §:ään kuin tietoliikennetiedustelulain 4 §:ään vaatimuksen siitä, että tiedustelumenetelmän käytön yleisenä edellytyksenä on välttämättömyys tärkeiden tietojen saamiseksi kansallista turvallisuutta vakavasti uhkaavasta, tiedustelun kohteena olevasta toiminnasta. Lisäksi hallintovaliokunta täsmensi tietoliikennetiedustelun käytön viimesijaisuutta suhteessa muihin siviilitiedustelumenetelmiin lisäämällä tietoliikennetiedustelulain 4 §:ään vaatimuksen, että tietoliikennetiedustelua saa käyttää vain silloin, kun tietoja ei voida hankkia muilla tiedustelumenetelmillä.[243] Viimesijaisuusedellytys täyttyy myös, jos muiden siviilitiedustelumenetelmien käyttö vaatisi huomattavasti enemmän voimavaroja tai viivästyttäisi tiedonhankintaa ylettömästi. Arvioitaessa tietoliikennetiedustelun käytön välttämättömyyttä viimesijaisuuden kautta ei tiedusteluviranomaisen kuitenkaan edellytetä konkreettisesti käyttävän tai yrittävän käyttää muita tiedustelumenetelmiä, vaan välttämättömyyden tarkastelu voi perustua kokonaisarviointiin esimerkiksi muiden siviilitiedustelumenetelmien tuloksettomuudesta.[244]

Välttämättömyys on yksi Euroopan ihmisoikeusoikeustuomioistuimen vaatimuksista yksityiselämän suojaa rajoitettaessa. Tapauksessa Roman Zakharov v. Russia Euroopan

[240] PeVL 35/2018 vp, s. 17. Ks. myös Melander 2018, s. 9.
[241] PeVL 35/2018 vp, s. 17. Ks. lisäksi PeVM 4/2018, s. 8-9.
[242] PeVL 35/2018 vp, s. 20.
[243] HaVM 30/2018 vp, s. 50-51; 95-96.
[244] HE 202/2017 vp, s. 237. Tässä viitataan välttämättömyyden arviointia koskien pakkokeinolain uudistamista koskevaan hallituksen esitykseen HE 222/2010 vp, s. 316.

ihmisoikeustuomioistuin muistutti aiempaan oikeuskäytäntöönsä viitaten, että kansallisella lainsäädännöllä tulee varmistaa, että salaisia tiedonhankintakeinoja sovelletaan vain silloin kun se on välttämätöntä demokraattisessa yhteiskunnassa, erityisesti tarjoamalla riittävät ja tehokkaat oikeussuojakeinot sekä takuut väärinkäyttöä vastaan.[245] Tuomioistuin katsoi, että tiedustelutoiminnan valtuuttavan tahon tulee pystyä varmistamaan, että tiedustelutoiminta täyttää välttämättömyysvaatimuksen. Välttämättömyysvaatimuksen arviointiin kuuluu myös suhteellisuusvaatimuksen arviointi esimerkiksi tarkastelemalla, voidaanko halutut päämäärät saavuttaa vähemmin puuttuvin keinoin.[246] Venäjän tiedustelujärjestelmässä tuomioistuin katsoi tuomioistuinkontrollin epäonnistuneeksi, sillä tuomioistuimet eivät testanneet välttämättömyys- ja suhteellisuusedellytyksen täyttymistä.[247]

Tapauksissa Centrum för Rättvisa v. Sweden sekä Big Brother Watch and Others tuomioistuin on lainsäädännön laatuvaatimuksia, myös välttämättömyysvaatimusta, arvioidessaan viitannut Roman Zakharov v. Russia tapauksessa linjaamiinsa yleisiin periaatteisiin[248]. Centrum för Rättvisa v. Sweden tapauksessa tuomioistuin keskittyi arvioimaan, onko Ruotsin kansallinen lainsäädäntö saatavilla ja sisältääkö se sellaiset riittävät ja tehokkaat suojakeinot ja takuut, että sitä voidaan pitää ennakoitavana ja välttämättömänä demokraattisessa yhteiskunnassa ihmisoikeussopimuksen 8 artiklan 2 kohdan tarkoittamalla tavalla. Tuomioistuin katsoi, että Ruotsin signaalitiedustelua koskevassa lainsäädännössä tuomioistuimen ennakollinen lupajärjestelmä tarjosi tärkeitä suojakeinoja järjestelmän väärinkäyttöä vastaan.[249]

Iso-Britannian lainsäädännön mukaan vastaava ministeri sai myöntää luvan tiedusteluun vain, jos hän katsoi sen olevan välttämätöntä kansallisen turvallisuuden vuoksi, estämään tai paljastamaan vakava rikos tai valtion taloudellisen hyvinvoinnin suojaamiseksi. Lisäksi käytetyn menetelmän ja päämäärän tulee olla oikeasuhtaiset. Lain mukaan välttämättömyyttä ja oikeasuhtaisuutta arvioitaessa tulee kiinnittää huomiota, voidaanko haluttu tieto saavuttaa toisella keinolla.[250] Tuomioistuin kuitenkin katsoi Big Brother Watch and Others v. The United Kingdom tuomiossaan, että valvontajärjestelmä ja laissa myönnetyt oikeussuojakeinot

[245] Roman Zakharov v. Russia (4.12.2015) kohta 236. Ks. myös esim. Kennedy v. The United Kingdom (18.5.2010), kohta 155.
[246] Roman Zakharov v. Russia (4.12.2015), kohta 260.
[247] Roman Zakharov v. Russia (4.12.2015), kohta 263.
[248] Roman Zakharov v. Russia (4.12.2015), kohdat 228-236; Centrum för Rättvisa v. Sweden (19.6.2018), kohdat 99-107; Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 303-310.
[249] Centrum för Rättvisa v. Sweden (19.6.2018), kohta 141.
[250] Big Brother Watch and Others v. The United Kingdom (13.9.2018) kohta 331.

eivät pystyneet täyttämään lain laatuvaatimuksia tai rajaamaan tiedustelutoimintaa siihen mikä on välttämätöntä demokraattisessa yhteiskunnassa. Lopputulokseen vaikutti esimerkiksi jo edelläkin mainittu kaapatun tietoliikenteen suodattamiseen käytettyihin valitsimiin kohdistuvan itsenäisen valvonnan puute. [251]

Unkarin kansallisessa lainsäädännössä salaista tiedonhankintaa saa käyttää vain, jos tehtävän suorittamiseen tarvittavia tietoja ei ole saatavilla muilla keinoin. [252] Tapauksessa Szabó and Vissy v. Hungary Unkarin kansallisessa lainsäädännössä vaadittiin, että ministerille tehdyssä lupavaatimuksessa tiedusteluviranomaisen tulee todistaa tiedustelutoiminnan välttämättömyys. Euroopan ihmisoikeustuomioistuin ei kuitenkaan ollut vakuuttunut siitä, että riittävä analyysi haluttujen päämäärien ja käytettyjen keinojen suhteesta on mahdollista tai taattua suoritettaessa kansalliseen turvallisuuteen liittyviä tehtäviä. Pelkästään vaatimus siitä, että viranomaisen tulee perustella lupahakemus ja tiedustelun välttämättömyys ei riitä täyttämään vaatimusta ehdottomasta välttämättömyydestä. Unkarin lainsäädännössä ei ollut sellaisia oikeussuojakeinoja, joiden perusteella tiedusteluviranomaisen eli TEK:n tulisi antaa salaisen tiedustelumenetelmän käyttöä tukevaa materiaalia tai esittää riittäviä tosiasioita, jotka puolestaan mahdollistaisivat välttämättömyyden arvioinnin kyseisen toimen kohdalla.[253]

Tuomioistuin on välttämättömyysvaatimusta koskien linjannut tuomiossaan Klass and Others v. Germany jo vuonna 1978, että salaista tiedonhankintaa koskevissa tilanteissa välttämättömyyttä tulee tulkita ehdottomana välttämättömyytenä. Tapauksessa tuomioistuin katsoi, että ihmisoikeussopimuksessa turvatun oikeuden rajoittamisen sallivia perusteita tulee tulkita kapeasti – kansalaisiin kohdistuvat, salaiset tiedonhankintakeinot ovat sallittuja Euroopan ihmisoikeussopimuksen nojalla vain silloin, kun se on ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi. Tuomioistuin on katsonut, että kun kyseessä on tämänkaltainen erityisluonteinen puuttuminen sekä tiedustelumenetelmien mahdollisuus puuttua kansalaisten yksityisyyteen huipputeknologian avulla, tulee välttämättömyysvaatimusta tulkita ehdottomana välttämättömyytenä. Ehdotonta välttämättömyyttä tulee tuomioistuimen mukaan tulkita tässä yhteydessä kahdenlaisesti: Ensinnäkin, tiedustelumenetelmä voi olla ihmisoikeussopimuksen mukainen vain, jos se on yleisellä tasolla ehdottoman välttämätöntä demokraattisten instituutioiden suojaamiseksi. Lisäksi tiedustelumenetelmän tulee olla ehdottoman välttämätöntä tärkeän tiedon saamiseksi

[251] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 387-388.
[252] Szabó and Vissy v. Hungary (12.1.2016), kohta 17
[253] Szabó and Vissy v. Hungary (12.1.2016), kohta 71.

yksittäisessä tiedustelutehtävässä. Jos nämä kaksi ehtoa eivät täyty, minkä tahansa tiedustelumenetelmän käyttö on tuomioistuimen näkökulmasta altis viranomaisten väärinkäytölle.[254]

Euroopan ihmisoikeustuomioistuimen vaatimus ehdottomasta välttämättömyydestä pyritään kansallisessa lainsäädännössä täyttämään yhtäältä asettamalla välttämättömyys kaiken siviilitiedustelun yleiseksi edellytykseksi ja toisaalta korostamalla tietoliikennetiedustelun viimesijaisuutta suhteessa muihin siviilitiedustelumenetelmiin. Tuomioistuinkontrollin olemassaolo on nähty oikeussuojaa vahvistavana tekijäksi, mutta sen tulee olla todellista, ja ollakseen todellista tuomioistuimella tulee olla hallussaan riittävät tiedot suorittaakseen arviointia lupaan liittyen. Koska pelkästään tuomioistuinkontrollin olemassaolo ja lakiin kirjattu vaatimus välttämättömyydestä eivät riitä täyttämään vaatimusta, tulee tuomioistuimella olla käytössään tarvittava määrä tietoa todellisen arvioinnin toteuttamiseksi, jonka esittämisen vastuu on suojelupoliisilla. Vastaavasti tuomioistuimella on vastuu todella testata välttämättömyys- ja suhteellisuusvaatimusten täyttymistä.

Ehdottoman välttämättömyyden täyttymisen arviointi jäänee viime kädessä tuomioistuimen varaan. Erityisesti se, voidaanko tiedot hankkia vähemmän puuttuvalla menetelmällä, noussee keskeiseksi kysymykseksi lupamenettelyssä, sillä juuri se on ehdottoman välttämättömyyden kannalta ratkaiseva tekijä. Välttämättömyysperiaatteeseen sisältyvän suhteellisuusvaatimuksen arviointi vaatii päämäärän ja käytettävän keinon sopusuhtaisuutta. Tiedustelun kohteiden sekä yleisten edellytysten ollessa samat tietoliikennetiedustelussa ja muissa siviilitiedustelumenetelmissä, jää erottavaksi tekijäksi ainoastaan se, onko yksittäisessä tiedustelutehtävässä tavoiteltava tieto sellaista, joka voidaan saada ainoastaan käyttämällä tietoliikennetiedustelua.

Viittaan ”vakava uhka kansalliselle turvallisuudelle” osalta tässä tutkimuksen osioon 3.2.2., jossa käsiteltiin kyseistä vaatimusta luottamuksellisen viestin salaisuuden suojan rajoittajana. Vakavan uhan kansalliselle turvallisuudelle aiheuttaa Suomen lainsäädännössä siis sellainen toiminta, joka on ulkoista, ja uhkaa välittömästi tai välillisesti valtion oikeudenkäyttöpiiriin kuuluvien ihmisten kollektiivista turvallisuutta. Toiminnalla tulee olla yhteys Suomeen ja uhan tulee kohdistua nimenomaisesti Suomen kansalliseen turvallisuuteen. Edellisessä osiossa

[254] Szabó and Vissy v. Hungary (12.1.2016), kohdat 72-73. Ks. myös Klass and Others v. Germany (6.9.1978), kohta 42.

käsiteltiin tietoliikennetiedustelun kohteita, ja lupavaatimusta sekä -päätöstä laatiessa kohteiden lisäksi tulee pitää mielessä tietoliikennetiedustelulle määritellyt yleiset edellytykset.

Euroopan ihmisoikeustuomioistuin ei ole oikeuskäytännössään määritellyt sisällöllisiä vaatimuksia kansallisen turvallisuuden käsitteelle sen laajuuden vuoksi. Valtio ei kuitenkaan voi pelkästään sen nojalla puuttua yksilön 8 artiklassa turvattuihin oikeuksiin, vaan Euroopan ihmisoikeustuomioistuin vaatii kansallista turvallisuuttava uhkaavat tekijät jollakin tarkkuudella yksilöitäväksi lainsäädäntöön – esimerkkinä Suomessa tietoliikennetiedustelulain 3 §, jossa luetellaan tietoliikennetiedustelun kohteet. Tällöin vaatimus hyväksyttävästä päämäärästä voidaan katsoa täytettävän yhtäältä määrittelemällä vakava uhka kansalliselle turvallisuudelle kaiken siviilitiedustelun yleiseksi edellytykseksi ja toisaalta nimeämällä tiedustelun kohteet erikseen laissa, joka omalta osaltaan kytkeytyy myös ennakoitavuusvaatimukseen.

Kuten edellisessä osiossa todettiin, kaikkiin kohdeluettelon kohteisiin ei ole erikseen lisätty vaatimusta uhan vakavuudesta, esimerkiksi kohdeluettelon kohdat 6 (”suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta”) ja 9 (”kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta”) on itsessään nähty sellaiseksi uhaksi, ettei niihin ole mielekästä lisätä mainintaa uhan vakavuudesta. Yleisenä edellytyksenä vakava uhka kansalliselle turvallisuudelle rajaa kohdeluettelon käyttöä. [255] Lupavaatimusta ja -päätöstä laatiessa on siis varmistuttava siitä, että tietoliikennetiedustelun kohteena oleva toiminta täyttää vaaditut kriteerit ja on tosiasiassa sellainen vakava uhka, jolla on kytkentä Suomeen ja vakava uhka aiheutuu nimenomaisesti Suomen kansalliselle turvallisuudelle. Esimerkiksi vaikka edellä 6 ja 9 mainitut kohteet täyttäisivätkin vakavan uhan tunnusmerkit ilman sen kirjaamista erikseen lakiin, johtuu perustuslain 10 §:stä vaatimus siitä, että kyseisellä uhalla on oltava kytkös Suomeen.

5.5. Hakuehdot ja hakuehtojen luokka

Tietoliikennetiedustelun käytössä sekä lupamenettelyssä keskeisiä käsitteitä ovat hakuehto ja hakuehtojen luokka, sillä tietoliikennetiedustelun kohdistaminen, jolla estetään yleinen ja kohdentamaton valvonta, perustuu hakuehtojen käyttöön automatisoidussa erottelussa. Hakuehdoille ei ole laissa tai sen esitöissä määritelty yksittäisiä sisältövaatimuksia, vaan hyväksyttävyyden perusteena pidetään laissa säädettyä vaatimusta siitä, että hakuehtona

[255] HaVM 30/2018 vp, s. 48-49.

käytetään sellaista tietoa, johon perustuen viestintäverkon osasta valitaan niin täsmällisesti ja rajatusti kuin mahdollista se tietoliikenne, johon tietoliikennetiedustelua kohdistetaan. Tällöin luottamuksellisen viestin salaisuuden suojaan puuttuminen rajoittuu vain siihen, mikä on tiedustelun tarkoitukseen nähden välttämätöntä. Hakuehtojen luokalla tarkoitetaan tietoliikennetiedustelulain 2 §:n 5 kohdan mukaan toisiinsa liittyviä, samaa asiakokonaisuutta kuvaavia hakuehtoja. Hakuehtoja määriteltäessä on kiinnitettävä huomiota myös lain 1 §:ssä säädettyyn syrjintäkieltoon sekä yleisiin poliisioikeudellisiin periaatteisiin, jotka rajoittavat suojelupoliisin harkintavaltaa.[256]

Hallituksen esityksessä hakuehdoille ja niiden luokille ei ollut lakiin kirjattuna minkäänlaista sisällöllistä määritelmää. Tähän puutteeseen kiinnitettiin lakiehdotuksesta perustuslakivaliokunnalle annetuissa asiantuntijalausunnoissa huomiota, ja esitettiin, että lain tasolle tulisi kirjata sisällöllinen määritelmä hakuehdoille ja niiden luokille, koska kyseiset käsitteet ovat keskeisessä asemassa tietoliikennetiedustelun kohdistamisessa[257]. Hakuehdoista annetun sääntelyn ei myöskään katsottu varmistavan sitä, että luottamuksellisen viestin salaisuuden suojaan puuttuminen toteutetaan mahdollisimman kohdennetusti ja rajatusti, kuten välttämättömyysvaatimuksesta tulisi seurata[258]. Perustuslakivaliokunta lausui omassa lausunnossaan vastaavasti, että sääntelyn tarkkarajaisuuteen ja täsmällisyyteen sekä hyväksyttävään kohdentumiseen perustuen laissa on säädettävä hyväksyttävistä hakuehdon ja hakuehtojen luokan perusteista[259].

Hallintovaliokunnan mukaan hakuehtojen hyväksyttävyys perustuu siihen, että hakuehdon on oltava sellainen tieto, jonka avulla voidaan mahdollisimman rajatusti ja täsmällisesti valita tietovirrasta se tietoliikenne, mikä on tietoliikennetiedustelun kohteena. Hakuehtojen luokan hyväksyttävyyden vaatimuksena on yksittäisen hakuehdon kohdalla se, mitä hakuehdoista edellä kerrottiin sekä lisäksi se, että samaan luokkaan kuuluvat hakuehdot liittyvät riittävästi toisiinsa ja kuvaavat samaa asiakokonaisuutta. Nämä määritelmät esitettiin lisättäväksi ensimmäisen lausuntokierroksen jälkeen lain 2 §:n uusiksi 4 ja 5 kohdiksi.[260]

Hallintovaliokunnan mietinnön jälkeen julkisuudessa käytiin keskustelua siitä, onko hallintovaliokunta ottanut perustuslakivaliokunnan antamaa lausuntoa riittävästi huomioon.

[256] HaVM 36/2018 vp, s. 97. Yleiset poliisioikeudelliset periaatteet on määritelty poliisilain 1 luvussa, ja niitä ovat mm. perus- ja ihmisoikeuksien kunnioittaminen, suhteellisuusperiaate, vähemmän haitan periaate sekä tarkoitussidonnaisuuden periaate.
[257] Melander 2018, s. 13.
[258] Lavapuro 2018, s. 7.
[259] PeVL 35/2018 vp, s. 20-21.
[260] HaVM 30/2018 vp, s. 94.

Silloinen eduskunnan puhemies Paula Risikko päätti vetää tiedustelulait eduskunnan käsittelystä ja palauttaa ne substanssivaliokuntiin, josta ne lähetettiin uudestaan perustuslakivaliokuntaan lausunnolle[261]. Perustuslakivaliokunta kuuli uudestaan vielä kolmea perustuslakiasiantuntijaa.

On huomioitava, että hakuehtojen määritelmä ei ollut perustuslakivaliokunnan lausunnossa asia, joka olisi estänyt lain säätämisen tavallisessa säätämisjärjestyksessä. Yleisen ja kohdentamattoman tietoliikenteen seurannan nimenomainen kielto oli kuitenkin yksi perustuslakivaliokunnan vaatimista muutoksista ja hakuehdot ovat tässä keskeinen tekijä, ja muun muassa tästä syystä myös hakuehtojen määritelmää käsiteltiin toisen lausuntokierroksen asiantuntijalausunnoissa[262]. Hallintovaliokunnan ehdottamaa määritelmää hakuehdolle ja hakuehtojen luokille pidettiin asiantuntijalausunnoissa järjestäen riittämättöminä, eikä sen katsottu täyttävän perustuslakivaliokunnan lausunnossa ehdotettua muotoa. Ehdotettujen määritelmien ei esimerkiksi katsottu kuvaavan sisällöllisiä kriteerejä, joiden mukaan hakuehdot tai niiden luokat tulisi määriteltäviksi[263]. Hakuehdon ja hakuehtojen luokan määritelmän tuli lausunnoissa esitetyn mukaan olla sellainen, joka rajaa tietoliikennetiedustelun toteuttamisen säännöstasolla ehdottoman välttämättömään[264].

Perustuslakivaliokunta katsoi omassa lausunnossaan asiantuntijalausuntojen mukaisesti, että hallintovaliokunnan ehdottama muotoilu koskien hakuehtoja ja niiden luokkia jättää avoimeksi sen, millä sisällöllisillä perusteilla hakuehtoja voidaan määritellä. Perustuslakivaliokunnan mukaan sääntelyä tuli täydentää, mutta määritelmien puutteen ei edelleenkään nähty olevan sellainen tekijä, joka estäisi siviilitiedustelulain säätämisen tavallisessa lainsäätämisjärjestyksessä[265]. Hallintovaliokunta lisäsi tietoliikennetiedustelulain 2 §:n 1 momentin 4 kohtaan vaatimuksen siitä, että luottamuksellisen viestin suojaan puuttumisen tulee rajautua tiedustelun tarkoituksen kannalta välttämättömään, ja säännös sai lopullisen muotonsa.

Hakuehto on siis tieto, jonka perusteella viestiliikenteestä suodatetaan tiedustelun kohteena oleva liikenne. Jos tietoliikennetiedustelun kohteena on muu kuin valtiollinen toimija tai siihen rinnastuva taho, hakuehto ei saa olla viestin sisältöä kuvaava. Tällöin se voi liittyä

[261] YLEn uutinen 14.2.2019: ”Tiedustelulait lähetetään takaisin valiokuntien käsittelyyn – Risikko: ”Emme jätä mitään kiviä kääntämättä”, katsottu 23.2.2020.
[262] Ks. esim. Lavapuro 2019, s. 5; Ojanen 2019, s. 5; Scheinin 2019, s. 3.
[263] Ojanen 2019, s. 6; Scheinin 2019, s. 4; Jääskeläinen 2019, s. 6.
[264] Ojanen 2019, s. 6; Lavapuro 2019, s. 6; Pöysti 2019, s. 7.
[265] PeVL 75/2018 vp, s. 3.

viestinnän ja tietoliikenteen muihin tietoihin, kuten tunnistamistietoihin. Koska kaikki viestintä ei kuulu luottamuksellisen viestin salaisuuden suojan piiriin, on lain 5 §:n 2 momentissa säädetty niistä tilanteista, jolloin viestin sisältöä kuvaavan hakuehdon käyttö on sallittua. Hakuehto saa kuvata viestin sisältöä, jos sitä käytetään vain vieraan valtion tai siihen rinnastuvan tahon tietoliikenteeseen tai se kuvaa haitallisen tietokoneohjelman tai –käskyn sisältöä.[266]

Hakuehtojen luokalla ei tarkoiteta yksittäistä teknistä tietoa, vaan termillä tarkoitetaan ”tarkkarajaista kuvausta tiedustelukysymyksen kannalta relevanteista hakuehdoista.” Jos samaan tarkkarajaisesti määriteltävään kokonaisuuteen sisältyy useita keskenään samankaltaisia hakuehtoja, joista vain osa on tiedossa tietoliikennetiedustelun alkaessa, voidaan tuomioistuimelta hakea lupa hakuehtojen luokan käyttöön. Tällöin tuomioistuimen lupapäätös koskee useista hakuehdoista koostuvan joukon sanallista kuvausta, mutta aiemmin haettu lupa kattaa myös tiedustelutoiminnasta saadun uuden tiedon perusteella muodostettavat uudet, yksittäiset hakuehdot.[267]

Koska hakuehtojen ja tietoliikennetiedustelun kohteena olevan, kansallista turvallisuutta vakavasti uhkaavan toiminnan välinen yhteys ei välttämättä ole ilmiselvä, tulee suojelupoliisin lupahakemuksessa perustella valitut hakuehdot tai niiden luokat ja tuoda esiin liittymä näiden välillä. Suojelupoliisin tulee myös tuoda esiin se, miksi ja minkälaista tietoa kyseisillä hakuehdoilla voidaan olettaa saatavan kyseessä olevasta toiminnasta. Jos tietoliikennetiedustelua koskevassa luvassa sallitaan tietyn hakuehtojen luokan käyttö, tarkoittaa tämä, että suojelupoliisi saa sallitun luokan rajoissa määritellä käytettävät hakuehdot itse. Tällöin valvontatoimessa tulee kiinnittää erityistä huomiota siihen, että hakuehtojen määrittely tapahtuu tuomioistuimen hyväksymän hakuehtojen luokan mukaisesti.[268]

Kieltämällä viestin sisällön käyttäminen hakuehtona pyritään suojaamaan tietoliikennetiedustelussa sivullisia henkilöitä. Verrattuna muihin siviilitiedustelumenetelmiin, tietoliikennetiedustelussa sivullisen henkilön rooli korostuu. Tietoliikennetiedustelussa sivullisella henkilöllä on suurempi riski joutua sattumanvaraisesti tiedustelun kohteeksi, sillä tietoliikennetiedustelun kohteena ei ole yksilöity telepäätelaite kuten esimerkiksi telekuuntelussa ja –valvonnassa. Jos henkilön viesti reitittyy hakuehtojen käytön piiriin, voi

[266] HE 202/2017 vp, s. 124.
[267] HE 202/2017 vp, s. 243.
[268] HE 202/2017 vp, s. 244.

se sattumanvaraisesti tulla tietoliikennetiedustelu kohteeksi.[269] Viestin sisällön on nähty muodostavan luottamuksellisen viestin ydinalue, ja sen käyttäminen hakuehtona puuttuu syvällisemmin sivullisten luottamukselliseen viestintään, koska sisällön ja hakuehdon vastaavuus on tarkastettava avaamalla tietoteknisesti kaiken suodatuksen piirissä oleva viestintä. Tietoliikennetiedustelussa pyritään turvaamaan sivullisten henkilöiden viestintäsalaisuuden ydinalue, jolloin hakuehtona ei saa käyttää luottamuksellinen viestin sisältöä.[270]

Euroopan ihmisoikeustuomioistuin on tuomiossaan Centrum för Rättvisa v. Sweden pitänyt hakuehtojen ja niiden luokkien erittelyn vaatimusta erityisenä valvontakeinona. Ruotsin signaalitiedustelua koskevassa lainsäädännössä tiedustelu sai kohdistua vain sellaisiin signaaleihin, jotka oli tunnistettu hakuehtojen käytön kautta. Hakuehdot tuli muotoilla siten, että yksilön henkilökohtaiseen loukkaamattomuuteen (personal integrity) puututtiin mahdollisimman vähän. Suoraan johonkin yksittäiseen luonnolliseen henkilöön kohdistuvia hakuehtoja voitiin käyttää vain siinä tapauksessa, että se oli erityisen tärkeää tiedustelutoiminnan kannalta. [271] Yksittäiseen, luonnolliseen henkilöön käytetyt hakuehdot tuli raportoida ulkomaantiedustelusta vastaavalle taholle (the Foreign Intelligence Inspectorate)[272]. Tuomioistuin on katsonut - tiedustelutoiminnan salaisen luonteen huomioon ottaen – valvontaa suorittavan tuomioistuimen (the Foreign Intelligence Court) valvonnan laaja-alaiseksi koska sekä kantoaallot (signal carriers) että hakuehdot ja niiden luokat oli alistettava tuomioistuimen ennakolliselle valvonnalle lupaa haettaessa.[273]

Tapauksessa Big Brother Watch and Others v. The United Kingdom Iso-Britannian tiedustelutoiminnassa käytettyjä hakuehtoja ei alistettu itsenäiselle valvontaelimelle, mikä oli ratkaisevassa asemassa tuomioistuimen arvioidessa tiedustelun sallivaa lupajärjestelmää. Tuomioistuimen näkökulmasta järjestelmä ei täyttänyt välttämättömyysvaatimusta, sillä kaapattavan tietoliikenteen valintaan ja seulontaan ei kohdistunut valvontaa eikä viestintätietojen valintaan kohdistunut oikeussuojakeinoja. [274] Iso-Britannian suorittama tiedustelutoiminta tapahtui neljässä eri vaiheessa: 1) tiedusteluviranomaiset kaappasivat (intercept) pienen määrän sellaisia internetkantoaaltoja (internet bearers), joilla oli

[269] HaVM 36/2018 vp, s. 35.
[270] HE 202/2017 vp, s. 124.
[271] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 16.
[272] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 36
[273] Centrum för Rättvisa v. Sweden (19.7.2018), kohta 139.
[274] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 387-388.

todennäköisimmin arvoa tiedustelun kannalta; 2) kaapatusta tietoliikenteestä suodatettiin lähes reaaliaikaisesti pois suurin osa (irrelevantti tieto); 3) jäljelle jäävään tietoliikenteeseen kohdistettiin tietokoneen avulla yksinkertaisia sekä monimutkaisia hakuehtoja, jotka suodattavat pois ei-tärkeän materiaalin; 4) jäljelle jäävä materiaali analysoitiin.[275] Euroopan ihmisoikeustuomioistuin peräänkuulutti tiukempia oikeussuojakeinoja kohdille 3 ja 4, sillä niissä yksityisyyden suojaan puuttuminen oli suurempaa verrattuna kahteen ensimmäiseen vaiheeseen, joita ei myöskään niin ikään alistettu itsenäiselle valvonnalle. Edelleenkään tuomioistuin ei katsonut, että hakuehtoja tulisi tuoda julki tai edes yksilöidä luvassa tai lupapäätöksessä, mutta katsoi, että tietoliikenteen suodattamiseen käytetyt hakuehdot ja valitsimet (search criteria and selectors) tulisi alistaa itsenäiselle valvontaelimelle.[276]

Iso-Britannian järjestelmässä valitsimien ja automaattisten hakujen avulla luotiin hakemisto (index), ja vain siihen sisältyvää materiaalia oli sallittua analysoida. Hakemiston materiaalia sai analysoida vain, jos se oli välttämätöntä ministerin antaman todistuksen (certificate) mukaan ja jos kohteena oleva henkilö ei tuohon aikaan oleskellut Iso-Britannian alueella. Tuomioistuin nosti esiin parlamentin tiedustelu- ja turvallisuuskomitean (Intelligence and Security Committee of Parliament) raportin huomion siitä, että ministerin luvan ohella antamassa todistuksessa se tietoliikenne, jota saa tutkia, erittäin laajoin käsittein. Tuomioistuin piti kuitenkin tärkeänä oikeussuojakeinona sitä, että laajamittaista tiedustelua ei saa kohdistaa Brittein saarilla oleskeleviin henkilöihin. Hakemiston kokosivat kokeneet ja hyvin koulutetut analyytikot, mutta sitä ei kuitenkaan alistettu edes kokeneemman analyytikon valvonnalle, jolloin sen kokoaminen oli täysin analyytikkojen ammatillisen harkintakyvyn varassa. [277]

Tuomioistuin kiinnitti huomiota siihen, että hakemisto, josta analyytikot valitsivat aineistonsa, oli luotu niiden valitsimien ja hakuehtojen kautta, joita ei alistettu itsenäiselle ennakkovalvonnalle. Tämä tarkoittaa, että käytännössä ainoa itsenäinen valvonta, joka kaapatun tietoliikenteen suodattamiseen ja valitsemiseen kohdistui, oli tietoliikennetiedustelukomissaarin (Interception of Communications Commissioner) suorittamaa jälkikäteistä valvontaa. Tiedustelujärjestelmässä, jossa tiedustelutoiminnan sallivalla luvalla ei juurikaan rajoiteta tiedusteluviranomaisen harkintavaltaa, tutkintavaiheessa sovellettavaan suodattamiseen ja valitsemiseen tulee Euroopan

[275] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohta 329.
[276] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 338-340.
[277] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 341-345. Ks. raportin kohta 156.

ihmisoikeustuomioistuimen mukaan kohdistua vahvempia oikeussuojakeinoja. Vaikka tuomioistuin ei nähnyt todisteita tiedusteluviranomaisten toimivaltuuksien väärinkäytöstä, se ei ollut vakuuttunut internetkantoaaltojen kaappaamista ja kaapatun materiaalin valitsemista koskevien oikeussuojakeinojen tehokkuudesta väärinkäytön estämiseksi. Suurin huolenaihe tuomioistuimelle oli kuitenkin kaapatun tietoliikenteen suodattamiseen käytettyihin valitsimiin ja hakuehtoihin kohdistuvan vahvan, itsenäisen valvonnan puuttuminen. [278]

Vaikka Euroopan ihmisoikeustuomioistuin katsoo hakuehtojen olevan keskeinen osa perus- ja ihmisoikeuksien toteutumisen valvontaa, tuomioistuin ei ole oikeuskäytännössään vaatinut hakuehtojen määritelmiä lakiin kirjattavaksi eikä välttämättä edes sisällytettäväksi tiedustelutoiminnan sallivassa luvassa[279]. Keskeiseksi näyttää edellä esitetyn myötä nousevan kuitenkin se, että hakuehdot tulee alistaa itsenäiselle valvonnalle. Suomessa hakuehtoja voidaan ennakollisesti valvoa niin suojelupoliisissa sisäisesti kuin tuomioistuimen ja tiedusteluvalvontavaltuutetun toimesta, jotka molemmat ovat niin ikään itsenäisiä viranomaisia. Lisäksi laissa on annettu hakuehdoille ja niiden luokkien sisällölle rajoituksia.

Vaikka hakuehdon hyväksyttävyyden perusteena nähdään tietoliikennetiedustelulain 2 §:n 4 kohdan mukaisesti sen täsmällisyys ja tarkkarajaisuus, joka mahdollistaa mahdollisimman rajoitetun puuttumisen luottamuksellisen viestin suojaan[280], ei hakuehdoille kuitenkaan ole laissa tai sen esitöissä määritelty täsmällistä sisältöä, jolloin sen hyväksyttävyys jää suojelupoliisin ja tuomioistuimen harkintaan. Hakuehtojen tulee lain mukaan olla sellaisia, joiden avulla viestintäverkon osasta valitaan mahdollisimman täsmällisesti ja rajatusti kohteena oleva tietoliikenne ja puuttuminen luottamuksellisen viestin salaisuuden suojaan rajautuu välttämättömään. Hakuehto ei myöskään saa kuvata viestin sisältöä, ellei tietoliikennetiedustelun kohteena ole valtiollinen toimija tai siihen rinnastuva taho. Vaikka lain tasolla ei ole edellä esitetyn lisäksi tarkemmin määritelty hakuehtojen sisällöllisiä vaatimuksia, hallituksen antamassa lakiesityksessä on tällaisia käsitelty. Hakuehtoina voidaan täten käyttää esimerkiksi viestin lähettäjän ja vastaanottajan sähköpostiosoitteet, IP-osoitealueet tai viestissä käytetty salaustekniikka[281].

Hakuehtojen voidaan katsoa kiinnittyvän osaltaan niin laillisuusvaatimukseen sisältyvään ennakoitavuusvaatimukseen kuin välttämättömyysvaatimukseenkin. Kansallisessa

[278] Big Brother Watch and Others v. The United Kingdom (13.9.2018), kohdat 346-347.
[279] Big Brother Watch and Others v. The United Kingdom (13.8.2018), kohta 340.
[280] HaVM 36/2018 vp, s. 95.
[281] HE 202/2017 vp, s. 239.

lainsäädännössä yhteys välttämättömyysvaatimukseen on melko suoraan havaittavissa: hakuehtojen avulla puuttuminen luottamuksellisen viestin suojaan rajataan tietoliikennetiedustelulain 2 §:n 1 momentin 4 kohdan mukaan välttämättömään. Lakiin kirjattu hakuehtojen määritelmä, vaikkakaan se ei ota konkreettisesti kantaa hakuehtojen sisältöön, pyrkii rajoittamaan tiedusteluviranomaisen harkintavaltaa asettamalla ehdot sille, millainen hakuehdon tulisi olla. Ongelmallisena voidaan pitää osaltaan sitä, että tarkkaa kuvausta siitä, millainen hakuehto tai niiden luokka on, ei ole laissa. Toisaalta voidaan pohtia, onko hakuehdoille mahdollista antaa sellaista kuvausta, joka antaisi riittävän tarkan kuvan niiden sisällöstä mutta ei aiheuttaisi riskejä tiedustelutoiminnan tehokkuudelle.

Keskusteltaessa hakuehtojen ja hakuehtojen luokkien riittävän tarkasta sisältökuvauksesta tämän tutkimuksen yhteydessä on tärkeää korostaa jo useasti edellä mainittua asiaa, että Euroopan ihmisoikeustuomioistuin ei vaadi ennakoitavuusvaatimuksen täyttymiseksi hakuehtojen luettelointia laissa taikka edes lupavaatimuksessa. Yllä käsitellystä oikeuskäytännöstä voidaan kuitenkin katsoa, että hakuehtoihin kohdistuva valvonta on keskeinen tekijä rajoituksen ja Euroopan ihmisoikeussopimuksen yhteensopivuuden kannalta. Esimerkiksi Iso-Britannian tapauksessa käytettyihin valitsimiin kohdistuva ennakollisen, itsenäisen valvonnan puute aiheutti sen, että tuomioistuin ei katsonut ehdottoman välttämättömyysvaatimuksen täyttyvän. Vastaavasti Centrum för Rättvisa v. Sweden ratkaisussa tuomioistuin katsoi hakuehtojen altistamisen tuomioistuimen etukäteiselle valvonnalle erityisen vahvaksi oikeussuojakeinoksi – tämä on tekijä, joka Suomenkin tietoliikennetiedustelussa voi vahvistaa yksilön oikeusturvaa.

5.6. Viestintäverkon osan yksilöinti

Hakuehtoja ei ole sallittua käyttää kaikkeen Suomen rajat ylittävään tietoliikenteeseen, vaan suojelupoliisin tulee lupavaatimuksessa tuomioistuimelle määritellä niin täsmällisesti kuin mahdollista se osa viestintäverkkoa, jossa liikkuvaan tietoliikenteeseen tiedustelu on tarkoitus kohdistaa, sekä perustella viestintäverkon osan valinta. Viestintäverkon osan laajuus kussakin tilanteessa riippuu esimerkiksi uhan luonteesta tai siitä viestintämenetelmästä, jota uhan taustalla olevat henkilöt oletettavasti käyttävät. [282] Tiedot luvassa vaadittua viestintäverkon osaa varten saadaan teknisten tietojen käsittelyllä. Samoin kuten itse tietoliikennetiedustelua toteutettaessa, myös viestintäverkon osan yksilöintiin tarvittavat tekniset tiedot hankkii

[282] HE 202/2017 vp, s. 123; s. 244.

puolustusvoimien tiedustelulaitos suojelupoliisin toimeksiannosta. Teknisten tietojen käsittelystä suojelupoliisin puolesta säädetään tietoliikennetiedustelulain 10 §:ssä sekä sotilastiedustelulain 73 §:ssä.

Puolustusvoimien tiedustelulaitokselle on sotilastiedustelulain 66 §:ssä säädetty oikeus kerätä ja tallentaa hetkellisesti tietoliikenteen teknisiä tietoja sekä käsitellä niitä automaattisen tietojenkäsittelyn avulla. Tietoliikenteen teknisillä tiedoilla tarkoitetaan sotilastiedustelulain 10 §:n 11 kohdassa muita tietoja kuin viestin sisältöä, esimerkiksi välitystietoja ja IP-osoitealueita. Teknisten tietojen käsittelyn avulla on mahdollista saada tietoa esimerkiksi siitä, mistä viestintäverkon osasta tietyltä maantieteelliseltä alueelta tulee tietoliikennevirtaa. Menetelmän avulla tietoliikennetiedustelua on mahdollista kohdistaa paremmin vain sellaisiin viestintäverkon osiin, joissa liikkuu tietoliikennetiedustelun kannalta tärkeää viestintää ja rajata ulkopuolelle tietoliikennetiedustelun kannalta merkityksetön tietoliikenne. Viestinnän teknisistä tiedoista tehdyllä analyysillä hankitaan tarkempia tietoja tietoliikennetiedustelussa vaadittavaa lupahakemusta sekä tiedustelun kohdentamista varten. Teknisten tietojen käsittely on lyhytkestoista, ja analyysilla on tarkoitus selvittää, liikkuuko määrätyssä viestintäverkon osassa tietoliikennettä tietyltä maantieteelliseltä alueelta tai tietyltä toimijalta – sillä ei siis voi selvittää esimerkiksi viestin sisältöä tai sen osapuolena olevaa luonnollista henkilöä. Kerättyjä ja tallennettuja viestinnän teknisiä tietoja ei saa käyttää muuhun kuin tarvittavaan tilastolliseen analyysiin, jonka tekemisen jälkeen siinä käytetyt tiedot hävitetään välittömästi.[283]

Teknisten tietojen hankkimisesta säädetään sotilastiedustelua koskevan lain 66 ja 67:n pykälissä [284]. Puolustusvoimien tiedustelulaitokselle toimittamassaan toimeksiannossa suojelupoliisin tulee antaa tiedot teknisten tietojen kohdennettua ja rationaalista hankkimista varten. Tällaisia ovat esimerkiksi alustava kuvaus myöhemmin käytettävistä hakuehdoista sekä tieto siitä maantieteellisestä alueesta, josta tietoliikennetiedustelun kohteena olevaan toimintaan liittyvä tietoliikenne on peräisin. Rajaamisen onnistumiseksi on tärkeää myös saada keskeiset tiedot tiedonsiirtäjiltä. Myös tässä tapauksessa tuomioistuimelta tulee hakea

[283] HE 203/2017 vp, s. 276-278.
[284] Tietoliikennetiedustelulain 10 §:n 2 momentissa viitataan teknisten tietojen käsittelyyn ja käsittelystä päättämiseen liittyen virheellisesti sotilastiedustelulain 63 ja 64 §:ään, kun lainsäädäntövaiheessa ko. pykälät numeroitiin uudestaan ja niistä säädetään nyt 66 ja 67 §:ssä.

lupa teknisten tietojen hankkimista varten, mutta luvan hakee suoraan puolustusvoimien tiedustelulaitos suojelupoliisin puolesta.[285]

Tuomioistuimelta teknisten tietojen hankkimiseen haettava lupa ei vaadi merkittävää harkintaa, vaan se rajoittuu siihen, miten teknisiä tietoja käsitellään, mistä viestintäverkon osasta niitä hankintaan ja kuinka pitkään lupa on voimassa.[286] Tuomioistuimen teknisten tietojen keräämiseen myönnetyn luvan voimassaoloaika on enintään kolme kuukautta. Lupahakemuksessa tulee ilmoittaa se maantieteellinen alue, jonne tai johon liikkuvaan tietoliikenteeseen liittyvää osaa viestintäverkosta selvitetään. Jos maantieteellinen alue ei ole tiedossa, voidaan lupahakemuksessa ilmoittaa myös verkkoalue. Luvassa tulee myös nimetä ne viestintäverkon osat, josta tietoa haetaan, esimerkiksi tietoliikennekaapelin kuitu tai kuidun aallonpituus. Lisäksi luvassa yksilöidään teknisten tietojen käsittelyä valvova ja johtava, tiedustelumenetelmien käyttöön perehtynyt virkamies sekä suunnitelma siitä, miten teknisten tietojen kerääminen ja tallentaminen toteutetaan.[287]

Saatuaan teknisten tietojen analyysista tiedot viestintäverkon osasta, suojelupoliisi sisällyttää sen tuomioistuimelle laatimaansa lupavaatimukseen. Pelkän viestintäverkon osan ilmoittamisen lisäksi suojelupoliisin tulee antaa perustelut sen valinnalle. Valitun viestintäverkon osan perustelut tulee käydä ilmi myös lupapäätöksessä. Tietoliikennetiedustelun kohteeksi valikoitu viestintäverkon osan tulee olla rajattu niin suppeaksi kuin jokaisessa yksittäistapauksessa on välttämätöntä.[288] Perustuslakivaliokunta on kiinnittänyt lainvalmisteluvaiheessa huomiota siihen, ettei laissa ole määritelty sitä, miten suuresta osasta viestintäverkkoa voi olla kysymys tietoliikennetiedustelua harjoitettaessa ja korostaa jo hallituksen esityksessä mainittua tiedusteluviranomaisen vastuuta määritellä osa mahdollisimman tarkasti. Suojelupoliisin vastuu asiassa korostuu esimerkiksi sen vuoksi, että tiedustelutoiminnasta päättävällä tuomioistuimella ei välttämättä ole erityisen tarkkaa ja yksityiskohtaista tietoa tämänkaltaisesta teknisestä yksityiskohdasta.[289]

Viestintäverkon osan määrittely, käytettävien hakuehtojen ohella, kiinnittyy kuitenkin vahvasti perustuslain 10 §:n välttämättömyyteen, josta johtuu tietoliikennetiedustelulain 1 §:n 4 momentin kielto yleisestä ja kohdentamattomasta tietoliikenteen seurannasta. Euroopan ihmisoikeustuomioistuimen ratkaisuissa kohdentamatonta ”tukkuvalvontaa” ei pidetä

[285] HE 202/2017 vp, s. 249.
[286] HE 203/2017 vp, s. 295.
[287] HE 203/2017 vp, s. 279-280.
[288] HE 202/2017 vp, s. 244-245.
[289] PeVL 35/2018 vp, s. 20. Ks. myös Melander 2018, s. 13.

itsessään ihmisoikeussopimuksen vastaisena[290], mutta Suomen kansallinen lainsäädäntö ei tätä salli[291]. Hakuehtojen ja viestintäverkon rajaamisen voidaan katsoa olevan kriittiset tekijät sen suhteen, miten rajatusta tiedustelutoiminnasta todellisuudessa on kyse.

Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä viestintäverkon osan yksilöinnistä ja sen rajaamisesta ei ole määritelty kriteerejä, mutta pohdittaessa yksityiselämän ja luottamuksellisen viestin salaisuuden suojaan puuttumisen rajoittamista ei sitä tule sivuuttaa. Viestintäverkon osan yksilöinti on keskeinen tekijä, jos tietoliikennetiedustelusta ei haluta tukkuvalvonnan kaltaista toimintaa.

Ratkaisussa Liberty and Others v. The United Kingdom Iso-Britannian lainsäädäntö salli hyvin laajan tietoliikenteen kaappaamisen (interception of communications). Lainsäädännössä ei yksilöity, millaista tietoliikennettä on sallittua siepata, vaan lain mukaan oli sallittua kaapata sellaista Iso-Britanniasta lähtevää ja sinne saapuvaa tietoliikennettä, mikä luvassa oli määritelty. Valittajien mukaan luvissa käytettiin ilmaisuja kuten ”kaikki kaupalliset merikaapelit (commercial submarine cables), joilla on yksi pääte (terminal) Iso-Britanniassa ja jotka kuljettavat kaupallista (commercial) tietoliikennettä Eurooppaan”, jolloin kaikki tähän kategoriaan sisältyvä tietoliikenne tulisi kaapatuksi (intercepted). Iso-Britannian valtionjohto myönsi selvityksessään tuomioistuimelle, että periaatteessa kenen tahansa henkilön, joka lähetti tai vastaanotti viestejä teleyhteyksien kautta Britannian ulkopuolelta tai ulkopuolelle saattoi joutua tiedustelun kohteeksi. Euroopan ihmisoikeustuomioistuin katsoo, että tästä johtuen tiedusteluviranomaiselle myönnetty oikeudellinen harkintavalta suorittaa konkreettista, salaista tiedonhankintaa oli käytännöllisesti katsoen rajoittamatonta[292], minkä tyyppinen tiedustelutoiminta on Suomessa säädetty perustuslain vastaiseksi.

Ruotsin lainsäädännössä signaalitiedustelun kohdentamisesta oli säädetty samankaltaisesti kuin Suomessa. Ruotsin signaalitiedustelua oli sallittua kohdistaa vain rajat ylittäviin kaapeleihin ja ne täytyy yksilöidä tiedustelutoimintaan vaaditussa luvassa. Tuomiossaan Centrum för Rättvisa v. Sweden Euroopan ihmisoikeustuomioistuin katsoi kattavan kohdeluettelon ohella tärkeäksi sen, että Ruotsin kansallinen lainsäädäntö rajasi signaalitiedustelun vain rajat ylittävään tietoliikenteeseen. Ihmisoikeustuomioistuin on pitänyt

[290] Ks. esimerkiksi tuomioistuimen ratkaisu Big Brother Watch and Others v. The United Kingdom (13.9.2018) kohta 314.
[291] Perustuslakivaliokunta katsoo mietinnössään PeVM 4/2018 vp, s. 7, että luottamuksellisen viestin rajoitteena toimiva välttämättömyysvaatimus edellyttää siihen puuttumisen olevan erittäin rajattua ja kohdennettua. Lisäksi tietoliikennetiedustelulain 1 § 4 momenttiin on kirjattu, ettei tietoliikennetiedustelun sallita olevan ”[…]yleistä ja kohdentamatonta tietoliikenteen seurantaa.”
[292] Liberty and Others v. The United Kingdom (1.8.2008) kohta 64.

Ruotsin tiedustelutuomioistuimen valvontaskaalaa erittäin kattavana osittain siitä syystä, että tiedustelun kohteena olevat kantoaallot on mainittava lupahakemuksessa ja täten ne alistetaan tuomioistuimen kontrollille.[293]

Vaatimus viestintäverkon osan rajaamisesta liittyy vahvasti välttämättömyysvaatimukseen, sillä sen avulla tietoliikennetiedustelu voidaan kohdistaa vain siihen mikä on välttämätöntä. Kuitenkin, kuten edellä todettu, laissa tai sen esitöissä ei missään määritellä, kuinka laajasta osasta viestintäverkkoa voi olla kysymys. Viestintäverkon rajaaminen on määritelty siten, että tietoliikennetiedustelua ei saa kohdistaa koko rajat ylittävään viestintäverkkoon. Tällöin voidaan kärjistetysti ajatella, olisiko kaikki alle 100 % osuuteen viestintäverkosta kohdistuva tiedustelu lainmukaista. Viestintäverkon osan määrittelyssä on siis tärkeää, että suojelupoliisi tosiasiallisesti perustelee pyydetyn osan laajuuden ja vastaavasti tuomioistuimen tulee todentaa, onko viestintäverkon laajuus tosiasiassa välttämättömyysedellytyksen täyttävä.

[293] Centrum för Rättvisa v. Sweden (19.6.2018), kohta 121.

6. Johtopäätökset

Tämän tutkimuksen päämääränä oli selvittää, miten siviilitiedustelussa suoritettavan tietoliikennetiedustelun ennakollisella lupamenettelyllä voidaan taata todellinen ennakkovalvonta. Todellisella ennakkovalvonnalla pyritään varmistamaan, että luottamuksellisen viestin suojaan puututaan mahdollisimman rajoitetusti eikä sitä loukata kuin siten, kuin rajoituksista on säädetty. Tällöin keskeinen kysymys on, miten ennakollisella lupamenettelyllä varmistetaan, että perus- ja ihmisoikeuksien rajoituksia sovelletaan siten, kuin on tarkoitettu. Tutkimuksen näkökulma painottui Euroopan ihmisoikeustuomioistuimen asiasta antamiin ratkaisuihin sekä itse lupapäätöksen ja -vaatimuksen sisältöön. Siviilitiedustelussa suoritettava tietoliikennetiedustelu puuttuu erityisesti yksilön yksityiselämän suojaan, tarkemmin luottamuksellisen viestin salaisuuden suojaan. Tämän vuoksi tutkimuskysymystä tarkasteltiin erityisesti luottamuksellisen viestin salaisuuden suojan rajoittamisen näkökulmasta.

Todellisen ennakkovalvonnan toteutumiseksi tuomioistuimella tulee olla todellinen mahdollisuus arvioida lupavaatimusta ja testata sen soveltuvuutta Euroopan ihmisoikeussopimuksesta johtuvien rajoitusvaatimusten näkökulmasta. Kansalliset perus- ja ihmisoikeuksien rajoitukset ovat yhteensopivia Euroopan ihmisoikeussopimuksen kanssa, jos ne täyttävät siitä johtuvat vaatimukset eli laillisuusvaatimuksen, välttämättömyysvaatimuksen sekä hyväksyttävän päämäärän vaatimuksen. Laillisuusvaatimus jakaantuu edelleen kolmeen alakohtaan: 1) kansallisessa laissa tulee olla peruste oikeuksiin puuttumiselle; 2) oikeuksia rajoittavan lainsäädännön tulee olla yhteensopiva oikeusvaltioperiaatteen kanssa sekä kansalaisen saatavilla ja 3) yksittäisen kansalaisen tulee voida ennakoida lainsäädännön seuraukset omalla kohdallaan.

Luottamuksellisen viestin suojan rajoittamisesta on säädetty laissa, ja niin laki kuin esityötkin ovat yksittäisen kansalaisen saatavilla. Oikeusvaltioperiaatteen mukaan julkisen toiminnan tulee perustua lakiin ja kaikessa julkisessa toiminnassa tulee noudattaa lakia – tietoliikennetiedustelun käytöstä sekä lupavaatimuksen ja -päätöksen sisällöstä on säädetty eduskuntalaissa, ja se sitoo kaikkia viranomaisia. Laissa on myös määritelty tietoliikennetiedustelun kohteet sekä rajattu sen ulkopuolelle Suomen sisäinen viestintä, mikä antaa yksilölle mahdollisuuden ennakoida lain vaikutuksia omalla kohdallaan. Välttämättömyysvaatimuksen täyttämiseksi laissa on kaiken siviilitiedustelun yleiseksi edellytykseksi asetettu välttämättömyys, ja tietoliikennetiedustelu on viimesijainen

tiedustelumenetelmä muihin nähden – tällöin sen käytön on oltava ehdottoman välttämätöntä. Tietoliikennetiedustelua saa käyttää sellaisiin toimiin, jotka muodostavat vakavan uhan kansalliselle turvallisuudelle, joka on yksi Euroopan ihmisoikeussopimuksen sallituista päämäristä. Yleisellä, lain sanamuodon tasolla vaatimukset näyttäisivät täyttyvän. Ratkaisevaksi tekijäksi siis muodostunee se, miten lakia sovelletaan käytännössä.

Keskeisenä tekijänä todellisen tuomioistuinkontrollin, ja täten todellisen ennakkovalvonnan, toteutumisen kannalta voidaan tutkimuksen perusteella pitää niin tuomioistuimen esittämiä perusteluja lupapäätöksen ratkaisussa kuin suojelupoliisin tuomioistuimelle antamia tietoja. Lupapäätöksen ja -vaatimuksen sisällöstä säädetään tietoliikennetiedustelulaissa. Tällöin se asettaa sekä suojelupoliisille että tuomioistuimelle vaatimukset siitä, mitä tietoja viranomaisen tulee sisällyttää niin vaatimukseen kuin päätökseen. Lupapäätös rajoittaa näin omalta osaltaan tiedusteluviranomaisen harkintavaltaa, ja siksi sen sisällöllä on keskeinen rooli luottamuksellisen viestin salaisuuden suojan kannalta.

Tuomioistuimen oman harkinnan näkyminen perusteluissa on osaltaan sellainen tekijä, johon salaisten pakkokeinojen lupien myöntämisessä on kiinnitetty huomiota ja joka on koettu puutteelliseksi. Toisaalta jo ennen lupavaatimuksen esittämistä tuomioistuimelle on siihen kohdistettava arviointia suojelupoliisin sisäisen valvonnan osalta. Vaikka päätös luvan myöntämisestä on tuomioistuimella, tulee suojelupoliisin viedä lupavaatimuksia tuomioistuinkäsittelyyn harkiten. Sen tulee lupaa laatiessa suorittaa jatkuvaa arviointia lupavaatimuksen tarpeellisuudesta sekä siitä, onko tietoliikennetiedustelulle olemassa todellista perustetta. Niin perustuslakivaliokunnan lausunnoista kuin Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä on nähtävissä, että tiedusteluviranomaisella, tässä tapauksessa suojelupoliisilla, on vastuu antaa tuomioistuimelle tarvittavat tiedot päätöksen tekemistä varten sekä osoittaa tiedustelumenetelmän ja yleisten periaatteiden yhteensopivuus.

Euroopan ihmisoikeustuomioistuin ei tässä tutkimuksessa käsitellyssä oikeuskäytännössä ole lausunut lupavaatimuksen sisällöstä lukuun ottamatta sitä, että lupapäätöksessä on mainittava se henkilö, johon tiedustelu kohdistuu tai ne edellytykset, joihin perustuen tiedustelua harjoitetaan. Voidaan kuitenkin huomauttaa, että Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään katsonut Ruotsin lainsäädännössä määritellyn lupavaatimuksen ja -päätöksen sisällön ihmisoikeussopimuksen kannalta hyväksyttävänä, joka on pitkälti yhtenevä Suomeen säädetyn kanssa. Erityiseksi oikeussuojakeinoksi on katsottu sekä hakuehtojen että tiedustelun kohteena olevien kantoaaltojen alistaminen tuomioistuimen ennakkovalvonnalle.

Vastaavasti Iso-Britannian lupamenettelyssä ongelmalliseksi nähtiin se, että seulontaan käytettäviin valitsimiin ei kohdistettu itsenäistä valvontaa.

Tietoliikennetiedustelun kohde on tietoliikennetiedustelulain mukaan nimettävä lupapäätöksessä ja -vaatimuksessa, ja lisäksi sallitut kohteet on määritelty laissa, jolloin tietoliikennetiedustelua ei saa kohdistaa muihin tekijöihin. Euroopan ihmisoikeustuomioistuin ei ole vaatinut jäsenvaltioiltaan tällaista tyhjentävää listausta ennakoitavuusvaatimuksen täyttymiseksi, ja esimerkiksi Szabó and Vissy v. Hungary tapauksessa suhteellisen väljästi määritellyt kohteet katsottiin riittävän selkeiksi. Myös Suomeen säädettyä kohdeluetteloa on arvosteltu sen laajoista ilmaisuista, mutta Unkarin tapauksessa Euroopan ihmisoikeustuomioistuin on muistuttanut, että lainsäädännön tulee pysyä muuttuvien olosuhteiden mukana, jolloin on perustelua välttää liikaa jäykkyyttä. Vastaavasti Centrum för Rättvisa v. Sweden tapauksessa tuomioistuin katsoi joidenkin signaalitiedustelulaissa nimettyjen kohteiden osalta ne ilmaistun laajasti, mutta piti menestyksekkäänä sitä, että niitä avattiin esitöissä, jotka ovat kansallisella tasolla keskeinen oikeuslähde. Tässäkin Suomeen säädetty malli on pitkälti samankaltainen kuin Ruotsissa, joten puhtaasti tähän nojautuen sääntelyä voidaan pitää onnistuneena.

Kansallisessa lainsäädännössä keskeistä on, että tietoliikennetiedustelun kohde muodostaa vakavan uhan Suomen kansalliselle turvallisuudelle. Vakava uhka on määritelty jo itsessään yhdeksi tietoliikennetiedustelun käytön yleiseksi edellytykseksi. Tietoliikennetiedustelulaissa säädetty listaus on perustuslakivaliokunnassa katsottu sellaiseksi, että siinä luetellut tekijät ja toimet voivat muodostaa vakavan uhan kansalliselle turvallisuudelle, vaikkakaan kaikissa kohteissa ei erikseen mainita vakavan uhan vaaraa. Tällöin on lupavaatimuksessa sekä -päätöksessä tärkeää tuoda esiin ne seikat, joilla perustellaan uhan vakavuusaste. Voidaan esimerkiksi pohtia, missä vaiheessa ja tilanteessa ”vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille, taloudellisille tai muille tärkeille eduille”, on luonteeltaan sellaista, että se muodostaa vakavan uhan kansalliselle turvallisuudelle.

Välttämättömyysvaatimusta tarkasteltaessa keskiöön nousee suurin osa luvan eri osa-alueista: hakuehdot ja niiden luokat, luvan kesto, viestintäverkon osa, tietoliikennetiedustelun viimesijaisuus sekä tietoliikennetiedustelun yleiset edellytykset. Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään katsonut, että välttämättömyysvaatimuksen täyttymiseksi ei riitä, että se mainitaan laissa tai sitä vaaditaan tiedusteluviranomaisen laatimassa luvassa. Szabo and Vissy v. Hungary tapauksessa nähtiin, että tiedusteluviranomaisen tulee antaa luvasta päättävälle taholle sellaiset tiedot, joiden avulla

välttämättömyyden arviointi on mahdollista. Tästä voidaan päätellä, että kansallisella tasolla lupavaatimuksessa ei riitä, että tietoliikennetiedustelun käyttö tai jokin muu osa-alue perustellaan sillä, että se on välttämätöntä, vaan jokaisessa yksittäistapauksessa välttämättömyyden tueksi tulee esittää riittävät tosiasiat.

Hakuehdot ja niiden luokat sekä viestintäverkon osan määrittely ovat keskeisiä tekijöitä tietoliikennetiedustelun rajaamisessa välttämättömään. Hakuehdoista ja niiden määritelmistä keskusteltiin lakia säädettäessä monessa eri vaiheessa, vaikka tätä ei katsottu sellaiseksi, joka estäisi lain säätämisen tavallisessa säätämisjärjestyksessä. Hakuehtojen ja niiden luokkien alistaminen tuomioistuinvalvonnalle on nähty Centrum för Rättvisa v. Sweden -ratkaisussa erityiseksi oikeussuojakeinoksi, jolloin sitä voidaan pitää sellaisena myös Suomen tietoliikennetiedustelussa. Hakuehtojen käsittelyssä korostuu suojelupoliisin esittämät perustelut käytettävien hakuehtojen sekä tiedustelun kohteen välillä sekä se, mitä tietoa kyseisillä hakuehdoilla on tarkoitus saada kohteena olevasta toiminnasta. Näiden tosiasioiden perusteella tuomioistuimelle tarjotaan mahdollisuus arvioida sitä, täyttyykö välttämättömyysvaatimus. Hakuehtoja määriteltäessä on varmistuttava siitä, että niitä koskevat rajoitukset täyttyvät. Tällaisia ovat esimerkiksi kielto viestin sisällön käyttämisestä hakuehtona. Tuomioistuimen salliessa hakuehtojen luokan käytön suojelupoliisilla on erityinen vastuu siitä, että luvan myöntämisen jälkeen käytettävät hakuehdot tosiasiallisesti kuuluvat sallittuun luokkaan ja samalla täyttävät muut hakuehtoja koskevat vaatimukset.

Szabó and Vissy v. Hungary tapauksessa Euroopan ihmisoikeustuomioistuin katsoi, että tuomioistuinkontrolli voi toimia tiedusteluviranomaisen harkintavallan rajoittajana esimerkiksi tulkittaessa laajoja termejä ja tarjota tällaisille termeille vakiintuneen tulkinnan sekä vakiintuneen käytännön siihen, milloin on olemassa perusteltu syy yksilön viestintään puuttumiselle. Kansallisella tasolla tällainen tulkinta ja käytäntö voisi tulla kyseeseen esimerkiksi juuri hakuehtojen kohdalla, joiden määritelmä ja sisältö herätti lainsäädäntövaiheessa keskustelua.

Samankaltaisesti suojelupoliisin tulee perustella se viestintäverkon osa, johon tietoliikennetiedustelua kohdistetaan. Laissa ei määritellä tarkkaan, miten suuresta osasta viestintäverkkoa voi olla kysymys - tietoliikennetiedustelusta on lähtökohtaisesti rajattu ulos Suomen sisäinen tietoliikenne, mutta samalla se ei saa kohdistua kaikkeen Suomen rajojen ulkopuoliseenkaan viestintään. Ratkaisevaksi tekijäksi muodostunee jokaisessa yksittäistapauksessa annetut perustelut viestintäverkon osan valinnalle ja yhteys tietoliikennetiedustelun kohteeseen. Ratkaisussa Centrum för Rättvisa v. Sweden Euroopan

ihmisoikeustuomioistuin katsoi merkittäväksi sen, että tiedustelun kohteena olevat kantoaallot nimettiin lupavaatimuksessa. Meriittinä katsottiin myös se, että signaalitiedustelua sai kohdistaa vain rajat ylittävään tietoliikenteeseen. Kuten edellä todettiin, tulee lupavaatimuksessa Euroopan ihmisoikeustuomioistuimen mukaan nimetä ne ihmisryhmät, keihin tiedustelu kohdistuu – tämänkaltaisella sääntelyllä kohderyhmäksi rajautuvat ne henkilöt, joiden viestintä kulkee Suomen valtion rajojen yli.

Välttämättömyysedellytystä tiedustelutoimien kohdalla tulee Euroopan ihmisoikeustuomioistuimen oikeuskäytännön perusteella tulkita ehdottomana välttämättömyytenä, ja kansallisella tasolla tietoliikennetiedustelun käyttämisessä ehdottoman välttämättömyyden vaatimus pyritään täyttämään sen viimesijaisuudella suhteessa muihin siviilitiedustelumenetelmiin. Kuten tätä käsittelevässä osiossa 5.4. todettiin, siviilitiedustelun eri menetelmien käytön yleisten edellytysten ja kohteiden ollessa samat, viimesijaisuus on se tekijä, joka korostaa tietoliikennetiedustelun erityisluonnetta muista siviilitiedustelumenetelmistä. Jos viimesijaisuuden arviointi on suojelupoliisin oman harkinnan varaista ja voi perustua kokonaisarviointiin muiden siviilitiedustelumenetelmien käytön tehottomuudesta tai voimavarojen käyttömäärästä, tulee tuomioistuimen lupamenettelyssä varmistaa ehdottoman välttämättömyyden tosiasiallinen täyttyminen. Tuomioistuinkontrollin epäonnistumiseen katsottiin Roman Zakharov v. Russia tapauksessa osasyyksi juuri välttämättömyysvaatimuksen testaamisen puute. Välttämättömyysvaatimus pitää sisällään myös suhteellisuusvaatimuksen, joka niin ikään kytkeytyy kiinteästi viimesijaisuusedellytykseen. Käytetyn menetelmän ja halutun päämäärän on oltava järkevässä suhteessa toisiinsa. Jos tieto voidaan hankkia vähemmän puuttuvalla tavalla, on sovellettava sitä menetelmää.

Tässä tutkimuksessa käsiteltyyn oikeuskäytäntöön perustuen voidaan katsoa, että tiedusteluviranomaisella on vastuu antaa tuomioistuimelle riittävät tiedot ja perustelut välttämättömyysvaatimuksen täyttymisen arvioimiseksi ja vastaavasti luvan myöntämän tuomioistuimen on tosiasiallisesti testattava vaatimuksen täyttymistä. Kansallisella tasolla yllä esitetyn perusteella tämä tarkoittaa lähinnä yksittäisten luvan osa-alueiden ja tietoliikennetiedustelun kohteen sekä sillä saavutettavan tiedon välisen yhteyden selvittämistä sekä perusteluja jokaisessa yksittäistapauksessa käsiteltävänä olevan tiedustelutehtävän viitekehyksessä.

Tiedustelutoiminnan keston rajojen määrittely on yksi niistä Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä määritellyistä minimivaatimuksista, jotka

kansallisessa laissa tulisi olla määriteltyinä järjestelmän väärinkäytön estämiseksi. Kansallisessa lainsäädännössä kuusi kuukautta on luvan maksimivoimassaoloaika, jonka tuomioistuin on esimerkiksi ratkaisussaan Centrum för Rättvisa v. Sweden katsonut hyväksyttäväksi. Laissa säädetään lisäksi, että tiedustelumenetelmän käyttö on lopetettava, jos sen käytölle ei ole enää perusteita. Kuten edellä on todettu, sinällään sääntely voidaan katsoa Euroopan ihmisoikeustuomioistuimen oikeuskäytännön mukaiseksi. On kuitenkin keskeistä, että välttämättömyysvaatimuksesta johtuvat edellytykset huomioidaan niin luvan keston kuin tietoliikennetiedustelun käytön lopettamisen arvioinnissa. Myös viranomaisen mahdollisuus keskeyttää luvan käyttö nähtiin Kennedy v. The United Kingdom tuomiossa tärkeäksi oikeussuojakeinoksi, koska se velvoitti tiedusteluviranomaisia arvioimaan luvan tarpeellisuutta jatkuvasti. Tämänkaltainen oikeus keskeyttää luvan käyttö on Suomessa säädetty tiedusteluvalvontavaltuutetulle, mutta sitä on pidettävä erityisenä valvontakeinona, jonka käyttäminen on tarkoitettu viimesijaiseksi. Keskeytysoikeuden tosiasiallinen merkitys tehokkaana valvontakeinona tai sen vaikutus suojelupoliisin jatkuvaan arviointiin luvan tarpeellisuudesta voidaan todeta vasta myöhemmin.

Tutkimuksessa käsitellystä oikeuskäytännöstä kuitenkin nähtiin, että Euroopan ihmisoikeustuomioistuimen mukaan laissa tulisi määritellä myös luvan uusimisen mahdollistavat olosuhteet - tästä ei ole tietoliikennetiedustelulaissa säädetty. Lupa voi olla voimassa kuusi kuukautta kerrallaan, jolloin voidaan olettaa, että se on mahdollista uusia. Sen tarkemmin ei kuitenkaan määritellä, mitä luvan uusimiseen liittyvässä vaatimuksessa tulee esittää tai millä perusteilla se voidaan uusia. Esimerkkitapauksista Iso-Britanniassa, Ruotsissa ja Venäjällä lupaa uusiessa vaadittiin tiedustelutehtävän uudelleen arviointia ja lisäksi Iso-Britanniassa tuli arvioida siihen mennessä saadun tiedon arvoa. Tällaisten vaatimusten lisääminen lainsäädäntöön mahdollisesti nostaisi luvan uusimisen kynnystä tai ainakin lisäisi sen tarpeellisuuden arviointia.

Tilanteessa, jossa luvan uusimisesta ei ole säännelty, korostuu taas kerran vaatimus välttämättömyyden arvioinnista sen suhteen, onko luvan uusimiselle olemassa tosiasiallinen tarve. Jos luvan uusimiseksi vaaditaan pelkästään samat tiedot kuin alkuperäiseen lupaan, voi syntyä tilanne, jossa jatkolupia myönnetään vähemmällä tarkastelulla kuin ensimmäisiä lupia. Tällaisessa tilanteessa tulisi tuomioistuimelle, ja mahdollisesti myös läsnä olevalle tiedusteluvalvontavaltuutetulle tulla joka tapauksessa kyseeseen kyselyoikeuden käyttö uusimisen tarpeesta. Suojelupoliisin olisi tässä tilanteessa mahdollista perustella luvan uusimisen tarvetta juurikin jo saavutetun tiedon arvioinnilla. Samalla saavutetun tiedon

arviointi mahdollistaa tehokkuuden testaamisen, mikä myös osaltaan vaikuttaa luvan uusimisen mahdollisuuteen.

Erityinen piirre lupamenettelyssä on suojelupoliisille säädetty oikeus päättää itse tietoliikennetiedustelun aloittamisesta tietyissä olosuhteissa. Kiiremenettely on sinänsä yhteensopiva tutkimuksessa käsitellyn oikeuskäytännöstä johtuvien vaatimusten kanssa, ja erityisesti tuomioistuimen suorittama jälkikäteinen arviointi on nähtävä oikeussuojaa vahvistavana tekijänä. Sääntely kuitenkin antaa mahdollisuuden väärin perustein hankitun tiedon säilyttämiselle ja hyödyntämiselle tietyin ehdoin, mikä sisältää mahdollisuuden järjestelmän väärinkäyttöön. Tässäkin on tärkeää seurata menettelyn käyttöä ja toimivuutta – siitä ei ole, kuten edellä todettu, tarkoitettu muodostuvan pääsääntö tietoliikennetiedustelun aloittamisessa.

Tuomioistuimen suorittamaa ennakkovalvontaa on Euroopan ihmisoikeuskäytännössä pidetty yleisesti parhaana oikeusturvatakeena salaisten tiedonhankinakeinojen käytöstä päätettäessä. Kansallisessa järjestelmässä on kuitenkin varmistettava, että tuomioistuinkontrolli on todellista. Helsingin käräjäoikeus on kokemuksensa vuoksi nähty parhaaksi valinnaksi siviilitiedustelumenetelmien käytön valtuuttajaksi, mutta samalla keskusteluissa on noussut esiin huoli siitä, että salaisten pakkokeinojen kohdalla tapahtuneet erheet toistuisivat myös siviilitiedustelun lupamenettelyssä. Tuomioistuinmenettelyssä korostuu sekä tiedusteluviranomaisen että tuomioistuimen vastuu: tiedusteluviranomaisen eli suojelupoliisin on annettava tuomioistuimelle tarpeelliset tiedot siten, että tuomioistuimella on todellinen mahdollisuus arvioida tiedustelumenetelmän tarpeellisuutta. Vastaavasti tuomioistuimella on velvollisuus käyttää kyselyoikeuttaan ja tosiasiallisesti suorittaa Euroopan ihmisoikeussopimuksesta johtuvat rajoitustestit.

Tuomioistuimen kokoonpano herätti lainsäädäntövaiheessa keskustelua. Euroopan ihmisoikeustuomioistuin ei ole tässä käsitellyssä oikeuskäytännössä ottanut kantaa tuomioistuimen kokoonpanoon, mutta verrattuna esimerkiksi Ruotsissa sovellettavaan järjestelyyn on Suomen käräjäoikeuden kokoonpano suhteellisen pieni – vähimmillään tietoliikennetiedustelusta päätettäessä paikalla on yksi käräjätuomari ja suojelupoliisin virkamies. Toisin kuin esimerkiksi tietoliikennetiedustelun lopettamisesta tai keskeyttämisestä päätettäessä, kahden tuomarin kokoonpanoa ei vaadita tiedustelumenetelmän käytöstä päätettäessä – näkökulma, johon perustuslakivaliokunta kiinnitti huomiota lausunnossaan.

Oikeusturvan toteutumisen näkökulmasta vahvennettu kokoonpano sekä tiedusteluvalvontavaltuutetun läsnäolo olisi optimaalista, mutta käytännön toteutusta voidaan perustellusti pohtia. Lain mukaan lupavaatimus on käsiteltävä kiireellisesti, ja useamman henkilön kokoontuminen voi tosiasiallisesti olla aikaa vievää. Toisaalta taas kyseessä on syvälle perus- ja ihmisoikeuksiin puuttuva menetelmä, joka lisäksi on täysin uusi, jolloin mahdollisimman laaja asiantuntijuuden varmistaminen on perustelua. Tässä, kuten monessa muussakin tietoliikennetiedusteluun liittyvässä näkökohdassa, on tärkeää arvioida ja seurata menettelyn toimivuutta ja kehittää järjestelmää sen mukaisesti.

Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä johtuvat laillisuusvaatimus ja vaatimus hyväksyttävästä päämäärästä näyttävät lainsäädännön sanamuodon tasolla toteutuvan Suomessa pitkälti hyvin. Kuten useasti todettu, käytännön toteutus on asiassa ratkaiseva tekijä, ja esimerkiksi välttämättömyysvaatimuksen täyttyminen pystytään todella toteamaan vasta käytännössä. Tällä hetkellä välttämättömyys on asetettu tietoliikennetiedustelun käytön yleiseksi edellytykseksi ja ehdoton välttämättömyys tulee arvioida jokaisessa yksittäistapauksessa tietoliikennetiedustelun käytön viimesijaisuuden kautta.

Luvan osa-alueista suurin osa kiinnittyy välttämättömyyden arviointiin, ja välttämättömyyden ollessa lisäksi yleinen edellytys tietoliikennetiedustelun käytölle, ei muulla lupavaatimukseen sisällytettävällä tiedolla ole merkitystä – jos tietoliikennetiedustelun käyttäminen ei ole välttämätöntä, sitä ei ole sallittua käyttää. Lupavaatimusta arvioitaessa on siis keskeistä varmistaa, että välttämättömyysvaatimus täyttyy niin yleisellä tasolla kuin luvan yksittäisten osa-alueiden kohdalla. Todellisen ennakkovalvonnan toteutumiseksi suojelupoliisin tulee antaa tuomioistuimelle tarvittavat tiedot välttämättömyysvaatimuksen täyttymisen arvioimiseksi ja vastaavasti tuomioistuimen tulee testata sen toteutuminen.

Lopuksi on tärkeä nostaa esiin, että lupavaatimus- ja päätös sekä lupamenettely kokonaisuudessaan on yksi osa isompaa tiedustelujärjestelmää, jossa valvontaa suoritetaan myös reaaliaikaisesti sekä jälkikäteisin oikeussuojakeinoin. Tärkeämpää, kuin lain jonkin yksittäisen osa-alueen arviointi hypoteettisella tasolla, on se, että järjestelmän toimivuutta ja yhdenmukaisuutta kansainvälisten ihmisoikeussopimuksien kanssa seurataan tarkasti ja ennen kaikkea kehitetään. Virheiltä on täysin uudessa ja testaamattomassa järjestelmässä miltei mahdotonta välttyä. Keskeistä on, että virheet tunnistetaan ja niitä parannetaan – järjestelmän kehittäminen on näkökohta, johon Euroopan ihmisoikeustuomioistuin kiinnitti huomiota

Centrum för Rättvisa -tapauksessaan ja se on osasyy siihen, miksi järjestelmää pidettiin menestyksekkäänä[294].

Hallintovaliokunnan mietinnössä tämä näkökulma otettiin myös huomioon, ja siihen lisättiin ehdotus eduskunnan lausumasta koskien sitä, että hallituksen on tarkasti seurattava siviilitiedustelulain tuloksellisuutta, tehokkuutta, toimivuutta sekä oikeusturvan toteutumista ja annettava tästä seurannasta hallintovaliokunnalle vuoden 2020 loppuun mennessä kirjallinen selvitys, sekä vuoden 2021 loppuun mennessä annettava seikkaperäisempi selonteko, joka sisältää mm. arvioinnin tiedustelulainsäädännön kehittämistarpeista[295].

Jatkotutkimuksen kannalta juuri järjestelmän sudenkuoppien tunnistaminen ja niiden kehittäminen on relevantti tutkimuskohde. Mielenkiintoista voi olla esimerkiksi seurata, miten lainsäädäntövaiheessa keskustelua aiheuttaneet teemat kehittyvät tulevien vuosien kuluessa vai nouseeko käytännössä esiin uusia, kehittämistä vaativia asioita. Yllä mainittu hallituksen selvitys ja vastaavasti tiedusteluvalvontavaltuutetun vuosikertomus voivat esimerkiksi antaa jonkinlaista pohjaa aiheesta tehtäville jatkotutkimuksille.

[294] Centrum för Rättvisa v. Sweden (19.6.2018), kohta 180.
[295] HaVM 36/2018 vp, s. 161-162. Eduskunta hyväksyi lausuman vastauksessaan EV 291/2018 vp.