

**Kansallinen turvallisuus vs. perusoikeudet:
Lainsäädäntötutkimus tiedustelulakihankkeesta**

Mika Havulinna (50007)
Pro gradu –tutkielma
Turun yliopisto
Oikeustieteellinen tiedekunta;
oikeussosiologia ja kriminologia
Syyskuu 2018

Turun yliopiston laatujärjestelmän mukaisesti
tämän julkaisun alkuperäisyys on tarkastettu Turnitin
OriginalityCheck -järjestelmällä.

TURUN YLIOPISTO
Oikeustieteellinen tiedekunta

HAVULINNA, MIKA: Kansallinen turvallisuus vs. perusoikeudet:
Lainsäädäntötutkimus tiedustelulakihankkeesta

Pro gradu -tutkielma, 97 s.

Oikeussosiologia ja kriminologia

Syyskuu 2018

Turun yliopiston laatujärjestelmän mukaisesti tämän julkaisun alkuperäisyys on tarkastettu Turnitin Originality Check –järjestelmällä.

Tutkimuksen aiheena on turvallisuusviranomaisten harjoittaman tiedustelutoiminnan ja erityisesti tietoliikennetiedustelun saattaminen osaksi kansallista lainsäädäntöämme.

Tiedonhankintalakitöryhmä muodostettiin 13.12.2013, ja sen tehtäväksi annettiin lainsäädännön kehittäminen turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi. Mietinnössä arvioitiin myös tiedustelua koskevan lainsäädännön kehittämistarpeita. Työryhmä ehdotti, että hallitus käynnistäisi tarvittavat toimenpiteet tiedustelua koskevan lain tai lakien säätämiseksi. Tiedustelulla olisi tarkoitus hankkia kansallisen turvallisuuden kannalta välttämätöntä tietoa muun muassa vakavista kansainvälisistä uhista.

Tutkimuksen tarkoituksena on selvittää minkälaisilla uhkakuvilla tai muilla perusteilla tiedustelulakihanketta Suomeen vaaditaan sekä minkälaisia argumentteja lainvalmistelussa mukana olevat osapuolet esittävät niistä toimivaltuuksista ja keinoista, joilla tiedustelua olisi tarkoitus harjoittaa. Lisäksi pyrkimyksenä on saada selville mitkä perus- ja ihmisoikeudet ja miten niitä vaaditaan huomioonotettavaksi säädösprosessin valmisteluvaiheessa.

Tutkimuksessa käytetään pääasiassa aineistoa, joka oli tiedustelulakihankkeesta saatavilla toukokuussa 2015 ja kohteena on lainsäädäntöprosessin ensimmäisen lausuntokierroksen valmisteluvaihe. Virallislähteinä tuossa vaiheessa olivat tiedonhankintalakitöryhmän mietintö lausuntopyyntöineen, liikenne- ja viestintäministeriön edustajan eriävä mielipide em. mietintöön ja mietinnöstä annetut 74 erillistä lausuntoa (252 A4 –sivua).

Tutkimuksen pääasiallisena tutkimusmenetelmänä on kvalitatiivinen eli laadullinen, jonka avulla on sisällönanalyysin keinoin löytää ja eritellä aineistosta esiin nousevia teemoja ja argumentteja hankkeen puolesta ja vastaan.

Lakihanketta puoltavien lausuntojen merkittävimmäksi teemaksi nousi tiedustelutiedon välttämättömyys turvallisuuden takaamiseksi. Vastustavien lausuntojen merkittävin teema oli, että esitetty tietoliikennetiedustelu on tehotonta. Esitettyjen tiedustelukeinojen vaarantamat keskeisimmät perusoikeudet ovat yksityiselämän suoja ja luottamuksellisen viestin salaisuuden suoja. Lisäksi voitiin todeta, ettei kansallinen turvallisuus sovellu luottamuksellisen viestin salaisuuden rajoitusperusteeksi.

Asiasanat: tiedustelu, tietoliikennetiedustelu, kansallinen turvallisuus, suojelupoliisi, perusoikeudet, yksityiselämän suoja, luottamuksellisen viestin salaisuuden suoja.

Sisällysluettelo

Lähdeluettelo.....	iv
Lyhenteet.....	xiii
Johdanto.....	1
1.1 Tutkimuksen tausta.....	1
1.2 Aiempi tutkimus aiheesta.....	4
1.3 Tutkimusongelma ja tutkimuksen tavoitteet.....	6
2 Keskeiset käsitteet.....	8
2.1 Kansallinen turvallisuus.....	8
2.2 Tiedustelu.....	10
2.3 Vakoilu.....	15
2.4 Kybertoimintaympäristö.....	15
3 Tiedustelulakihankeen taustaa ja nykytila.....	18
3.1 Yleistä.....	18
3.2 Tiedustelutoiminta muuttuvassa turvallisuusympäristössä.....	21
3.3 Kansallisesta turvallisuudesta vastaavien viranomaisten lakisääteiset tehtävät.....	22
3.4 Suojelupoliisin ja puolustusvoimien tiedonhankinta kotimaassa.....	26
3.5 Suojelupoliisin ja puolustusvoimien ulkomaita koskeva tiedonhankinta.....	29
3.6 Kansainvälinen tiedusteluyhteistyö.....	30
4 Turvallisuuden takaaminen tiedustelun keinoin ja perusoikeuksien vaatimukset.....	35
4.1 Turvallisuus ja sitä uhkaavat tekijät muuttuvassa ympäristössä.....	35
4.2 Yksityiselämän suoja ja luottamuksellisen viestin salaisuuden suoja perustuslaissa.....	42
4.3 Perusoikeuksien yleiset rajoitusedellytykset.....	51
4.4 Kansainvälisten perus- ja ihmisoikeussopimusten vaatimukset.....	57
5 Tutkimusasetelma.....	61
5.1 Tutkimuskysymys.....	61
5.2 Aineisto ja tutkimusmetodi.....	61
5.2.1 Aineisto.....	61
5.2.2 Laadullinen tutkimus.....	63
5.2.3 Aineistolähtöinen sisällönanalyysi.....	64
6 Tiedonhankintalakityöryhmän mietintö.....	68
7 Mietinnöstä annettujen lausuntojen analyysi.....	72
7.1 Lausunnoissa esiin tulleet uhat.....	72
7.2 Lausunnoissa esiintyvät puoltavat argumentit.....	75
7.3 Lausunnoissa esiintyvät vastustavat argumentit.....	79
7.4 Lausunnoissa esiintyvät huomioon otettavat perus- ja ihmisoikeuskysymykset.....	83
7.4.1 Perusoikeuksien yleiset rajoitusedellytykset teemoina.....	85
8 Johtopäätökset.....	93

Lähdeluettelo

Kirjallisuus ja artikkelit

Aldrich, Richard J.: International intelligence cooperation in practice. Teoksessa International intelligence cooperation and accountability / edited by Hans Born, Ian Leigh, and Aidan Wills. London : Routledge, 2011. s.18 – 42.

Breakspear, Alan: A New Definition of Intelligence. Intelligence and National Security 2013. Vol. 28, No. 5, s. 678-693.

Daase, Christopher – Kessler, Oliver: Knowns and Unknowns in the ‘War on Terror’: Uncertainty and the Political Construction of Danger. Security Dialogue vol. 38, no. 4: s. 411–434, December 2007. <http://journals.sagepub.com/home/sdi> (luettu 30.11.2016)

Ervasti, Kaijus: Eräitä näkökohtia empiirisen tiedon hyväksikäyttämistä oikeustieteessä. Lakimies 3/1998 s. 364–388

Ervasti, Kaijus: Oikeussosiologia ja oikeuspoliittinen tutkimus osana oikeustiedettä. Oikeustiede – Jurisjurisprudencia 2011:XLIV s. 61 – 132.

Eräsaari, Risto: Kuinka turvaton on riittävän turvallinen? Kunnallisalan kehittämissäätiön Polemia-sarjan julkaisu nro 46. Vammala 2002.

Fägersten, Björn: Sharing secrets: explaining international intelligence cooperation. Department of Political Science, Lund University, 2010.

Hankilanoja, Arto: Poliisin salainen tiedonhankinta. Talentum. Helsinki 2014.

Hautamäki, Veli-Pekka: Perusoikeuden ydinalue argumenttina. Lakimies 1/2011 s. 82–98

Helminen, Klaus - Kuusimäki, Matti - Rantaeskola, Satu: Poliisilaki. Talentum 2012.

Hirvonen, Ari: Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki 2011.

Keinänen, Anssi – Väättänen, Ulla: Empiirinen oikeustutkimus – mitä ja milloin? Edilex 2015/7. Julkaistu Edilexissä 3.3.2015. www.edilex.fi/artikkelit/14917.

Koskela, Hille: Pelkokierre - pelon politiikka, turvamarkkinat ja kamppailu kaupunkitilasta. Gaudeamus. Helsinki 2009.

Kuosma, Tapio: Vakoilusta globaaliin urkintaan: demokratia vs. uusi fasismi. Nordbooks. Kemi 2015

Kurttila, Mikko: Mitä tiedustelusta kirjoitettiin? – Suojelupoliisi ja tiedonhankintalakityöryhmä mediassa 2013 -2015. Tampereen yliopisto 2015. Pro gradu –tutkielma.

Laitinen, Kari: Muuttuva turvallisuusympäristömme ja keskustelu turvallisuudesta. Kosmopolis 39 (2009) : 2, 4. artikkeli. <http://elektra.helsinki.fi/se/k/1236-1372/39/2/muuttuva.pdf> (luettu 2.2.2017).

Limnell, Jarno: Maailma ja Suomi 9/11 jälkeen. WSOY. Helsinki 2011.

Limnell, Jarno: Suomen uhkakuvapolitiikka 2000-luvun alussa. Maanpuolustuskorkeakoulu, strategian laitos. Helsinki 2009.

Lohse, Mikael: Rikostiedustelu terrorismin torjunnassa. Defensor Legis N:o 6/2005. s. 1187 – 1200.

Lohse, Mikael: Kybervakoilu. Defensor Legis 4/2015, s. 762 – 771.

Lonka, Harriet –Limnell, Jarno: Strategiasta käytäntöön: Suomi kyberlainsäädäntöä kehittämässä. Oikeus 2015 (44); 2: 202–213.

Lämsineva, Pekka: Perusoikeudet – nyt. Teoksessa Perusoikeuspuheenvuoroja, (toim.) Lämsineva, Pekka - Viljanen, Veli-Pekka. Turku 1998.

Metsäranta, Tuomas: Poliisin salaiset tiedonhankintakeinot ja yksityiselämän suoja. Turun yliopisto, oikeustieteellinen tiedekunta. Turku 2015.

Nieminen, Liisa (toim.): Perusoikeudet Suomessa. Yksityiselämän ja perhe-elämän suoja perusoikeutena, s. 107 – 147. Lakimiesliiton kustannus. Helsinki 1999.

Paara, Timo: Terrorismin torjuntaan perustuvan verkkovalvonnan suhde yksityiselämän suojaan. Pro gradu –tutkielma. Turun yliopisto, oikeustieteellinen tiedekunta 2015.

Kerola, Päivi: Oxfordin sanakirjojen toimitus: ”Totuudenjälkeinen” on vuoden sana Ylen uutiset. 16.11.2016. Yleisradio (luettu 25.6.2018).

Pakarinen, Auri: Tapaustutkimuksia lainvalmistelun kehittämisestä ja sääntelyn toimivuudesta. Itä-Suomen yliopisto. Joensuu 2012.

Paul, Jan-Peter: Tiedustelu 2000-luvulla. Tammi. Helsinki 2005.

Rentola, Kimmo: Tiedustelun historian ongelmia. Tieteessä Tapahtuu 7/2009.

Riialti, Jari: Laajenevan turvallisuuskäsityksen malli Sisäisen turvallisuuden ohjelmissa 2004 – 2012, Tampereen yliopisto, Johtamiskorkeakoulu, turvallisuushallinto. 2016.

Sun Tzu (Sunzi): Sodankäynnin taito. Suomentanut Heikki Karkkolainen. Suomennos perustuu englanninkieliseen käännökseen: The art of war / toimittanut ja englannintanut Samuel B. Griffith. Tietosanoma. Helsinki 1990.

Saraviita, Ilkka: Perustuslaki. Talentum. Helsinki 2011.

Sokala, Hannu: Supo haluaa tietää, kenelle puhut ja mitä kirjoitat. 18.2.2016. <https://yle.fi/aihe/artikkeli/2016/02/18/supo-haluaa-tietaa-kenelle-puhut-ja-mita-kirjoitat> (luettu 28.6.2018).

Tala, Jyrki: Lainsäädäntötutkimus – turhaa vai tarpeellista? Oikeus 2004/4: s.378–397.

Tala, Jyrki: Lakien laadinta ja vaikutukset. Helsinki 2005: Edita. (Tala 2005a).

Tala, Jyrki: Lainsäädäntötutkimus – tarpeellinen näkökulma oikeustieteessä. Defensor Legis 2005, s. 1321-1322. (Tala 2005b).

Tiilikainen, Teija - Helander, Petri – Heliskoski, Joni: Euroopan perustuslaki. Edita 2005.

Tuomi, Jouni - Sarajärvi, Anneli: Laadullinen tutkimus ja sisällönanalyysi. Tammi. Helsinki 2009.

Viljanen, Veli-Pekka: *Perusoikeuksien rajoitusedellytykset*. Vantaa 2001.

Viljanen, Veli-Pekka: Yksityiselämän suoja (PL 10 §). Teoksessa *Perusoikeudet*. Hallberg, Pekka – Karapuu, Heikki – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka. WSOYpro. Helsinki 2011, s.139 – 166 ja s. 389–411.

Virta, Sirpa: Turvallisuuden tutkimus. Tieteenalat ja monitieteisyyden lähtökohtia. Tiede ja ase. 2012. Saatavilla: <<http://journal.fi/ta/article/view/7470>>. (Lainattu: 1.2.2017).

Walkila, Sonya: Perusoikeuksien turvaaminen Euroopan unionissa – tasapainoilua tavoitteiden ja keinojen ristiaallokossa. Defensor Legis N:o 4/2015.

Virallislähteet

HE 309/1993 vp: Hallituksen esitys eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

HE 1/1998 vp: Hallituksen esitys eduskunnalle uudeksi Suomen hallitusmuodoksi.

HE 264/2006 vp: Hallituksen esitys Eduskunnalle puolustusvoimalaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 346/2014 vp: Hallituksen esitys eduskunnalle laiksi poliisin hallinnosta annetun lain muuttamisesta ja eräiksi siihen liittyviksi laeiksi.

Kansallinen turvallisuustutkimuksen strategia. Valtioneuvoston Sektoritutkimuksen neuvottelukunnan turvallisuusjaosto. Sektoritutkimuksen neuvottelukunnan julkaisuja 17:2009.

Lainkirjoittajan opas. Oikeusministeriö, lainvalmisteluosasto. Oikeusministeriön julkaisu 37/2013.

Luottamuksellisen viestin salaisuus, perustuslakisääntelyn tarkistaminen. Oikeusministeriön julkaisu 41/2016.

PeVM 25/1994 vp: Perustuslakivaliokunnan mietintö n:o 25 hallituksen esityksestä perustuslakien perusoikeussäännösten muuttamisesta

PeVL 32/2013 vp — HE 14/2013 vp: Perustuslakivaliokunnan lausunto. Hallituksen esitys eduskunnalle laeiksi esitutkintalain ja pakkokeinolain muuttamisesta sekä eräiksi niihin liittyviksi laeiksi

Siviilitiedustelulainsäädäntö. Siviilitiedustelulakityöryhmä. Sisäministeriön julkaisu 8/2017

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

Suojelupoliisin ohjesääntö 1.1.2014. Dnro 489/2013

Suojelupoliisin vuosikirja 2015.

Suomen kansallinen riskiarvio 2015: Sisäministeriön julkaisu 3/2016.

Suomen kyberturvallisuusstrategia: Valtioneuvoston periaatepäätös 24.1.2013. Sisältää Turvallisuuskomitean taustamuistion Suomen kyberturvallisuusstrategiasta.

Tiedonhankintalakityöryhmän mietintö: Suomalaisen tiedustelulainsäädännön suuntaviivoja, Puolustusministeriö 13.12.2013.

Yhteiskunnan turvallisuusstrategia. Valtioneuvoston periaatepäätös 16.12.2010 (YTS 2010)

Oikeustapaukset

EU-tuomioistuim

Unionin tuomioistuimen tuomio (suuri jaosto) 8.4.2014: yhdistetyt asiat C-293/12 ja C-594/12. Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym. ECLI:EU:C:2014:238

Lausunnot

Tomi Voutilainen 16.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/238133_Voutilainen.pdf

Valtiovarainministeriö 15.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/238038_vm_lausunto.pdf

Suomen Asianajajaliitto 15.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/238057_asianajajaliitto_lausunto.docx

Keskuskauppakamari 15.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/238058_Keskuskauppakamarin_lausunto.pdf

Puolustusministeriö 13.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237992_PLM_PO_lausunto_tyoryhman_mietinnosta_130415.pdf

Keskusrikospoliisi 13.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237996_kpr_lausunto.docx

FiCOM ry 10.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237927_FiCom_Lausunto_Tiedustelulainsäädäntö-tr_mietinnöstä_v1-0F_20150410.pdf

IAMCP Finland 10.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237937_IAMCP_lausunto.pdf

Piraattipuolue r.p. 10.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237938_piraattipuolue.pdf

Huoltovarmuuskeskus 10.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237942_Tiedustelulainsäädäntö_Huoltovarmuuskeskus.docx

Suomen Puolustus- ja Ilmailuteollisuusyhdistys PIA ry 10.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237969_PIA_lausunto_tiedonhankintalakitr.docx

Poliisiammattikorkeakoulu 10.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237970_Poliisi_Suomalaisen_tiedustelulainsäädännön_suuntaviivoja.pdf

Microsoft Oy 09.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237848_Microsoft_4633928.pdf

Juha Lavapuro 09.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237977_Juha_Lavapuro_.docx

Valtioneuvoston kanslia 09.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/238006_Valtioneuvoston_kanslian_lausunto_puolustusministeriön_työry.pdf

Puolustusministeriö 08.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237786_turvallisuuskomitean_lausunto.pdf

Puolustusministeriö 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237743_HO_lausunto_tiedustelulainsäädäntö.pdf

Rajavartiolaitoksen esikunta 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237744_Rajavartiolaitoksen_lausunto.pdf

Palkansaajajärjestö Pardia ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237745_Pardian_lausunto_Tiedustelumuistio.doc

Tieto Finland Oy 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237746_Tieto_oyj_lausunto_1139299.pdf

SSH Communications Security 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237747_SSH_Lausunto_Tiedustelulainsäädännöstä_2015_FINAL.doc

Nokia Oyj 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237748_Nokia_LausuntoHuhti72015.pdf

TIVIA Tieto- ja viestintätekniiikan ammattilaiset 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237749_TIVIA_7.4.2015.docx

BaseN Oy 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237750_BaseN_Lausunto_PLM_07042015.pdf

Elinkeinoelämän keskusliitto EK 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237751_EKn_lausunto_tiedonhankintalakityöryhmän_mietinnöstä_PM.pdf

Poliisihallitus 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237752_Poliisihallituksen_lausunto_tiedonhankintalakityöryhmän_mietinnöstä.pdf

Suomen Sadankomitea ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237754_Sadankomitean_lausunto.rtf

Suomen Kristillisdemokraatit rp 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237759_kristilliset.docx

Suojelupoliisi 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237761_Suojelupoliisin_lausunto_2.4.2015.pdf

Viestinnän keskusliitto ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237763_viestinnän_keskusliitto_150407Tietoliikennetiedustelu.pdf

Ohjelmistoyrittäjät ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237764_Ohjelmistoyrittäjät_ry_lausunto_tiedonhankintalaki_Puolustusministeriö_.pdf

FISC ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237765_FISCTiedonhankintalakiryhmän_mietintö_lausunto_FISC06042015_final.pdf

Tulli

[http://www.hare.vn.fi/upload/asiakirjat/19825/237766_Tullin_LAUSUNTO_-_Suomalaisen_tiedustelulainsäädännön_suuntaviivoja_\(FINAL_7.4.15\).pdf](http://www.hare.vn.fi/upload/asiakirjat/19825/237766_Tullin_LAUSUNTO_-_Suomalaisen_tiedustelulainsäädännön_suuntaviivoja_(FINAL_7.4.15).pdf)

Fujitsu Finland Oy

http://www.hare.vn.fi/upload/asiakirjat/19825/237767_Fujitsu_.docx

Tieteen tietotekniikan Keskus Oy (CSC) 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237768_CSC_lausunto_Tiedonhankintalakityöryhmän_mietintöön.docx

Valtakunnansyyttäjänvirasto 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237771_syyttajan_virastolausunto_7.4.15_20150407155711.pdf

Ficix ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237772_FICIX-lausunto-tiedustelum.docx

Suomen Journalistiliitto ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237773_journalistiliitto_1138_001.pdf

Amcham Finland 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237774_Amcham_Finlandin_lausunto.docx

IKI ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237775_Iki_lausunto_tiedustelulainsaadannon_suuntaviivoista_2015-04-07.pdf

Ohjelmistoyrittäjät ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237776_ohjelmistoyrittajat_ry_2448677.pdf

Tietosuojavaltuutetun toimisto 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237777_tietosuojavaltuutetun_lausunto_verkkovalvonta_20150407173931.pdf

Puolustusvoimien Diplomi-insinöörit r.y. 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237778_PVDI_lausunto.docx

Electronic Frontier Finland ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237779_Effi-ry-lausunto-tlt-mietinnosta.pdf

DNA Oy 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237780_DNA_lausunto_070415.pdf

Prof-Tel Oy 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237781_Proftel_PLM_07-04-2015-lausunto.pdf

Suomen Rauhanturvaajaliitto ry 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237782_rauhanturvaajaliitto_3681199.pdf

Maa- ja metsätalousministeriö 07.04.2015

http://www.hare.vn.fi/upload/asiakirjat/19825/237783_mmm_Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf

Eduskunnan oikeusasiamiehen kanslia

http://www.hare.vn.fi/upload/asiakirjat/19825/237784_eduskunnan_oikeusasiamies_lausunto729.pdf

Martin Scheinin

http://www.hare.vn.fi/upload/asiakirjat/19825/237740_Martin_S_lausunto.docx

Nixu Oyj

http://www.hare.vn.fi/upload/asiakirjat/19825/237741_Nixun_lausunto_tiedustelulainsäädäntöön_Huhtikuu2015.docx

Puolustusministeriö

http://www.hare.vn.fi/upload/asiakirjat/19825/237733_Viestintäyksikön_vastas_lausuntopyyntöön_tiedonhankintakityöryhmän_mietinnöstä.pdf

Finnnet-liitto ry

http://www.hare.vn.fi/upload/asiakirjat/19825/237734_Lausunto_Finnet_Tiedustelulainsuuntaviivoja.doc

Sosiaali- ja terveystieteiden ministeriö

http://www.hare.vn.fi/upload/asiakirjat/19825/237735_STM_lausunto_PLM_n_lausuntopyyntöön_koskien_tiedonhankintala.pdf

Liikenne- ja viestintäministeriö

http://www.hare.vn.fi/upload/asiakirjat/19825/237736_Liikenne_ja_viestintäministeriön_lausunto.pdf

Patria Oyj

http://www.hare.vn.fi/upload/asiakirjat/19825/237737_Patria_lausunto_Suomalaisen_tiedustelulainsaadannon_suuntaviivoja_020415.pdf

Pääesikunta

http://www.hare.vn.fi/upload/asiakirjat/19825/237738_PE_lausunto_AL6271_V1.docx

Maanpuolustuksen Insinöörit MPI ry

http://www.hare.vn.fi/upload/asiakirjat/19825/237727_MPi_lausunto.doc

Ruotsalainen Kansanpuolue

http://www.hare.vn.fi/upload/asiakirjat/19825/237730_RKP_DEFMIN_riktlinjer_för_underrättelse_agstiftning_mars_2015.doc

Suomen Erillisverkot Oy

http://www.hare.vn.fi/upload/asiakirjat/19825/237731_Suomen_Erillisverkkojen_lausunto_tiedonhankintakityöryhmän_mietintöön.pdf

Opetus- ja kulttuuriministeriö

http://www.hare.vn.fi/upload/asiakirjat/19825/237732_OKM_lausunto_-_Tiedonhankintakityöryhmän_mietintö.pdf

Viestintävirasto

http://www.hare.vn.fi/upload/asiakirjat/19825/237723_Viestintäviraston_lausunto_Puolustusministeriölle_tiedonhankintakityöryhmän_mietinnöstä.pdf

Valtioneuvoston oikeuskansleri

http://www.hare.vn.fi/upload/asiakirjat/19825/237724_OKV_9_20_2015_Lausunto.doc

Sisäministeriö

http://www.hare.vn.fi/upload/asiakirjat/19825/237725_SM_lausunto.docx

Vihreä Liitto rp.

http://www.hare.vn.fi/upload/asiakirjat/19825/237726_Vihreät_Tiedustelulainsaadanto2015.doc

Suomen Keskusta rp.

http://www.hare.vn.fi/upload/asiakirjat/19825/237722_Keskusta_tiedustelulainsaadännön_suuntaviivoja.doc

Oikeusministeriö

http://www.hare.vn.fi/upload/asiakirjat/19825/238000_om_17_43_2015_20150414135207.pdf

Suomen Sosialidemokraattinen Puolue

http://www.hare.vn.fi/upload/asiakirjat/19825/237721_SDP_lausunto_tiedonhankintatr_mietintöön_valmis.docx

Maanpuolustuskoulutusyhdistys

http://www.hare.vn.fi/upload/asiakirjat/19825/237720_MPK_lausunto_tiedonhankintalakityöryhmän_mietinnöstä.docx

Vasemmistoliitto rp

http://www.hare.vn.fi/upload/asiakirjat/19825/237719_VAS_lausunto_tiedonhankintalakityöryhmän_mietinnöstä.doc

TeliaSonera Finland Oyj

http://www.hare.vn.fi/upload/asiakirjat/19825/237717_Soneran_lausunto_julkinen.pdf

Cinia Group Oy

http://www.hare.vn.fi/upload/asiakirjat/19825/237718_Cinian_lausunto_tiedonhankintalakityöryhmän_mietinnöstä.pdf

Finnvera

http://www.hare.vn.fi/upload/asiakirjat/19825/237715_Finnveran_lausuntodocx.docx

Lyhenteet

CIA	Central Intelligence Agency (Yhdysvaltain keskustiedustelupalvelu)
EIS	Euroopan ihmisoikeussopimus; Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi
EIT	Euroopan ihmisoikeustuomioistuin
ETL	Esitutkintalaki (22.7.2011/2011,voimassa 1.1.2014 alkaen)
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
EY	Euroopan yhteisöt
FSB	Venäjän federaation turvallisuuspalvelu (Federalnaja služba bezopasnosti)
HE	hallituksen esitys
KP-sopimus	YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus
LVM	liikenne- ja viestintäministeriö
NSA	National Security Agency (Kansallinen turvallisuusvirasto)
PeVL	perustuslakivaliokunnan lausunto
PeVM	perustuslakivaliokunnan mietintö
PKL	pakkokeinolaki (22.7.2011/806, voimassa 1.1.2014 alkaen)
PL	Suomen perustuslaki (11.6.1999/731)
PoliisiL	poliisilaki (22.7.2011/872, voimassa 1.1.2014 alkaen)
SopS	Suomen säädöskokoelman sopimussarjassa
SUPO	suojelupoliisi
TeletointaL	Teletointalaki
vp	valtiopäivät
YK	Yhdistyneet kansakunnat

Johdanto

1.1 Tutkimuksen tausta

“The Unknown

As we know,
There are known knowns.
There are things we know we know.
We also know
There are known unknowns.
That is to say
We know there are some things
We do not know.
But there are also unknown unknowns,
The ones we don't know
We don't know.”¹

Kuka ikinä käännsikin Yhdysvaltain puolustusministeri Rumsfeld’in lauseet helmikuussa 2002 pidetystä lehdistötilaisuudesta runoksi, onnistui hän kiteyttämään ulko- ja turvallisuuspolitiikan tämän päivän keskeisen ongelman – epävarmuuden. Rumsfeld’in mukaan on olemassa kolme tilaa koskien tietoa ja sen puutetta. Ensinnäkin on olemassa *varmaa tietoa* (‘known knowns’), jonka perusteella poliittisia ohjelmia ja sotilasstrategioita voidaan synnyttää ja kehitellä. Toiseksi olemassa on jotain tai jonkinlaista tietoa, siitä *mitä emme tiedä* (‘known unknowns’) – epävarmuustekijöitä - jotka voidaan kesyttää analyttisesti ja integroida uudelleen päätöksentekoprosessiin laskennallisina riskeinä. Kolmanneksi on olemassa tietoa, jota *emme tiedä ja jota emme voikaan tietää* (‘unknown unknowns’) - arvaamaton villikortti - joka voi kaataa kaikkein huolellisimmankin suunnitelman. Lehdistötilaisuudessaan Rumsfeld jätti kertomatta tiedon tai sen puutteen neljännen kategorian: tiedon, jota *emme halua tietää*. Nämä ovat asioita, jotka me voisimme tietää, mutta mieluummin päätämme olla niitä tietämättä esimerkiksi unohtamalla, vaimentamalla tai torjumalla.²

Edellä oleva osoittaa oikean ja varman tiedon tarpeellisuuden ja välttämättömyyden, jotta voidaan tehdä kelvollisia ja ennustettavia ratkaisuja tulevaisuuteen. Toisaalta tiedon neljäs kategoria paljastaa

¹Puolustusministeri Donald Rumsfeld’in vastaus puhuessaan USA:n puolustusministeriön lehdistötilaisuudessa 12.2.2002; julkaistu uudelleen muotoiltuna runona (Seely 2003:2). Lähde: Daase – Oliver 2007, s. 411.

² Daase – Oliver 2007, s. 412.

myös päätöksentekoon liittyvät mahdollisuudet käytettävissä olevan tiedon ja tietämättömyyden tarkoitukselliseen väärinkäyttöön nykyisessä ”totuudenjälkeisessä ajassa”³.

Suomen kansallisen turvallisuuden esille nouseminen turvallisuuspoliittisessa keskustelussa, on ainakin osaksi johtunut Suomen turvallisuusympäristössä tapahtuneista muutoksista niin globaalisti kuin lähialueilla. Tässä tutkimuksessa tarkastellaan Suomen kansalliselle turvallisuuden kannalta merkityksellisiä uusia uhkakuvia muuttuneessa turvallisuusympäristössä sekä tiedustelulakihanketta, jonka keinoin pyritään turvaamaan kansallista turvallisuutta tulevaisuudessa. Mielenkiintoni tutkimusaiheeseen heräsi Suomessa talvella 2016 - 2017 käydyin turvallisuuskeskustelun kautta, mikä johti minut tiedustelulakihankkeen jäljille. Kansallisesta turvallisuudesta vastaavien viranomaisten suorittaman tiedustelutoiminnan salliminen lailla on merkittävässä roolissa käynnissä olevassa turvallisuuskeskustelussa. Suomi on yksi Euroopan harvoista maista, joissa ei ole lakia tiedustelutoiminnasta. Niin kansalaisten kuin yhteiskunnan kannalta olisi nähdäkseeni tärkeää, että nykyiset asetustasoiset tiedustelutoiminnan mahdollistavat valtuudet, ohjeet ja niihin liittyvä muu lainsäädäntö koottaisiin yhteen yhdeksi tai useammaksi siviili- ja sotilastiedustelua koskeviksi laeiksi. Tämä selventäisi sekä kansalaisille että tiedustelutoimintaa harjoittaville viranomaisille ensinnäkin sen, minkälaisia toimia kansalaisiin voidaan kohdentaa, ja toisekseen sen, minkälaisia tiedustelutoimia ja millä perusteilla viranomainen voi suorittaa ja kehen se voi niitä kohdistaa.

Tiedustelulakihankkeesta käytävä keskustelu on ollut hyvin esillä tiedotusvälineissä, muun muassa valtakunnallisten sanomalehtien pääkirjoituksissa ja artikkeleissa sekä YLE:n ja MTV3:n ajankohtaisohjelmissä. Tiedotusvälineet ovat tuoneet ansiokkaasti tiedustelulakihankeeseen kansalaisten tietoisuuteen. Tätä kautta lakihanke on noussut myös kansalaisten huulille osaksi kansalaiskeskustelua. Varsinkin kansalaiskeskustelussa, ja miksei myös osassa toimittajienkin ulostuloista, tiedustelutoiminnan ymmärretään olevan pääasiassa vain viranomaisten suorittamaa kaiken kattavaa, internetissä ja muissa tietoverkoissa tapahtuvan viestiliikenteen seuraamista eri menetelmin ja kokonaisvaltaisesti (massavalvontaa). Tutuiksi ovat varmasti tulleet varsinkin termit verkkourkinta, verkkotiedustelu ja massavalvonta, sekä pääasiassa yleensä kolmekirjaimiset erilaiset yhdistelmät kuten CIA, FSB ja NSA. Lisäksi tutuksi on tullut ainakin yksi oikea henkilö, yhdysvaltalainen, USA:n tiedusteluelimille työskennellyt ”tietovuotaja” Edward Snowden.

³ Kerola 2016. Totuudenjälkeinen aika viittaa olosuhteisiin, joissa objektiiviset faktat vaikuttavat yleiseen mielipiteeseen vähemmän kuin tunteisiin ja henkilökohtaisiin vakaumuksiin vetoaminen.

Aiheen ympärillä käytävä mediakeskustelu on myös liittynyt kyberturvallisuuteen ja hybridisodankäyntiin, sekä Euroopan viimeisimpiin terrori-iskuihin Brysselissä 22.3.2016 ja Pariisissa 13.11.2015. Aihetta on käsitelty mm. YLE:n ajankohtaisohjelmissa ohjelmaotsikoilla:

- *”Pakolaisvirta, maakaupat, informaatio­sota. Millä keinoin Venäjä painostaa Suomea?”*
- *”Turvallisuusilmapiiri kiristynyt.”*
- *”Poliisi ja armeija haluavat Suomessakin päästä seuraamaan, mitä kansalaiset tekevät verkossa.”*

Lakihanketta koskeva keskustelu ja siihen kohdistuva kritiikki on pääasiassa koskenut lain mahdollistavaa verkkotiedustelua, jonka nähdään uhkaavan kansalaisten perustuslaillisia oikeuksia. Pääasiassa sen katsotaan uhkaavan yksityisyyden suojaa ja luottamuksellisen viestin salaisuuden suojaa. Lakihankkeesta käytävän keskustelun keskittyessä lakihankkeen perustuslaillisiin ongelmiin, pyrin tutkimuksessani selvittämään varsinaisten tutkimuskysymysten lisäksi, mitä tiedustelulla tiedustelulakihankkeen kontekstissa tarkoitetaan ja minkälaisia tiedustelutoiminnan muotoja lakihankkeella mahdollistettaisiin.

Suomessa yhteiskunnan turvallisuudesta huolehtivat viranomaiset harjoittavat niille laissa määrättyjen tehtäviensä hoitamiseksi vaadittavaa tiedustelua. Tutkimuksen aihepiiri on mielestäni tärkeä, koska turvallisuusviranomaisille ei ole kuitenkaan säädetty toimivaltuuksia harjoittaa tehtäviensä edellyttämää tiedustelua. Nykytilanteessa turvallisuusviranomaisten tiedonhankinta perustuu pääosin rikostorjuntatoimivaltuuksiin ja kaikkien saatavilla oleviin avoimiin lähteisiin sekä kansainvälisellä tiedusteluyhteistyöllä saataviin tietoihin.⁴ Koska tiedustelutoiminta on jäänyt akateemisessa tutkimuksessa vähälle huomiolle, teen luvussa kolme selkoa myös tiedustelulakihankkeen taustoista ja sen nykytilasta. Tästä syystä taustojen selvittäminen on mielestäni oleellista varsinaisen tutkimusongelman kannalta.

Koska Suomessa turvallisuusviranomaiset kuitenkin harjoittavat tiedustelutoimintaa määrättyjen ohjeiden rajoissa, ongelmalliseksi tilanne on silti nähtävä, koska meillä ole sääösperustaa sille, mitkä ovat tiedustelutoiminnan tavoitteet ja pyrkimykset eikä siitä minkälaisilla tiedustelutoimilla näihin tavoitteisiin olisi luvallista päästä. Valmisteilla olevat lakiesitykset siviili- ja sotilastiedustelusta selkeyttäisivät turvallisuusviranomaisten toimivaltuuksia ja tehtävän jakoa tiedonhankinnan saralla.

⁴ Sisäministeriön julkaisu 8/2017, s. 19

Tiedonhankintalakityöryhmän näkemyksen mukaan ”*turvallisuusviranomaisten tiedonhankinta-toimivaltuudet ovat puutteellisia toiminnan yhteiskunnalliseen merkittävyyteen nähden sekä muihin maihin verrattuna*”. Lisäksi työryhmä pitää tilannetta epätydyttävänä, ”*kun otetaan huomioon, että Suomen kansainvälisessä turvallisuustoimintaympäristössä on viime vuosina tapahtunut merkittäviä muutoksia*”.⁵

1.2 Aiempi tutkimus aiheesta

Tiedustelua on tutkittu ja siitä on kirjoitettu melko kattavasti eri maiden tiedustelun ja sen historian osalta. Yleisteoksia tiedusteluorganisaatioista ja niiden historiasta löytyy melko paljon. Suomen sotilastiedustelusta ja suojelupoliisin toiminnasta ja historiasta on kirjoitettu muutamia tieto- ja historiikkikirjoja. Näistä esimerkkeinä; *Matti Simolan* ”Ratakatu 12 : Suojelupoliisi 1949-2009” ja *Tim Weinerin* (suom. Mika Tiirinen) ”CIA: Yhdysvaltain keskustiedustelupalvelun historia”. Sekä ulkomaisissa että kotimaisissa teoksissa keskitytään pääasiassa tiedustelun ja kansainvälisen politiikan välisiin suhteisiin Kylmän sodan aikana, jolloin vastakkain olivat lähinnä Yhdysvaltojen ja Neuvostoliiton intressit eripuolilla maailmaa.

Turvallisuus- ja tiedustelualan tutkimus on Rentolan mukaan noussut vasta muutaman viime vuosikymmenen kuluessa varteenotettavaksi tutkimuskohteeksi, ja joka on vähitellen hyväksytty käyvän tieteenharjoittamisen piiriin.⁶ Akateemista tutkimusta tiedustelusta on tähän mennessä Suomessa tehtykin melko vähän, eikä aihepiiriä sen käsitteistöineen ole toistaiseksi kovinkaan selkeästi ymmärretty. Kurttila toteaaakin pro gradu -tutkielmansa johtopäätöksissään, että suomalainen ymmärrys koskien tiedustelua, tiedusteluvaltuuksia ja käynnissä olevaa tiedustelulakihanketta kohtaan on vasta syntymässä. Aidoksi ymmärrykseksi tiedustelun on mahdollista nousta vasta kun sen aihepiiri käsitteistöineen ja tiedustelutoiminnan tarpeiden ymmärtäminen ovat kohtuullisella tasolla eri osapuolten välillä.⁷ Tämä opinnäytetyö pyrkii vastaamaan osaltaan aiheesta tehdyn tutkimuksen vähäisyyden haasteeseen.

Aiempi tutkimus:

Mikko Kurttila: Mitä tiedustelusta kirjoitettiin? – Suojelupoliisi ja tiedonhankintalakityöryhmä mediassa 2013 -2015 (Pro gradu –tutkielma 2015, Tampereen yliopisto, hallintotiede turvallisuushallinnon maisteriohjelma).

⁵ Tiedonhankintalakityöryhmän mietintö 2015, s. 14.

⁶ Rentola 2009, s. 1.

⁷ Kurttila 2015, s. 71.

Kurttilan tutkimuksen kohteena oli tiedonhankintalakiyöryhmän mietintöön ja suojelupoliisin tiedustelutoimivaltuuksien lisäämistä koskeva julkinen kirjoittelu. Hänen tavoitteena oli muun muassa selvittää tiedustelutoimivaltuuksiin liittyvästä julkisesta kirjoittelusta esiin nousevia aiheita puoltavia näkökulmia ja toisaalta sitä vastustavia argumentteja.⁸ Hänelle syntyi tutkimuksessaan käyttämän aineiston perusteella sellainen vaikutelma, ettei julkista keskustelua käyneillä osapuolilla ole kovinkaan selkeää kuvaa tiedustelusta. Vaikka Kurttilan mielestä tiedustelu aiheena näyttäytyi osapuolille hankalasti hahmotettavana, siitä huolimatta oli aiheesta julkista keskustelua käyneillä vahva näkemys tai käsitys tiedustelutoiminnasta.⁹

Timo Paara: Terrorismin torjuntaan perustuvan verkkovalvonnan suhde yksityiselämän suojaan. (Pro gradu –tutkielma 2015, Turun yliopisto, valtiosääntöoikeus).

Paara keskittyy tutkimuksessaan tarkastelemaan niitä vaikutuksia, joita tiedonhankintalakiyöryhmän esittämällä verkkoliikenteen massavalvonnalla olisi yksityiselämän ja viestinnän luottamuksellisuuden suojaan. Arvioinnin kohteena ovat hänen tutkimuksessaan PL:n yksityiselämän ja viestinnän luottamuksellisuuden suojaan turvaavan 10 §:n, EU:n perusoikeuskirjan ja EIS:n sekä YK:n KP-sopimuksen yksityiselämän suojaan koskevat artiklat. Paaran mukaan selkein perustuslaillinen konfliktitilanne kaavaillun verkkovalvonnan osalta on se, ettei kansallista turvallisuutta mainita perustuslain 10 §:n 3 momentissa viestinnän luottamuksellisuuden suojan rajoitusperusteena.¹⁰

Tiedustelulakihanketta perustellaan mm. terrorismirikosten torjunnalla, tähän aiheeseen liittyvää tutkimusta on tehnyt esimerkiksi Mikael Lohse 2005 valmistuneessa lisensiaattitutkimuksessaan, jonka aiheena oli ”Rikostiedustelu terrorismin torjunnassa: tutkimus tiedustelusta osana terrorismirikosten preventiota ja tiedustelutoimien aloittamista koskevasta päätöksenteosta”. Lohselta on valmistunut 2012 myös terrorismiin liittyvä väitöskirja nimeltään ”Terrorismirikoksen valmistelu ja edistäminen”.

Pääasiallisena uhkana Suomenkin kansalliselle turvallisuudelle nähdään usein ainakin yleisessä keskustelussa ja turvallisuusviranomaisten julkaisemissa uhka-arvioissa kansainvälinen terrorismi. Terrorismiuhkaan liittyen Lohse toteaa lisensiaattitutkimukseensa perustuvassa artikkelissaan, että

⁸ Ibid, s. 8.

⁹ Kurttila 2015, s. 71.

¹⁰ Paara 2015, tiivistelmä.

tämän hetkiset viranomaisten tiedusteluvaltuudet normaalioloissa eivät mahdollista terrorismin torjumista rikos- eivätkä sotilastiedustelulla. Tiedonhankintapäätöksen kytkeminen rikosepäilyyn lykkää käytännössä tiedustelun aloittamishetken siihen, kunnes perustellusti oletettavat syyt henkilön syyllistymisestä terroririkokseen ovat täyttyneet. Lohsen näkemykseen mukaan kansallisen turvallisuuden tunnustava tiedusteluperuste on siksi saatava poliisilakiin tai muuhun säädökseen säännönmukaiseksi toimivaltaperusteeksi, jotta akuuttiin terroriuhkaan voidaan puuttua ennakolta.¹¹

Maanpuolustuskorkeakoulun julkaisuista löysin useita otsikoiltaan mielenkiintoisia ja hyvin tuoreita suoraan tiedusteluun liittyviä opinnäytetöitä, jotka on valitettavasti osoitettu vain viranomaiskäyttöön (suojaustaso IV).¹² Onneksi muutamia tiedustelutoimintaan liittyviä opinnäytteitä on myös julkisesti saatavilla. Vaikka ne käsittelevätkin kyber- ja informaationsodankäyntiä sekä kyberuhkia, on niissä käsitelty myös kyberympäristössä tapahtuvaa tiedustelua ja sen torjuntaa, sekä tiedustelua sotilastiedustelun näkökulmasta yleisesti. Näin ollen ne toimivat osaltaan hyvin lähteenä taustoittaessa tutkielman teoreettista viitekehystä.

1.3 Tutkimusongelma ja tutkimuksen tavoitteet

Tutkimuksen tarkoituksena on selvittää, minkälaisilla uhkakuvilla tai muilla perusteilla tiedustelulakihanketta Suomeen vaaditaan: minkälaisia argumentteja lainvalmistelussa mukana olevat osapuolet esittävät niistä toimivaltuuksista ja keinoista, joilla tiedustelua olisi tarkoitus harjoittaa? Lisäksi pyrkimyksenä on saada selville mitkä perus- ja ihmisoikeudet ja miten niitä vaaditaan huomioonotettavaksi säädösprosessin valmisteluvaiheessa. Tutkimusongelma jakaantuu kolmeen alakysymykseen:

1. Mitkä ovat pääasialliset uhat, joita tiedustelulla pyritään torjumaan?
2. Minkälaisin argumentein tiedustelulakihanketta puolletaan tai vastustetaan? Minkälaisin reunaehdoin tietoliikennetiedustelu voitaisiin hyväksyä?
3. Mitä perus- ja ihmisoikeuskysymyksiä esitetään mietinnössä ja lausunnoissa sekä miten niitä vaaditaan huomioonotettavaksi lakihankkeessa?

¹¹ Lohse 2005, s. 1200.

¹² Erkkilä, Jyrki (2013): Informaation luotettavuuden arviointi avoimien lähteiden tiedustelussa.

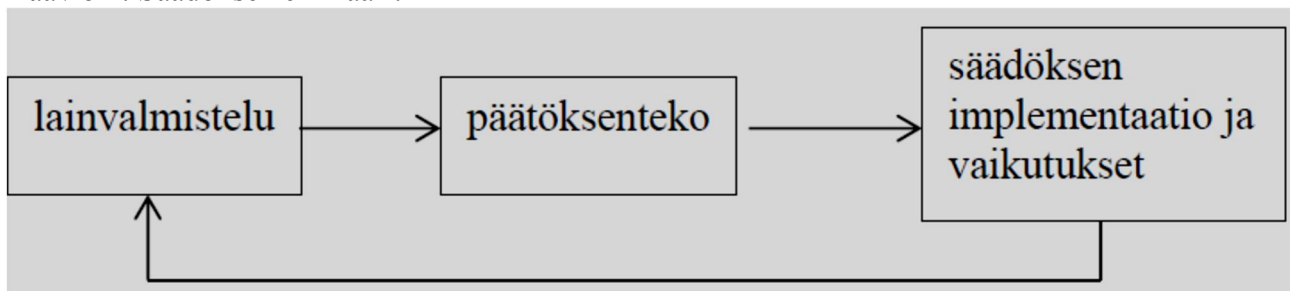
Toppinen, Mika (2015): Ei-puolustusellisten kybersuorituskykyjen käyttömahdollisuudet pienen valtion näkökulmasta.

Kylä-Harakka, Jani (2015): Kansallinen tiedustelu kriisinhallintaoperaatioissa 2030.

Ala-Nikula, Matti (2015): Venäjän tiedustelu- ja turvallisuuspalveluiden ulkomailla harjoittama poliittinen tiedustelu.

Koska tämä tutkimus on nimensä mukaisesti lainsäädäntötutkimus, on syytä hieman avata mistä siinä on kyse. Lainsäädäntötutkimus jäsentyy kohteen perusteella karkeasti kahteen pääalueeseen: a) lainsäädäntöä kokonaisuutena, instituutiona, koskevaan tutkimukseen ja b) yksittäisiin laki- tai säädöshankkeisiin kohdistuvaan tutkimukseen. Yksittäistä laki- ja säädöshanketta koskien lainsäädäntötutkimuksen huomio ja tutkimusintressi voidaan kiteyttää pyrkimykseen vastata ennen muuta seuraaviin kysymyksiin: miksi ja miten säädökset syntyvät sekä miten säädökset toteutuvat ja vaikuttavat. Tätä tutkimusintressiä havainnollistaa seuraava kaavio säädöshankkeen elinkaaresta.¹³

Kaavio 1. Sädöksen elinkaari.



Tämä tutkimus keskittyy edellä olevan kuvion ensimmäiseen osaan – lainvalmisteluun ja tarkemmin sanoen lausunto- ja kuulemisvaiheeseen – ja sen syntymisen taustalla olevien tarpeiden selvittämiseen eli vastausta haetaan kysymällä miksi ja miten tiedustelulait halutaan osaksi Suomen lainsäädäntöä. Näiden lakien toteutumisen ja vaikutuksien arviointi jää myöhempien tutkimusten tehtäväksi.

Vaikka lainsäädäntötutkimuksessa nykyään hyvin usein keskitytään arvioimaan lainvalmistelun laatua, ei siihen ole syytä tässä tutkimuksen mennä kahdestakin syystä. Ensinnäkin tiedustelulakien valmistelu on vasta niin alkuvaiheessa, ettei hallituksen esitystä ole vielä annettu ja toiseksi, lainvalmistelun laadun arviointi ei edes palvelisi tutkimuskysymyksiini vastaamista.

Tiedonhankintalakityöryhmä korostaa mietinnön luovutuskirjeessään Puolustusministeriölle, että turvallisuusviranomaisten tiedonhankintakyvyn parantamisella tavoitellaan pääasiallisesti viranomaisten mahdollisuuksia parantaa niiden kykyä torjua vakavia kansallista turvallisuutta uhkaavia tekoja, eikä niinkään parantaa tietoturva.¹⁴ Tämän vuoksi olen rajannut tutkimuksesta pois kaiken sellaisen, joka koskee tietoturvaauhkien torjuntaa. Myöskään tietoverkkorikollisuutta ei käsitellä tässä tutkimuksessa. Tietoturvaauhkat ovat kuitenkin mukana tutkimuksessa siltä osin kun

¹³ Tala 2004, s. 379.

¹⁴ Tiedonhankintalakityöryhmän mietintö 2015, s. 9.

lausunnoista on poimittu niissä mainittuja uhkia. Sellaiset argumentit, joissa on vaadittu huomioonotettavaksi elinkeinoelämään kohdistuvia vaikutuksia, tiedustelutoiminnan lupamenettelyyn ja valvontaan liittyviä vaatimuksia, ovat myös rajattu tutkimuksen ulkopuolelle.

Mietinnössä työryhmä on selvittänyt millaista lainsäädäntöä on voimassa verrokkimaissa Ruotsissa, Norjassa, Tanskassa, Alankomaissa ja Saksassa koskien tiedustelua, jolla pyritään torjumaan kansalliseen turvallisuuteen kohdistuvia uhkia ja tietoverkkoympäristössä tapahtuvasta tiedustelusta. Tässä tutkimuksessa jätän kansainvälisen vertailun tutkimuksen ulkopuolelle, koska sillä ei ole merkitystä tutkimuskysymyksieni kannalta.

Tutkimuksessa keskitytään pääasiassa peruslaillisiin kysymyksiin suhteessa tietoliikenne-tiedusteluun, joka on saanut eniten tilaa niin lausunnon kohteena olevassa mietinnössä kuin siihen annetuissa lausunnoissa ja julkisessa keskustelussa. Näillä rajauksilla olen pyrkinyt löytämään mielekkään ja selkeästi rajatun ongelmanasettelun, jotta pystyisin vastaamaan tutkimuskysymyksiini.

2 Keskeiset käsitteet

Tämän tutkimuksen viitekehyksen ymmärtämiseksi, on välttämätöntä esittää turvallisuuteen ja tiedusteluun olennaisesti tutkimukseen liittyvät käsitteet, mitä tiedustelulla tarkoitetaan ja miten se tässä tutkimuksessa ymmärretään sekä esittelemällä tiedustelutoimintojen organisoimista.

2.1 Kansallinen turvallisuus

Suomessa ei ole tehty varsinaista kansallisen turvallisuuden määrittelyä säädösten tasolla, eikä sitä ole määritelty millään hallinnonalalla muutenkaan. Tiedonhankintalaki työryhmän mietinnössä ei suoraan määritellä kansallista turvallisuutta, kuten ei myöskään valtioneuvoston periaatepäätöksessä yhteiskunnan turvallisuusstrategiasta 16.12.2010. Mietinnössä puhutaan kansallisesta turvallisuudesta 2.2. luvussa, jonka otsikkona on Kansallinen turvallisuusympäristö.

Perinteisesti määriteltynä kansallinen turvallisuus ymmärretään yhteiskunnan turvallisuutena, josta huolehtiminen on valtiovallan keskeisimpiä tehtäviä. Kansallisen turvallisuuden takaamiseksi on *”ulko-, turvallisuus- ja puolustuspolitiikan tärkeimpinä tehtävinä Suomen itsenäisyyden, alueellisen koskemattomuuden ja perusarvojen turvaaminen, väestön turvallisuuden ja hyvinvoinnin edistäminen sekä yhteiskunnan toimivuuden ylläpitäminen normaali- ja poikkeusoloissa”*.¹⁵

¹⁵ Yhteiskunnan turvallisuusstrategia 2010, s. 1, 3.

Yhteiskunnan turvallisuusstrategien laatineen työryhmän mukaan yhteiskuntamme elintärkeitä toimintoja kansallisen turvallisuuden näkökulmasta ovat:

- ”*valtion johtaminen,*
- *kansainvälinen toiminta,*
- *Suomen puolustuskyky,*
- *sisäinen turvallisuus,*
- *talouden ja infrastruktuurin toimivuus,*
- *väestön toimeentuloturva ja toimintakyky,*
- *henkinen kriisinkestävyys*”.¹⁶

Sellaiset uhkat, jotka kohdistuvat edellä lueteltuihin etuihin, voidaan mietinnön mukaan katsoa sellaisiksi uhkiksi, jotka vaarantavat kansallista turvallisuutta. Työryhmän näkemyksen mukaan globalisaatio on ilmiönä vaikeuttanut valtioiden ulkoisen ja sisäisen turvallisuuden välistä tarkkarajaista erottelua toisistaan. Koska niiden raja on muuttunut häilyvämmäksi, on niiden erottaminen toisistaan aiemmasta poiketen nykyisin entistä vaikeampaa. Lisäksi työryhmän kannan mukaan uhkien ja riskien pakottaminen koskemaan vain tiettyä maantieteellistä aluetta, ”on entistä vaikeampaa taloudellisten, teknisten ja sosiaalisten järjestelmien valtiorajat ylittävästä luonteesta ja keskinäisriippuvuudesta johtuen”.¹⁷

Kansallisen turvallisuuden määrittelyn ongelmia kuvastaa hyvin myös EU:n teettämä tutkimus muutamien jäsenmaiden kansallisista turvallisuusstrategioista. Tutkimuksen mukaan ”kansallinen turvallisuus” on käsitteenä nykyisin hyvin laaja, koska se käsittää ulkoisen valtiollisen uhan lisäksi terrorismin, pandemiat, ilmastonmuutoksen ja järjestäytyneen rikollisuuden tuottamat uhat, sekä perinteiset sisäisen turvallisuuden teemat.¹⁸

Vaikka kansallisen turvallisuuden tarkkarajaisessa määrittelyä ei ole aiemmin tehty ilmeisesti johtuen sen sisällön suhteellisuudesta ja kontekstisidonnaisuudesta, on sitä uhkaava *toiminta* onnistuttu määrittelemään säädösehdotuksen muotoon. Oikeusministeriön asiantuntijatyöryhmän ehdotuksessa (11.10.2016, 41/2016) koskien luottamuksellisen viestin suojan rajoitusedellytyksien muuttamista tarkoitettaisiin *kansallista turvallisuutta vakavasti uhkaavalla toiminnalla*:

”[V]altiojärjestystä tai yhteiskunnan perustoimintoja uhkaavaa toimintaa, kuten terrorismiin liittyvää toimintaa tai väkivaltaista radikalisoitumista taikka ulkomaisten tiedustelupalvelujen toimintaa. Säännöksessä tarkoitettu toiminta voi olla sellaista,

¹⁶ Ibid, s. 15.

¹⁷ Tiedonhankintalakitöryhmän mietintö 2015, s. 18.

¹⁸ Virta 2012, s. 122.

joka konkretisoituessaan olisi rikos, mutta johon ei vielä voida kohdistaa konkreettista ja yksilöityä rikosepäilyä. Samoin kyse voi olla toiminnasta, joka ei ole Suomen lain mukaan rikos, kuten Suomen turvallisuuden kannalta keskeisen valtion levottomuudet ja laajamittaisen Suomeen kohdistuvan maahantulon ohjaaminen.”¹⁹

2.2 Tiedustelu

Tiedustelulla on hyvin pitkä historia, koska sitä on harjoitettu niin kauan kuin ihminen on käynyt sotaa. Ensimmäisen tiedossamme oleva sodankäynnin taitoa koskeva teos on kirjoitettu lähes 2500 vuotta sitten Kiinassa. Sotataidon klassikkona pidettävässä kirjassa *Sodankäynnin taito* kiinalainen Sun Tzu käsittelee muun muassa sodan strategiaa, taktiikkaa ja psykologiaa. Yhdessä ydinluvussa hän käsittelee yhtenä sotaan valmistautumisen tärkeänä osa-alueena salaisten operaatioiden organisoimista ja vihollisesta hankittua ennakkotietoa.

Sun Tzun mukaan ennakkotieto mahdollistaa sen, että valistuneen hallitsijan ja kenraalin saavutukset ylittävät tavallisten ihmisten saavutukset. Tarvittava ennakkotieto on hankittava niiltä, jotka tuntevat vihollisen. Sun Tzun mukaan hallitsija tarvitsee viittä erilaista tyyppiä olevaa salaista asiamiestä, joita ovat;

- *paikallinen agentti*. Vihollisalueen henkilöitä, jotka hallitsija ottaa palvelukseensa.
- *salainen agentti*. Vihollisen virkamiehiä, jotka hallitsija ottaa palvelukseensa.
- *kaksoisagentti*. Vihollisen vakoilijoita, jotka hallitsija ottaa palvelukseensa.
- *uhrattava agentti*. He ovat hallitsijan omia vakoilijoita, joille tarkoituksellisesti annetaan vääriä tietoja.
- *vakoilija*. He ovat hallitsijan omia asiamiehiä, jotka palaavat tietoineen hallitsijan luokse.²⁰

Tutkiessani tiedustelua koskevia teoksia huomiona on ollut, ettei *tiedustelulle* tai *tiedustelutoiminnalle* ole yhtä oikeaa määritelmää. Tämä tulee esille varsinkin ulkomaisessa kirjallisuudessa kuten myös kotimaisessa. Määritelmää pohdittaessa tulee ymmärtää minkälaisesta tiedustelusta kulloinkin on kyse; kenen toimesta sitä tehdään sekä mille taholle tiedustelutoimintaa suoritetaan ja mitä tietoja halutaan kerätä. Tiedustelu –sanan määrittelemisen vaikeutta ymmärtääksemme on syytä avata hieman sen englanninkielisen Intelligence –sanan merkitystä.

¹⁹ Oikeusministeriön julkaisu 41/2016, s. 13.

²⁰ Sun Tzu 1990, s. 147 – 149.

Alan Breakspear²¹ pyrkii artikkelissaan A New Definition of Intelligence vastaamaan kysymykseen, mitä tiedustelu on ja mikä on sen tarkoitus. Vastatakseen näihin kysymyksiin hän lähtee liikkeelle etsimällä vastausta intelligence –sanon peruserkityksistä. Sanakirjat yleensä kattavat intelligence -sanon molemmat puolet – kyvyn hankkia ja käyttää hankittua tietoa. Esimerkiksi Oxford –sanakirja (The online Oxford Dictionary) antaa seuraavat määritelmät sanalle intelligence:

- ”the ability to acquire and apply knowledge and skills: *an eminent man of great intelligence*
- a person or being with the ability to acquire and apply knowledge and skills: *extraterrestrial intelligences*
- the collection of information of military or political value: *the chief of military intelligence*
- people employed in the collection of military or political information: *British intelligence has secured numerous local informers*
- military or political information: *the gathering of intelligence*
- archaic* information in general; news.”

Edellä olevista viimeisin määritelmä on hyödyllinen muistutus vanhasta ja yleisestä intelligence –sanon merkityksestä pelkkänä tietona tai uutisena. Määritelmistä taasen aiemmat asettavat rinnakkain tiedon ja taidon sotilaallisen tai poliittisen tiedon kanssa, jotka ovat pelkistettyjä ja melkein vanhahtavia siinä intelligence -sanon laajassa käytössä liittyen tiedusteluorganisaatioihin ja tiedustelutoimiin 2000 –luvulla.

Cambridge –sanakirja (The online Cambridge Dictionary) kattaa myös molemmat merkitykset. Sanakirjassa Intelligence –sanalla tarkoitetaan ”kykyä oppi, ymmärtää ja tehdä päätöksiä tai muodostaa mielipiteitä perustuen järkeen” ja myös ”salaista tietoa muiden maiden valtionjohdosta, erityisesti vihollishallinnosta, tai ryhmä ihmisiä, jotka keräävät ja käsittelevät tätä tietoa”.²² Jälleen kykyä oppia on verrattu salaiseen tietoon, joka yleensä on tarkoitettu tukemaan päätöksentekoa, joka taasen vuorostaan on mukautumisen ja oppimisen tulosta.²³

Breakspear’in mukaan hallinnon tehtävänä on auttaa yhteiskuntaa sopeutumaan muutoksiin. Olipa omaksuttu hallinnon muoto mikä tahansa tulee sen rakenteiden olla sellaiset, että ne mahdollistavat

²¹ Alan Breakspear on University of Victoria –yliopiston professori ja tiedustelualan tutkija ja Kanadan kansainvälisen neuvoston (The Canadian International Council) entinen johtaja.

²² ‘the ability to learn, understand and make judgments or have opinions that are based on reason’ and also ‘secret information about the governments of other countries, especially enemy governments, or a group of people who collect and deal with this information’.

²³ Breakspear 2013, s. 678 – 679.

sen organisaation kyvyn ennakoida muutoksia sen ulkoisessa ympäristössä, ja siten hyödyntää tarjoutuvia mahdollisuuksia - myönteinen muutos - tai välttää haitallisten vaikutusten uhkia - negatiivinen muutos. Tarvittavat työkalut ovat ennakointi ja oivalluskyky, jotka muotoutuvat tiedustelutoiminnan avulla – sen molemmissa merkityksissä – oppiminen ja tietämys sekä organisatorinen päätöksentekotuki.²⁴

Breakspear'in mukaan tiedustelualalla työskentelevät, kuten monet muutkin alansa ammattilaiset ja oppineet, ovat harvoin taipuvaisia itsetutkiskeluun. He tukeutuvat usein kaskumaisiin tai aforistisiin kuvauksiin ammatistaan ja työstään. Entinen korkea-arvoinen tiedustelu-upseeri Kanadan sotilastiedustelusta Breakspear'in kuuleman mukaan kuvasi tiedustelua seuraavasti: "Intelligence is *hard* information; that is, information that is *hard* to get because someone doesn't want you to have it". Tämä yksinkertaistettu kuvaus on Breakspear'in mukaan kylläkin käypä, mutta sen informaation sisältö auttaa hyvin vähän kansalaisia ja mediaa ymmärtämään tiedustelun roolia ja sen vaikuttavuutta.²⁵

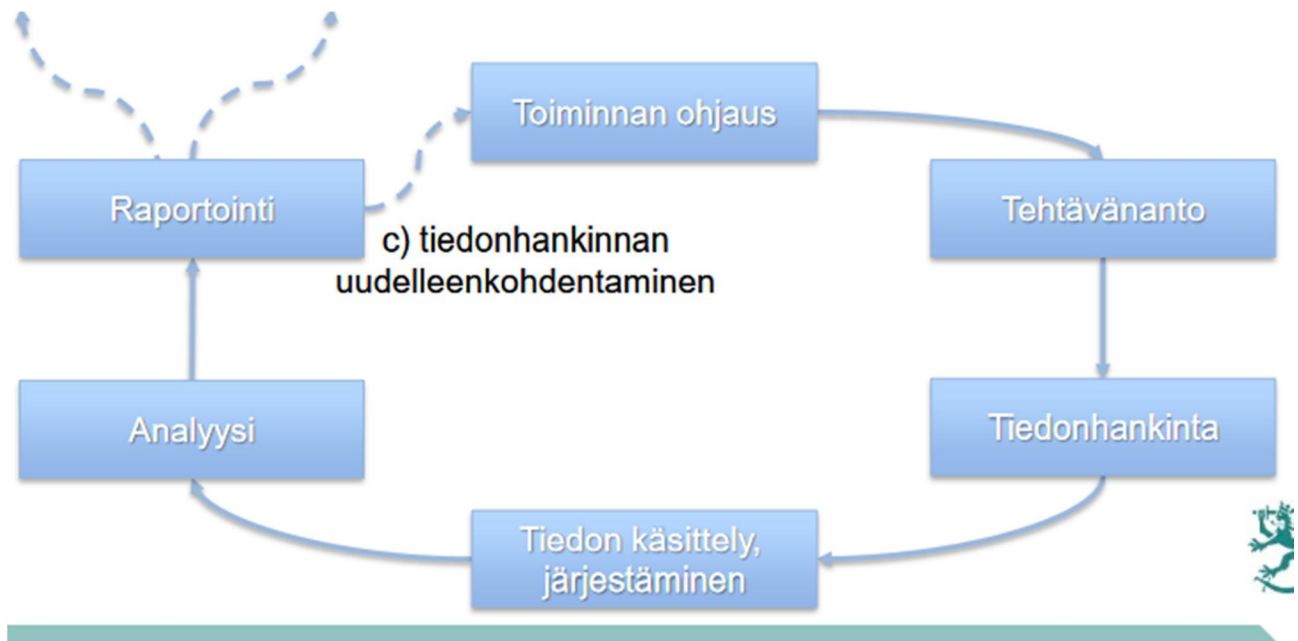
Kuten jo edellä on todettu, tiedustelu on käsite, jolla on monta merkitystä. 1) Ensinnäkin sillä usein tarkoitetaan tuotetta tai paremmin sanottuna yksityiskohtaista ja rajattua *lopputulosta* saadusta tai kerätystä *tiedosta*. "Tarvitsen tietoa valtiosta X" tai "Onko mitään uutta tietoa panttivankitilanteesta?" voisivat olla tavallisia tilanteita *tieto* –sanana käytöstä liittyen tiedusteluun. Tieto –sanana käyttö tässä yhteydessä viittaa informaatioon, joka on kerätty ja analysoitu tarkoituksena lisätä tietoa ja ymmärrystä jostain tietystä aiheesta. 2) Toiseksi tiedustelu voi tarkoittaa myös *toimintaa*, jossa avoin ja salainen aineisto on muutettu käyttökelpoiseksi informaatioksi, joka välitetään päätöksentekijöille. Yleisesti tiedustelua on kuvattu kehämäisenä toimintaprosessina sisältäen sellaiset vaiheet kuten; tehtäväksi antaminen, tiedon kerääminen, sen analysoiminen ja välittäminen sitä tarvitseville. Tämä kehämalli (kuva 1) vahvistaa ajatusta tiedustelusta nimenomaan toimintana. 3) Kolmanneksi tiedustelu voi viitata myös *organisaatioon*, joka on perustettu suorittamaan edellä mainittuja tiedusteluun liittyviä toimintoja. Sherman Kent esitteli vuonna 1949 tämän kolmikohtaisen määritelmän, jota ovat toistaneet ja lainanneet useat tutkijat. Monet tutkijat sisällyttävät tiedustelun määritelmäänsä yhden tai useamman osan edellä mainituista määritelmistä. Lisäksi perinteiseen määritelmädebatettiin liittyy usein se, pitääkö tiedustelun olla tekemisissä ulkomaisten entiteettien

²⁴ Breakspear 2013, s. 678 – 679.

²⁵ Breakspear 2013, s. 682.

kanssa, vai pitääkö siihen liittyä oleellisesti salailu ja salassapito, vaiko pitääkö siihen liittyä olennaisena osana tiedustelupalveluiden salainen toiminta.²⁶

Kuva 1. Kehämalli²⁷



Tiedustelutoimintaan liittyy vakiintuneesti vastapuoli, joka on tiedustelutoiminnan kohteena. Vaikkakin tiedustelua kohdistetaan myös oman valtion sisälle tai oman organisaation toimijoihin, ajatellaan tiedustelun yleensä olevan tiedon keruuta ja ymmärryksen lisäämistä vastapuolesta.

Puhuttaessa tiedustelutoiminnan käytössä olevista keinoista ja välineistä, on yleensä jaettu kolmeen osa-alueeseen; 1) henkilö- (Humint), 2) signaali- (Sigint) ja 3) avointen lähteiden (Osint) tiedusteluun. Harjoitettaessa *henkilötiedustelua* henkilöä ohjeistetaan joko hankkimaan tai antamaan hallussaan olevaa tietoa tiedusteluviranomaiselle. *Signaalitiedustelua* harjoitettaessa kerätään, tallennetaan ja käsitellään sähköisessä tai radiosignaali muodossa olevaa informaatiota. Tiedustelun perustuessa *avoimiin lähteisiin*, tiedonhankinnan kohteena ovat julkisesti ja vapaasti saatavilla oleva aineisto eri muodoissa.²⁸

Tiedustelua ja sen toimintamuotoja sekä käytettävien keinojen käsitteistön määrittely on Suomessa toistaiseksi hyvin vakiintumatonta varsinkin siksi, ettei niistä ei ole säädetty laissa.

²⁶ Fägersten 2010, s. 31 – 32.

²⁷ Sisäministeriön / poliisijohtaja Petri Knape esitelmä 8.2.2017, dia-esitys s. 12. https://tietoyhteiskunta-akatemia.fi/wp-content/uploads/2017/02/Sis%C3%A4ministeri%C3%B6_Knape.pdf (luettu 3.9.2018)

²⁸ Sisäministeriön julkaisu 28/2014, s. 25.

Tiedonhankintalakityöryhmä on mietinnössä onnistunut määrittelemään hyvin ymmärrettävästi tiedustelun ja sen tarkoituksen, mikä on tuon määritelmän mukaan:

”Julkisiin ja ei-julkisiin lähteisiin kohdistuvaa tiedonhankintaa, jonka tarkoituksena on kartoittaa ja lisätä ymmärrystä erilaisista uhista, riskeistä, mahdollisuuksista ja muutoksista niin maan sisällä kuin rajojen ulkopuolella. Tiedustelutoiminnan tavoitteena on tuottaa varhaisvaiheen tietoa, joka mahdollistaa uhkiin, riskeihin, mahdollisuuksiin ja muutoksiin vaikuttamisen ja varautumisen. Tiedusteluun kuuluu tiedon analysointi, jonka avulla erilaisia turvallisuusympäristön epävarmuustekijöitä pyritään jäsentämään, vähentämään ja tapauskohtaisesti myös hyödyntämään.”²⁹

Käyttäessäni sanaa tiedustelu, tarkoitetaan sillä siis aina aktiivista toimintaa, johon liittyy tehtävänanto, tietojen kerääminen ja hankkiminen julkisesti saatavilla olevista tai salassa pidettävistä lähteistä, informaation analysointi ja jakaminen tavoitteena vähentää päätöksentekijöiden epävarmuutta turvallisuuteen liittyvässä päätöksenteossa.³⁰

Tämä tutkimus korostaa tiedustelun ulottuvuutta ja näkökantaa nimenomaan toimintana, jättäen avoimeksi sen ollaanko tekemisissä ulkomaisten tai sisäisten asioiden kanssa. Eikä myöskään rajata tiedustelun määritelmää koskemaan vain salaisia metodeja tai tiedon lähteitä. Se on nähtävä laajasti toimintana, eikä vain passiivisena sanana tarkoittaen vain tietoa, kysymystä tai kyselyä. Tiedustelu käsittelee aina jollain tavoin erilaista tietoa, vaikkakaan kaikki tietojenkäsittely ei aina ole tiedustelua sen edellä mainitussa merkityksessä. Tutkimuksessa keskitytään ainoastaan valtiollisiin toimijoihin, joilla on tai joille ollaan lainsäädännöllä luomassa mandaattia tiedustelutoiminnan harjoittamiseen.

Tiedustelu jaetaan perinteisesti vielä sitä harjoittavan tahon ja hankittavan tiedon käyttötarkoituksen mukaisesti neljään päälinjaan sotilas-, siviili-, turvallisuus- ja rikostiedusteluun, mietinnössä nämä päälinjat on määritelty seuraavasti:

- 1. ”Sotilasviranomaisen suorittaa sotilastiedustelua, jolla tuotetaan strategista ja operatiivista toimintaympäristötietoa ja -arvioita ylimmän valtionjohdon ja puolustusvoimien johdon päätöksenteon tueksi. Sotilastiedustelu vastaa strategisen, operatiivisen ja taktisen ennakkovaroituksen antamisesta, maalittamistuesta ja puolustusvoimien tarvitsemista paikka- ja olosuhdetiedoista. Ennakkovaroitus mahdollistaa vastatoimenpiteiden toteuttamisen uhkaa vastaavasti.”*

²⁹ Tiedonhankintalakityöryhmän mietintö 2015, s. 15.

³⁰ Fägersten 2010, s. 31 – 32.

2. *”Siviiliviranomainen suorittaa siviilitiedustelua, jolla tuotetaan tietoa ylimmän valtionjohdon päätöksenteon ja oman operatiivisen toiminnan tueksi muista kuin sotilaallisen maanpuolustuksen alaan liittyvistä aiheista.”*
3. *”Turvallisuustiedustelun tarkoituksena on havaita, tunnistaa, ymmärtää ja torjua valtion sisäiseen tai ulkoiseen turvallisuuteen kohdistuvia uhkia. Turvallisuustiedustelun tiedonhankinta kohdistuu laajaan toimintaympäristöön eikä se ole samalla tavalla rikossidonnaista kuin rikostiedustelu.”*
4. *”Lainvalvontaviranomainen suorittaa rikostiedustelua, jonka tarkoituksena on hankkia rikoksen estämisen, paljastamisen tai selvittämisen kannalta merkityksellistä tietoa rikollisista, rikoksista ja rikokseteko-olosuhteista.”³¹ Esitutkinnassa rikostiedustelutietoa käytetään lisäksi tutkinnan suuntaamisessa sekä todisteena.³²*

2.3 Vakoilu

Vakoilu on osa tiedustelutoimintaa ja se määritellään yleensä luvattomaksi ja oikeudettomaksi tiedustelutoiminnaksi, jonka avulla pyritään hankkimaan tietoja sen kohteelta salassa ja vastoin kohteen tahtoa. Yleisesti ottaen voidaan pitää sääntönä, että vakoilun avulla pyritään saamaan tietoa valtioiden hallinnosta ja niiden sotilaallisista organisaatioista, mutta myös yksittäisistä henkilöistä tai jostain erityisestä henkilökunnasta, joka tai jotka työskentelevät valtion organisaatioissa. Kohteina varsinkin nykyään ovat tietoliikenneyhteydet sekä tietoverkot siihen kiinnittyneine käyttäjinne. Keinovalikoimaan kuuluvat ihmisten suorittama vakoilu, apuvälineiden käyttö (mm. vakoilusatelliitit), salakuuntelu, signaalitiedustelu ja internet. Valtioiden välinen vakoilu kohdistuu yleensä ulkopoliittiseen päätöksentekokoneistoon, asevoimiin ja muihin turvallisuusorganisaatioihin.³³ Tässä tutkimuksessa ei varsinaisesti käsitellä vakoilua, mutta lukijan on hyvä ymmärtää sen ero tiedustelutoimintaan, joka on yleensä luvanvaraista ja siihen kohdistuu parlamentaarinen tai muunlainen jälkivalvonta.

2.4 Kybertoimintaympäristö

Kuten tiedonhankintalakityöryhmä toteaa, ovat kaikki tietoyhteiskunnat ja kansainvälisiin markkinoihin nojaavat taloudet riippuvaisia tietoinfrastruktuurin häiriöttömästä toiminnasta. Toimintavarma tietoinfrastruktuuri toimii myös yhteiskuntamme kokonaisturvallisuuden takuumiehenä. Suomen kriittisestä tietoliikenneinfrastruktuurista ja sen palveluista suuren osan omistaa ja tuottaa yksityinen sektori, jonka rooli yhteiskunnan elintärkeiden toimintojen

³¹ Tiedonhankintalakityöryhmän mietintö 2015, s. 15 – 16.

³² Sisäministeriön julkaisu 28/2014, s. 27.

³³ Kuosma 2015, s. 29 – 32.

turvaamisessa onkin tärkeä. Tietoturvan avulla suojataan ja taataan tietoverkkojen ja -järjestelmien sekä sähköisen viestinnän toimivuus ja häiriöttömyys. ”Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että määrätty tieto on vain niiden käyttöön oikeutettujen saatavilla (luottamuksellisuus), ettei tietoa voida muuttaa muiden kuin siihen oikeutettujen toimesta (eheys), ja että tieto ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (käytettävyys). Tietoturvaohjelmien havaitseminen ja niiltä suojautuminen perustuu niin hallinnossa kuin yksityiselläkin sektorilla käytännössä kaupallisiin tietoturvaohjelmiin ja –palveluihin”.³⁴

Tiedonhankintalakiyöryhmän mukaan tietoturvaohjelmat pitää määritelmällisesti erottaa ja ymmärtää pitää erillään tietoverkkouhkeista, joilla pyritään vaikuttamaan valtion elinkelpoisuuteen tai sen keskeisiin turvallisuusasetuksiin. Keskeisimpiä tietoverkkouhkeita ovat kybervakoilu, kyberterrorismi ja kyberoperaatiot. Tämän kaltaisissa toimissa yksityiset tai valtiolliset tahot käyttävät nimenomaan tietoverkkoja välineenä horjuttaakseen kohdevaltion kansallista turvallisuutta.³⁵

Suomen kyberturvallisuusstrategian laatineen työryhmän mukaan ”kybertoimintaympäristö on sähköisessä muodossa olevan informaation (tiedon) käsittelyyn tarkoitettu, yhdestä tai useammasta tietojärjestelmästä muodostuva toimintaympäristö”. Tässä ympäristössä dataa ja informaatiota varastoidaan, muokataan ja siirretään viestintäverkkojen avulla ja siihen kuuluvat myös datan ja informaation käsittelyyn liittyvät fyysiset rakenteet, kuten tietokoneet, palvelinsalit ja tietoliikennekaapelit- ja mastot.³⁶ Globaali kybertoimintaympäristö taas työryhmän mukaan ”muodostuu monimutkaisesta ja –kerroksisesta maailmanlaajuisesta informaatioverkostosta, johon kuuluu kansallisia turvallisuusviranomaisten, muun julkishallinnon ja yrity maailman tietoverkkoja sekä teollisuuden ja kriittisen infrastruktuurin valvonta- ja ohjausjärjestelmiä”. Kybertoimintaympäristö on maailman laajuinen ja se on yhdistänyt valtioita, yrityksiä ja kansalaisia reaaliaikaisesti entistä läheisemmiksi.³⁷

Yhteiskunnat eripuolilla maailmaa ovat nykyisin hyvin riippuvaisia teknisten järjestelmien toimivuudesta. Kuitenkin tämä yhteiskunnan toimintoja kannatteleva tekninen infrastruktuuri on haavoittuva ja näin ollen siitä on tullut houkutteleva kohde rikollisille ja terroristeille. Yhteiskunnan toimivuuden turvaamiseksi Suomen kyberturvallisuusstrategian laatinut työryhmä onkin määritellyt niin sanotun kriittisen infrastruktuurin, joka pitää sisällään yhteiskunnan toiminnan kannalta

³⁴ Tiedonhankintalakiyöryhmän mietintö 2015, s. 34.

³⁵ Ibid, s. 21.

³⁶ Suomen kyberturvallisuusstrategia 2013, s. 12.

³⁷ Ibid, s. 17.

välttämättömät fyysiset ja sähköiset rakenteet, järjestelmät ja palvelut. Siihen kuuluvat pankki- ja rahoitusjärjestelmä, energiahuolto, elintarvikehuolto, tieto- ja viestintäjärjestelmät, terveydenhuolto, sosiaaliturva ja pelastuspalvelut, kuljetus- ja logistiikka sekä vesihuolto.³⁸

Tietoyhteiskuntana Suomi on hyvin pitkälle kehittynyt ja näin ollen erittäin riippuvainen tietoverkkojen ja –järjestelmien toiminnasta. Tästä johtuen juuri kybertoimintaympäristöstä tulevat uhkat ovat meidän kokonaisturvallisuuden kannalta hyvin merkittäviä tekijöitä, joihin on syytä varautua. Useat valtiot sekä muut toimijat eivät ole pelkästään tyytyneet kehittämään järjestelmiään suojautuakseen kyberuhkilta, vaan ne ovat kehittäneet itselleen sellaista kybersuorituskykyä, joka on luonut niille osaamista ja kyvyn häiritä, vahingoittaa tai hyväksikäyttää toisten tietojärjestelmiä. Globaalin teknologisen toimintaympäristön keskinäisriippuvuudesta johtuen kybertoimintaympäristön kautta voidaan vaikuttaa koko yhteiskunnan toimintaan ja sen kaikkiin toimijoihin. Suomen kansallisessa riskiarviossa todetaankin, että kybertoimintaympäristön kehityksen seurauksena turvallisuuteemme kohdistuvat uhat ovat yhä monimuotoisempia ja että niiden potentiaaliset seuraukset ovat entistä vakavampia.³⁹

Vaikka kehitys on lisännyt merkittävästi hyvinvointia, on sen tuloksena syntynyt kyberturvallisuusstrategiatyöryhmän mukaan myös aivan uusia riskitekijöitä. Tietoteknisten laitteiden ja järjestelmien toimimattomuudesta, informaatio-infrastruktuurin luhistumisesta tai vakavista kyberhyökkäyksistä voi aiheutua erittäin kielteisiä vaikutuksia valtionhallinnolle, julkisten palveluiden tuottajille ja elinkeinoelämälle, näin ollen koko yhteiskunnan toiminnalle.⁴⁰

Suomen kyberturvallisuusstrategian mukaan kyberturvallisuus on tavoitetila, ”*jossa kybertoimintaympäristöön voidaan luottaa ja jossa sen toiminta turvataan. Oltessa tuossa tavoitetilassa kybertoimintaympäristöstä ei aiheudu vaaraa, haittaa tai häiriötä sähköisen tiedon (informaation) käsittelystä riippuvaiselle toiminnalle eikä sen toimivuudelle. Tavoitteena on saavuttaa ennakkoon kyky hallita ja tarvittaessa sietää kyberuhkia ja niiden vaikutuksia, jotka voivat aiheuttaa merkittävää haittaa tai vaaraa Suomelle tai sen väestölle*”.⁴¹

Nykyään on vallalla ajatus, että kaikkeen pitää pystyä varautumaan. Tällöin varautumisen haasteeksi muodostuu toimintojen ja infrastruktuurin verkostojen keskinäisriippuvuus. Tämä tulee Lonkan ja

³⁸ Kansallinen turvallisuustutkimuksen strategia, s. 25.

³⁹ Suomen kansallinen riskiarvio 2015, s. 18.

⁴⁰ Suomen kyberturvallisuusstrategia 2013, s. 17.

⁴¹ Suomen kyberturvallisuusstrategia 2013, s. 13.

Limnellin mukaan erinomaisesti esille World Economic Forumin vuoden 2015 uhka-arviossa, jossa korostuu erityisesti sekä eri uhkatekijöiden keskinäinen vuorovaikutus että turvallisuuden kompleksinen uhkakokonaisuus. Toisaalta samalla, kun teknologiajärjestelmät ovat uhkien toteutumisen ja siten varautumistoiminnan kohde, ne ovat myös väistämättä osa ratkaisua ja välttämätön osa varautumista sinällään.⁴²

3 Tiedustelulakihankkeen taustaa ja nykytila

3.1 Yleistä

Tämän luvun tarkoituksena on perehdyttää lukija lakihankkeen ja tutkimuksen taustoihin sekä viitekehykseen eli tiedustelutoimintaan ja sitä harjoittaviin organisaatioihin Suomessa.

Turvallisuusviranomaisten tiedonhankintakyvyn kehittämisen tavoitteena on tiedonhankintalakitöryhmän mukaan mahdollistaa kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitseminen ja tunnistaminen sekä niiden torjuminen. Tällaiset uhat voidaan yleisesti jakaa siviililuonteisiin ja sotilaallisiin. Pääasiallisina siviililuonteisina turvallisuusuhkina mietinnössä mainitaan kansainvälinen terrorismi, ulkovaltojen Suomeen ja sen etuihin kohdistamaa vakoilu ja vakava kansainvälinen järjestäytynyt rikollisuus. Sotilaallisten uhkien osalta mietinnössä kiinnitetään huomiota niiden muuttuneeseen luonteeseen. Nykyisin sotilasoperaatiot sisältävät usein erilaisia epäsymmetrisiä hybridisodankäynnin keinoja, kuten tietoverkkohyökkäyksiä sekä painostus- ja disinformaatio-operaatioita, jotka alkavat jo ennen varsinaisia sotatoimia. Ajallisesti modernit sotilasoperaatiot siis alkavat jo rauhan aikana.⁴³

Tiedonhankintalakitöryhmän mukaan koko maailman kattava tietoverkkoympäristö on mahdollistanut rajat ylittävän vakoilun, joka on ilmiönä noussut merkittäväksi uhaksi varsinkin viime vuosina. Uhkien havaitsemisen ja tunnistamisen sekä niiden torjumisen lisäksi tiedustelulakihankkeen tavoitteena on parantaa ylimmän valtionjohdon tiedonsaantia uhista ja Suomen turvallisuusympäristössä tapahtuvista muutoksista. Turvallisuusviranomaisilla on työryhmän näkemyksen mukaan oltava kyky tuottaa valtion ylimmälle johdolle tietoa, joka puolueetonta ja luotettavaa, lisäksi tiedon oltava käytettävissä riittävän ajoissa ennen merkittävää päätöksentekoa. Tällainen merkityksellinen tieto antaa valtionjohdolle mahdollisuuden vaikuttaa ja varautua turvallisuusympäristössämme esiintyviin uhkiin, riskeihin ja mahdollisuuksiin. Tiedonhankintalakitöryhmän mukaan tiedustelutietoa hankkimalla voisimme paremmin taata

⁴² Lonka – Limnell 2015, s. 202.

⁴³ Tiedonhankintalakitöryhmän mietintö 2015, s. 18 – 19.

kansallista turvallisuutta, jonka työryhmä näkee tärkeäksi koko yhteiskunnan kannalta ja myös elinkeinoelämän toimivuuden kannalta.⁴⁴

Poliisiviranomaiset ovat yhteiskunnallisten intressien vuoksi harjoittaneet Suomessa salaista tiedonhankintaa eli tiedustelutoimintaa kohdehenkilön tietämättä jo ennen kuin näistä toimivaltuuksista oli laissa säädetty. Ennen lakitasoisia toimivaltasäännöksiä poliisin toimivallan katsottiin perustuvan tavanomaiseen oikeuteen eli kirjoittamattomaan poliisin yleisvaltuuteen, jonka katsottiin perustuvan yleisen järjestyksen ja turvallisuuden ylläpitämisen maksimiin. Senaikaisen oikeuskäsityksen mukaan ajateltiin, että poliisilla oli oikeus suorittaa tehtäviään kaikilla niillä tavoilla, joita ei laissa ollut erikseen kielletty. Vuodesta 1992 lähtien ryhtyi poliisin ylijohdo ohjaamaan salaista tiedonhankintaa hallinnollisin määräyksin ja ohjein. Samana vuonna säädettiin ensimmäinen laki (Teletointila 676/92) koskien salaisen tiedonhankinnan toimivaltuutusta: poliisin oikeus saada puhelinliikenteen tunnistetietoja teleyrityksiltä. Nykyisin poliisin kaikki salaisen tiedonhankinnan toimivaltuudet perustuvat lainsäädäntöön.⁴⁵

Tiedustelulakihanke sai alkusysäyksen 2013 valmistuneesta Suomen kyberturvallisuusstrategiasta, jonka mukaan kansallista lainsäädäntöä tulisi tarkastella ja kehittää kyberturvallisuuden parantamiseksi. Strategian taustamuistion mukaan valtion turvallisuutta vaarantavien kyberuhkien torjumiseksi meillä olisi selvitettävä lainsäädännössä ja kansainvälisissä sopimuksissa olevien velvoitteiden mahdollisesti asettamat esteet ja rajoitteet sekä tiedon käsittelyä koskevat velvoitteet, jotka voivat haitata kyberuhkien tehokkaaseen torjumiseen tarvittavan tiedon saantia ja jakamista eri viranomaisten ja muiden toimijoiden kesken. Samalla tulisi arvioida sitä, onko vastuuviranomaisille syytä luoda nykyistä paremmat toimivaltuudet, jotka mahdollistaisivat tiedon keräämiseen, kokoamiseen ja saannin kyberuhista ja niiden aiheuttajista ennakkollisesti jo ennen uhan realisoitumista.⁴⁶

Taustamuistiossa otettiin erillisenä kysymyksenä esille myös varsinaisen tiedustelutoiminnan kehittämiseen liittyvät lainsäädännön muutostarpeet ja lainsäädäntöä esitettiin kehitettäväksi poliisitoiminnan ja puolustusvoimien osalta. Poliisitoiminnan osalta kehittämiskohteina olivat eritoten tiedustelua koskevat toimivaltuudet ja toimivaltuudet kyberrikollisuuden tutkintaan niiden ennaltaehkäisemiseksi, havaitsemiseksi ja torjumiseksi. Puolustusvoimien osalta muistiossa

⁴⁴ Tiedonhankintalaki työryhmän mietintö 2015, s. 13 – 14.

⁴⁵ Hankilanoja 2014, s. 69 – 70.

⁴⁶ Kyberturvallisuusstrategian taustamuistio, s. 35.

esitettiin, että lainsäädännön uudistamisen yhteydessä kybervaikutuskeinoja ja -tiedustelua koskevia toimivaltasäännöksiä tulisi selkeyttää ja parantaa. Vielä todettiin, että mikäli toimivaltuuksia laajennetaan, tulisi samalla erityisesti huomioida ja varmistaa ihmis- ja perusoikeuksien toteutuminen esimerkiksi lisättäessä tiedusteluoikeuksia.⁴⁷

Tiedustelulakihankkeen valmistelun aloittamiseen liittyy myös suojelupoliisin hallinnollista asemaa ja sen valvonnan kehittämistä selvittäneen työryhmän 24.9.2014 valmistunut loppuraportti. Työryhmän tehtävänantoon kuului myös suojelupoliisin toiminnan kehittämistarpeiden arviointi tulevien turvallisuusuhkien varalle. Työryhmän näkemyksen mukaan suojelupoliisin toimintaympäristö on merkittävästi muuttunut ja monimutkaistunut. Yhtenä merkittävänä muutoksena työryhmä näki suojelupoliisin toimintaympäristön tietoteknistyminen. Toimintaympäristön muutoksista johtuen suojelupoliisille tulisi työryhmän mielestä luoda uusia tiedustelua koskevia toimivaltuuksia, jotta sillä olisi kyky vastata näihin muutoksiin.⁴⁸

Puolustusministeriö asetti 13.12.2013 tiedonhankintalakityöryhmän selvittämään lainsäädäntöä, jolla voitaisiin parantaa turvallisuusviranomaisten tiedonhankintakykyä kybetoimintaympäristön uhkista. Työryhmän oli tarkoitus saada työnsä valmiiksi 30.6.2014, puolustusministeriö jatkoi määräaikaan 31.12.2014 saakka.⁴⁹ Lausuntopyynnössä pyydettiin lausumaan erityisesti työryhmän kehittämis ehdotuksista⁵⁰ ja johtopäätöksistä sekä ehdotusten vaikutuksista lausunnonantajan toimintaan tai toimialaan.

Vireillä olevat siviili- ja sotilastiedustelua koskevat lait selkeyttäisivät lainsäädäntöä, koska tällöin salaisista tiedonhankintakeinoista olisi lainsäädännössä kootusti kaikki ne keinot ja valtuudet selkeästi kahdessa niitä nimenomaisesti koskevassa laissa. Nykytilanteessa ne ovat hajallaan poliisi- ja pakkokeinolaissa sekä sotilaskurinpidosta ja rikostorjunnasta puolustusvoimista annetussa laissa (255/2014). Varsinkin kansalaisen näkökulmasta ajatellen erilliset lait lisäisivät kansalaisten ymmärrystä siitä, mitä toimia meihin kaikkiin voidaan osoittaa ilman rikosepäilyä.

⁴⁷ Ibid, s. 35.

⁴⁸ Sisäministeriön julkaisu 28/2014, työryhmän loppuraportti 2014, kuvailulehti.

⁴⁹ Tiedonhankintalakityöryhmän mietintö 2015, s. 7.

⁵⁰ Kehittämis ehdotus –kappaleen pääotsikot ovat Tietoliikennetiedustelu sekä Ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu.

3.2 Tiedustelutoiminta muuttuvassa turvallisuusympäristössä

Tiedonhankintalakityöryhmän käsityksen mukaan yleisesti lisääntynyt kansainvälistyminen ja tekninen kehitys ovat viime vuosina saaneet aikaan merkittäviä muutoksia Suomen turvallisuusympäristössä, joka näin ollen nähdään myös yhä monimutkaisempana. Lisäksi sisäisen ja ulkoisen turvallisuuden välinen raja on hämärtynyt, ja niihin kohdistuvat uhat limittyvätkin toisiinsa entistä läheisemmin. Vakavimmat kansallista turvallisuutta horjuttavat uhat ovat useimmiten kansainvälistä alkuperää tai niillä on ainakin kytköksiä ulkomaille. Vaikka tietotekniikan kehitys yleensä nähdään positiivisena ja hyvinvointia synnyttävänä ilmiönä, sisältää se myös haittapuolensa. Uhkien lähteenä voi olla valtiollinen tai ei-valtiollinen toimija. Koska nykyteknologia on lähes kaikkien saatavilla, on tämä vaikeuttanut uhkien lähteen tunnistamista ja erottamista toisistaan. Globaali tietoverkko soveltuu erinomaisesti alustaksi erilaisille hyökkäyksille, joiden tarkoituksena on usein kohdevaltion poliittinen ja taloudellinen painostaminen.⁵¹

Valtion sisäisten ja ulkoisten turvallisuusuhkien tunnistamisesta huolehtivan suojelupoliisin näkemyksen mukaan Suomen turvallisuusympäristö on nykyään yhä vaikeammin ennustettava ja monimutkaisempi. Terrori-iskut Pariisissa marraskuussa 2015, Brysselissä maaliskuussa 2016, Tukholmassa huhtikuussa 2017 ja Suomen Turussa elokuussa 2017 muistuttavat meitä siitä, että demokraattisesti hallittuihin ja avoimiin yhteiskuntiin kohdistuvat siviili- ja sotilasuhat ovat yleistyneet ja ne ovat todellisia. SUPO:n mukaan Suomen siviilitiedustelu ympäristö on muuttunut niin terrorismintorjunnan kuin vakoilun osalta hyvin nopeasti viimeisen 3 – 4 vuoden aikana. Nopean muutostahdin lisäksi muutokset ovat olleet vaikeasti ennakoitavia, esimerkkinä turvapaikanhakijoiden määrän räjähdysmäinen kasvu lyhyessä ajassa Suomessa vuonna 2015.⁵²

Warwick yliopiston kansainvälisen turvallisuuden laitoksen *professori Richard J. Aldrich*'in mukaan on nykyään toistuvasti havaittu, ettei tiedustelu ole koskaan ennen ollut niin tärkeässä asemassa maailman politiikassa kuin se on ollut 2000-luvun alusta lukien. Ajatus tehokkaasta tiedustelutoiminnasta on keskeistä terrorismin ja järjestäytyneen rikollisuuden vastaisessa toiminnassa sekä muiden kansallista turvallisuutta uhkaavien toimien torjunnassa.⁵³

⁵¹ Tiedonhankintalakityöryhmän mietintö 2015, s. 13.

⁵² SUPO:n vuosikirja 2015, s. 4.

⁵³ Aldrich 2011, s. 19.

Onnistuakseen toimissaan Suomen turvallisuusstrategian mukaan valtion ylimmällä johdolla tulee olla käytössään tietoa ympäristöstämme ja sen tapahtumista sekä niiden vaikutuksista toimintaamme valtiona. Varsinkin yhteiskuntarauhaa ja turvallisuuttamme uhkaavissa tilanteissa korostuu käytettävissä olevan tilannetietoisuuden tarkoituksenmukaisuus ja nopeus kykyyn vastata muutoksiin, tiedon on luonnollisesti perustuttava oikeaan ja relevanttiin tietoon sekä arvioihin. Oikeita ratkaisuja tehdäkseen on valtiojohdon ymmärrettävä päätöksentekonsa perusteet, siihen liittyvät seuraukset ja muiden reaktiot sekä mahdolliset riskit, jotka päätökseen voi sisältyä. Näiden seikkojen vuoksi valtiojohdolla tulee olla riittävä tilannetietoisuus, joka mahdollistaa oikea-aikaisen päätöksenteon. Tilannetietoisuuden perustana on tilannekuva, joka syntyy asiantuntijoiden kokoamana kuvauksena senhetkisistä olosuhteista, uhkatilanteen synnyttäneistä tapahtumista, sitä koskevista taustatiedoista ja tilanteen kehittymistä koskevista arvioista, lisäksi kuvaan kuuluu tilanteessa mukana olevien toimijoiden toimivaltuudet uhkaan vastaamiseksi.⁵⁴

3.3 Kansallisesta turvallisuudesta vastaavien viranomaisten lakisääteiset tehtävät

Kansalliseen turvallisuuteen kohdistuvien siviililuonteisten uhkien torjunnassa merkittävin rooli on sisäministeriön hallinnonalaan kuuluvalla suojelupoliisilla. SUPO:ssa toivotaankin lainsäädäntöä, joka mahdollistaisi pakkokeinona käytettävän tietoverkossa tapahtuvan tiedustelun jo ennen varsinaista rikosepäilyä. Nykyisin salaisia tiedonhankintakeinoja saa käyttää vain kun on perusteltu syy olettaa tietyn tai tiettyjen henkilöiden syyllistyvän rikokseen. SUPO:n apulaispäällikkö Petri Knapen mukaan kansallisesta turvallisuudesta vastaavat turvallisuusviranomaiset ovat auttamattomasti myöhässä, jos käytettävissä olevat toimivaltuudet ja tiedonhankinta on mahdollista tehokkaasti vasta silloin, kun rikos on jo tekeillä tai tehty.⁵⁵

Sisäministeriön hallinnonalan viranomaisena poliisin ja suojelupoliisin yhtenä tehtävänä on torjua kansalliseen turvallisuuteen kohdistuvia siviililuonteisia uhkia. Poliisin tiedonhankinta-toimivaltuudet ovat pakkokeino- ja poliisilaisissa hiljattain uudistettu. Mielestäni on jotenkin nurinkurista, ettei suojelupoliisille ole säädetty nimenomaisia toimivaltuuksia tiedustelutoimintaan eikä tiedonhankintaa varten, sille määrättyjen tehtävien luonteesta huolimatta, sen tiedonhankintatoimivaltuudet perustuvat ainoastaan poliisia koskeviin yleisiin säädöksiin.⁵⁶

⁵⁴ Yhteiskunnan turvallisuusstrategia 2010, s. 56 – 57.

⁵⁵ Sokala 2016, artikkeli.

⁵⁶ Tiedonhankintalakityöryhmän mietintö 2015, s. 14.

Puolustusministeriön hallinnonalaan kuuluva Puolustusvoimat taas vastaa Suomen sotilaallisesta puolustamisesta. Puolustusvoimien tiedustelullisesta tiedonhankinnasta eli sotilastiedustelusta ei myöskään ole säädetty lailla. Vaikka Puolustusvoimista annetun lain (551/2007) valmisteluasiakirjojen mukaan tiedonhankinta on yksi puolustusvoimien tehtävistä, ei siinä kuitenkaan ole varsinaisesti säädetty toimivaltuuksista tiedonhankintaan.⁵⁷

Poliisin tärkeimmät tehtävät on määritelty poliisilain (PoliisiL, 872/2011) 1 luvun 1 §:ssä, jonka ensimmäinen momentti kuuluu seuraavasti:

”Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen.”

Lisäksi poliisilain 1 luvun 1 §:ssä luetellaan myös muita poliisin tehtäviä turvallisuuden ylläpitämiseksi, kuten esimerkiksi yhteistyö muiden viranomaisten ja kansalaisten kanssa.

Poliisin toimivaltuuksista ja tiedonhankintakeinoista säädetään poliisilain lisäksi myös esitutkintalaissa (ETL 805/2011) ja pakkokeinolaissa (PKL, 806/2011), jotka valmisteltiin rinnan ja tulivat voimaan samaan aikaan nykyisen poliisilain kanssa 1.1.2014.⁵⁸ Rikosten *estämiseksi ja paljastamiseksi* tarvittavat tiedonhankintatoimivaltuudet on säädetty poliisilaissa, kun taas rikosten *selvittämiseksi* tarvittavat tiedonhankintatoimivaltuudet on säädetty pakkokeino- ja esitutkintalaeissa. Poliisi- ja pakkokeinolain antamat tiedonhankintakeinot ovat hyvin samankaltaisia, säädösten erona on vain se tarkoitus, johon näitä keinoja käytetään. Poliisilain keinovalikoimalla pyritään rikosten estämiseen ja paljastamiseen, sitä vastoin pakkokeinolain antamien keinojen tarkoituksena on rikosten selvittäminen.⁵⁹

Rikosten estämisen ja paljastamisen määritelmät on kirjattu poliisilain 5 lukuun, jossa säädetään myös poliisin käytettävissä olevista salaisista tiedonhankintakeinoista. Poliisilain 5:1.2 §:n mukaan *”rikoksen estämisellä tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa”*. Saman lain 5 luvun 1 §:n

⁵⁷ Ibid, s. 14.

⁵⁸ Helminen - Kuusimäki - Rantaeskola 2012, s. 11.

⁵⁹ Tiedonhankintalakityöryhmän mietintö 2015, s. 23.

3. momentti kuuluu seuraavasti: ”rikoksen paljastamisella tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty”.

Tämän päivän siviilitiedustelusta ja kansalliseen turvallisuuteen kohdistuvien uhkien torjunnasta vastaa suojelupoliisi, jonka tehtävät perustuvat sille annettuun ohjesääntöön (1.1.2014, Dnro 489/2013), jonka säädösperusteena ovat asetuksen tasoiset säädökset⁶⁰ ja poliisin hallinnosta annetun lakiin (14.2.1992/110) 10 §:ssä.⁶¹ Suojelupoliisin tehtävänä on sisäministeriön ohjauksen mukaisesti ”torjua sellaisia hankkeita ja rikoksia, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta, sekä suorittaa tällaisten rikosten tutkintaa. Sen tulee myös ylläpitää ja kehittää yleistä valmiutta valtakunnan turvallisuutta vaarantavan toiminnan estämiseksi”.⁶²

Koska poliisin hallinnosta annetun lain 10 § ei tarkemmin konkretisoi tarkemmin suojelupoliisin tehtäviä, antaa Poliisihallitus määräajoin määräyksen suojelupoliisin tehtävistä ja yhteistoiminnasta muun poliisin kanssa. Voimassa olevan määräyksen mukaan suojelupoliisin päätehtävät ovat:

- ”terrorismin torjuminen, ennalta estäminen ja paljastaminen,
- laittoman tiedustelutoiminnan torjuminen, ennalta estäminen ja paljastaminen,
- turvallisuustyö”.⁶³

Lisäksi suojelupoliisin tehtäviä ovat muun muassa:

- ”joukkotuhoojien leviämisen estäminen yhteistyössä muiden viranomaisten kanssa,
- valtion turvallisuusympäristön analysointi,
- kansallisen ja kansainvälisen tilannekuvan ylläpitäminen toimialallaan,
- valtion sisäiseen turvallisuuteen liittyvän laittoman aktivismin torjuminen, ennalta estäminen ja paljastaminen,
- toimialaansa kuuluvan turvallisuustiedustelun suorittaminen,
- eräiden toimialaansa kuuluvien rikosten tutkiminen”.⁶⁴

⁶⁰ Asetus poliisin hallinnosta, 15.3.1996/158 ja Valtioneuvoston asetus poliisista, 1080/2013.

⁶¹ Tiedonhankintalakityöryhmän mietintö 2015, s. 23.

⁶² Suojelupoliisin ohjesääntö 1 §.

⁶³ Tiedonhankintalakityöryhmän mietintö 2015, s. 24.

⁶⁴ Ibid, s. 24.

Hallituksen esityksessä (HE 346/2014 vp.) kuvataan melko laaja-alaisesti suojelupoliisin tiedonhankintaa ja turvallisuuden takaamiseksi suoritettavia toimia. Hallituksen esityksen mukaan suojelupoliisille määrättyjen tehtävien menestyksellinen suorittaminen edellyttää sen toimintavoilta tiedustelullista otetta. Säädettyjen tehtävien toteuttamisen edellytyksenä on Suomen turvallisuusympäristön aktiivinen ja laaja-alainen seuranta sekä ennakoiva tiedonhankinta. Suojelupoliisin tehtävänä on hankkia ja analysoida informaatiota, joka on valtion turvallisuusetuihin kohdistuvien uhkien ennalta estämisen kannalta välttämätöntä. Valtion turvallisuuteen kohdistuvista uhkista SUPO saa tietoa avoimista lähteistä, omalla operatiivisella toiminnalla, kotimaisilta yhteistyökumppaneilta ja ulkomaisilta turvallisuus- ja tiedusteluviranomaisilta. Suojelupoliisin kotimaan valtuuksista koskien salaisia tiedonhankintakeinoja ja pakkokeinoja on säädetty poliisilaissa (PoliisiL, 872/2011) ja pakkokeinolaissa (PKL, 806/2011). Suojelupoliisin tiedonhankintavaltuuksista ulkomailla ei ole laissa säädetty.⁶⁵

Puolustusvoimien tehtävät on säädetty puolustusvoimista annetussa laissa (551/2007), jonka 2 §:n mukaan puolustusvoimilla on kolme pääasiallista tehtävää: ”1) Suomen sotilaallinen puolustaminen, 2) muiden viranomaisten tukeminen ja 3) osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan ja sotilastehtäviin muussa kansainvälisessä kriisinhallinnassa”. Ensimmäisenä mainittuun tehtävään 2 §:n mukaan kuuluu muun muassa ”alueellisen koskemattomuuden turvaaminen, kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen sekä laillisen yhteiskuntajärjestyksen puolustaminen”.

Puolustusvoimien tärkeimpänä tehtävänä voidaan ajatella olevan alueellisen koskemattomuuden turvaaminen, joka on valtion suvereniteetin ja sen olemassaolon yksi tunnusmerkeistä. Suvereenin valtion on kyettävä kontrolloimaan rajoilla merkittyä aluettaan ja väestöään. Suomen kyky valvoa ja varmistaa alueellinen koskemattomuus asevoimin alueloukkauksilta liittyy hallituksen kykyyn ylläpitää toimivaa poliittista järjestelmää ja sen kykyyn tehdä ulkopoliittisia ratkaisuja.⁶⁶ Suomen alueellisen koskemattomuuden valvonnasta ja turvaamisesta on säädetty aluevalvontalaissa (18.8.2000/755) ja asetuksessa aluevalvonnasta (16.11.2000/971).

Hallituksen esityksessä Puolustusvoimista annetun lain 2 §:n yksityiskohtaisten perustelujen mukaan puolustusjärjestelmän avulla muodostetaan ja ylläpidetään sotilasstrategista tilannekuvaa, jota päätöksenteko edellyttää. Tarvittava tilannekuva luodaan HE:n kuvauksen mukaan tiedustelu- ja

⁶⁵ HE 346/2014 vp, s. 3.

⁶⁶ Saraviita 2011, s. 42

valvontajärjestelmällä, joka seuraa Suomen turvallisuusympäristössä tapahtuvaa kehitystä, tekee määrityksiä toimintaympäristömme muutoksista ja näin tuottaa tietoa sen hetkisestä tilanteesta.⁶⁷

3.4 Suojelupoliisin ja puolustusvoimien tiedonhankinta kotimaassa

Edellisessä kappaleessa lueteltujen tehtävien suorittamiseksi suojelupoliisin on kyettävä muun muassa hankkimaan tietoa laittomista ja valtion turvallisuutta vaarantavista hankkeista ja rikoksista. Tiedonhankintalakityöryhmän mukaan tunnusomaista tällaisilla hankkeilla ja rikoksilla on, että ne pyritään valmistelemaan julkisuudelta salassa. Näin ollen suojelupoliisin torjuntatoimien kohteeksi ei käytännössä juurikaan valikoidu julkisesti saatavilla olevaa tietoa. Jotta ei-julkisesti saatavien tietojen hankkiminen olisi tehokasta, on tiedonhankinta suoritettava salassa sen kohteelta. Poliisiviranomaisena tähän toimintaan suojelupoliisin käytössä ovat poliisilaissa säädetty salaiset tiedonhankintakeinot rikoksen estämiseksi ja paljastamiseksi.⁶⁸

PolL 5 luvussa säädetty salaiset tiedonhankintakeinot voidaan jaotella kolmeen pääryhmään luvun väliotsikointia seuraten:

1. *”Tiedonhankinta televerkoista:*

- *telekuuntelu*
- *tietojen hankkiminen telekuuntelun sijasta*
- *televalvonta*
- *tukiasematietojen hankkiminen.*

2. *Tarkkailutyypiset keinot:*

- *suunnitelmallinen tarkkailu*
- *peitelty tiedonhankinta*
- *tekninen tarkkailu, joka jakautuu seuraaviin tarkkailulajeihin:*
 - *tekninen kuuntelu*
 - *tekninen katselu*
 - *tekninen seuranta ja*
 - *tekninen laitetarkkailu*
- *telesoitteen ja telepäätelaitteen yksilöintitietojen hankkiminen.*

3. *Erityiset salaiset tiedonhankintakeinot:*

- *peitetöiminta*
- *valeosto*
- *tietolähteen ohjattu käyttö*
- *valvottu läpilasku.”⁶⁹*

⁶⁷ HE 264/2006 vp, s. 17 -18.

⁶⁸ Tiedonhankintalakityöryhmän mietintö 2015, s. 26 – 27.

⁶⁹ Helminen-Kuusimäki-Rantaeskola 2012, s. 398.

Poliisilain 5 luvun 3 §:ssä määritellään kaikki ne rikokset, joiden paljastamiseksi voidaan käyttää laissa tarkoitettua salaista tiedonhankintaa:

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

Nämä PoIL 5:3 mukaiset rikokset ovat lähes yhtenevät suojelupoliisille määrättyjen tehtävien kanssa, varsinkin terrorismin ja laittoman tiedustelutoiminnan ennalta estämisen ja paljastamisen kanssa.

Lohsen mukaan valtion turvallisuutta vaarantavia hankkeita ovat muun muassa toisten valtioiden harjoittama valtakunnallisesti merkityksellisten Suomessa olevien kohteita vastaan suunnattu vakoilu niin reaali maailmassa kuin tietoverkoissa. Tällaisesta toiminnasta hankittavaa tiedonhankintaa kutsutaan vastavakoiluksi. Tämän puolustuksellisen toiminnan mahdollistaa edellä luetellut PoIL 5 luvussa säädetyt salaiset tiedonhankintakeinot, joiden käytön yleisenä edellytyksenä on, että niillä oletettavasti voidaan saada rikoksen *estämiseksi tai paljastamiseksi* tarvittavia tietoja (PoIL 5:2.1). Salaiset tiedonhankintakeinot ovat Lohsen mukaan paitsi rikoslähtöisesti määriteltäviä, myös personoituja toimivaltuuksia. Niitä voidaan käyttää vain kun rikostiedustelutietojen, tarkkailuhavaintojen, muiden vihjetietojen tai kun rikosanalyysin perusteella on muodostettu perusteltu epäily kohdehenkilön syyllistymisestä rikokseen. Mikäli tällaista tiettyyn henkilöön liittyvää rikostorjuntaperustetta ei ole tullut tietoon, salaisten tiedonhankintakeinojen käyttö ei ole sallittua.⁷⁰

Suojelupoliisin hallinnollisen asemaa ollaan muuttamassa. Sitä ollaan siirtämässä Poliisihallituksen alaisuudesta suoraan sisäministeriön alaiseksi poliisiyksiköksi. Suojelupoliisin hallinnollista asemaa selvittäneen työryhmän mukaan hallinnon siirrolla sisäministeriön alaisuuteen osaltaan vahvistettaisiin suojelupoliisin toimintaan kohdistuvaa poliittisten toimijoiden strategista ohjausta.

⁷⁰ Lohse 2015, s. 765.

Lisäksi siirto selkeyttäisi työryhmän mukaan suojelupoliisin asemaa sekä kotimaisessa viranomaiskentässä että kansainvälisessä turvallisuus- ja tiedustelupalveluiden välisessä yhteistyössä. Työryhmän näkemyksen mukaan nykyisessä ohjausmekanismissa suojelupoliisin on katsottu olevan turhan etäällä turvallisuuspoliittisista päätöksentekijöistä. Kaavailtu muutos kaventaisi tätä etäisyyttä ja selkeyttäisi suojelupoliisin suoria yhteistyö- ja raportointisuhteita turvallisuudesta vastaaviin päätöksentekijöihin. Muutoksella lisättäisiin myös valtiojohdon mahdollisuuksia vaikuttaa suojelupoliisin tiedonhankinnan suuntaamiseen, minkä tavoitteena on parantaa SUPO:n kykyä tuottaa sisäistä turvallisuuttamme ja ulko- ja turvallisuuspoliittista päätöksentekoa tukevaa tietoa.⁷¹ Edellä luetellut toimet suojelupoliisin hallinnollisen aseman muuttamisesta olisivat merkittäviä parannuksia osana suojelupoliisin parlamentaariseen ohjaukseen ja valvontaan.

Suojelupoliisin hallinnollista asemaa ja valvonnan kehittämistä selvittäneen työryhmän loppuraportissa käsiteltiin myös kysymystä suojelupoliisin tiedonhankintatoimivaltuuksien laajentamisesta koskemaan hankkeiden torjuntaa. Suojelupoliisin tulee pystyä vastaamaan toimintaympäristönsä muutokseen, joka vaatisi työryhmän näkemyksen mukaan uusia tiedustelullisia toimivaltuuksia. Näiden uudenlaisten tiedustelutoimivaltuuksien avulla olisi tarkoitus hankia valtakunnan turvallisuutta vaarantavien hankkeiden torjumiseksi tarpeellista tietoa henkilöiltä (tietolähde) ja tietoverkoista, tilanteessa, jossa hankkeet eivät vielä olisikaan edenneet estettävän, paljastettavan tai selvitetävän rikoksen asteelle.⁷²

Tiedonhankintalakiyöryhmä jakaa puolustusvoimien harjoittaman tiedonhankinnan kahteen osaluueeseen; sotilastiedusteluun ja sotilasvastatiedusteluun. Sotilastiedustelun kohteena on Suomen ulkopuolinen toimintaympäristö, kun taas sotilasvastatiedustelutoimintaa harjoitetaan Suomen alueella. Sotilasvastatiedustelussa on kyse maamme sotilaalliseen puolustukseen kohdistuvan laittoman tiedustelutoiminnan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta ehkäisemisestä ja paljastamisesta. Pyrkimyksenä on estää ulkovaltojen tiedonhankinta Suomessa esimerkiksi puolustusvoimien suorituskyvystä ja kokoonpanosta.⁷³

Puolustusvoimien sotilasvastatiedustelutehtävästä säädetään sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa. Puolustusvoimien toimivaltaa koskevien säännösten rikosten

⁷¹ Tiedonhankintalakiyöryhmän mietintö 2015, s. 25.

⁷² Sisäministeriön julkaisu 28/2014. Kuvailulehti.

⁷³ Tiedonhankintalakiyöryhmän mietintö 2015, s. 29.

ennalta estämiseksi ja paljastamiseksi ovat suojelupoliisin vastaavia säännöksiä rajatumpia. Ne koskevat vain sellaisia rikoksia, jotka kohdistuvat sotilaallisen maanpuolustuksemme tiedustelutoimintaan ja liittyvät sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan.⁷⁴

3.5 Suojelupoliisin ja puolustusvoimien ulkomaita koskeva tiedonhankinta

Tiedonhankintalakityöryhmän näkemyksen mukaan ulkomaita koskevilla tiedoilla on yhä suurempi merkitys, koska Suomen turvallisuusympäristö on viimeisten vuosikymmenten aikana voimakkaasti kansainvälistynyt. Suojelupoliisin tehtävistä annetussa määräyksessä on useita tehtäviä, jotka liittyvät ulkomaista alkuperää olevien uhkien torjuntaan kansainvälisen tilannekuvan muodostamiseen ja raportointiin. Suojelupoliisin tiedonhankintatoimivaltuuksia rikoksen estämiseksi ja paljastamiseksi voidaan käyttää vain Suomen alueella. Suojelupoliisin tiedonhankinnasta ulkomailla ei ole säädetty.⁷⁵

Tästä johtuen on suojelupoliisin vierasvaltioita ja muita ulkomaisia toimijoita koskeva tiedonhankinta ja -saanti pitkälti kansainvälisen tiedusteluyhteistyön, avointen lähteiden seuraamisen sekä sen oman yhdyshenkilötoiminnan varassa. Suojelupoliisilla ja sen edeltäjillä on pitkä historia laajasta kahdenvälisestä (bilateraali) ja monenvälisestä (multilateraali) yhteistyöstä ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa. Tiedusteluyhteistyön pyrkimyksenä on varmistaa, että Suomen turvallisuusviranomaisilla on käytössään valtion turvallisuuden takaamiseksi tarvittavia ulkomaisia tiedustelutietoja. Turvallisuuskysymykset ovat nykyään vaikutuksiltaan globaaleja, jonka seurauksena ulkomaisten tiedustelutietojen merkitys on korostunut entisestään. Tästä kehityksestä johtuen suojelupoliisi onkin viime vuosina määrätietoisesti pyrkinyt kasvattamaan kansainvälistä yhteistyöverkostoaan, joka tällä hetkellä pitää sisällään kaikkien turvallisuutemme kannalta olennaisten maiden tiedustelu- ja turvallisuuselimet.⁷⁶ Suojelupoliisi on ollut 1990-luvulta alkaen jäsenenä ns. Bernin klubissa, jonka jäseniä ovat pääasiassa turvallisuuspalvelut. Suojelupoliisin yhteistyöverkosto on melko mittava, siihen kuuluu noin 80 ulkomaista turvallisuuspoliisi-, turvallisuuspalvelu- ja tiedustelupalveluviranomaista.⁷⁷

Suojelupoliisilla on nykyisin yhdyshenkilöitä sijoitettuna eräisiin Euroopan ulkopuolisiin maihin. Yhdyshenkilöiden toimipaikkana toimii paikallinen Suomen suurlähetystö, ja heillä on diplomaattisen edustajan asema sen tuottamin oikeuksin ja erivapauksin. Yhdyshenkilöiden tehtävänä

⁷⁴ Ibid. s. 29 – 30.

⁷⁵ Tiedonhankintalakityöryhmän mietintö 2015, s. 31.

⁷⁶ Ibid. s. 32.

⁷⁷ Sisäministeriön julkaisu 28/2014, s. 29.

on osallistua Suomen kansalliseen turvallisuuteen kohdistuvien ulkoisten uhkien torjuntaan. Tämän tehtävän hoitamiseksi heidän tulee pitää yhteyttä sijoitusmaan sekä siellä edustettuina olevien muiden maiden turvallisuusviranomaisiin. Lainsäädännöllisesti yhdyshenkilöiden toiminta perustuu poliisin kansainvälistä tietojenvaihtoa ja henkilötietojen käsittelystä poliisitoimessa annetun lain säännöksiin.⁷⁸ Ulkomaita koskevan tiedustelun osalta oma roolinsa on myös tietojenvaihdolla Euroopan unionin tiedusteluanalyysikeskuksen kanssa.⁷⁹

Kuten edellä on todettu, kohdistuu sotilastiedustelu Suomen ulkopuoliseen toimintaympäristöön ja sen kohteena ovat pääosin valtiolliset toimijat. Puolustusvoimien tärkeimmän tehtävän, valtakunnan itsenäisyyden ja alueellisen koskemattomuuden puolustaminen, on katsottu sisältävän sotilastiedustelutoiminnan, vaikka sitä ei ole erikseen mainittu puolustusvoimista annetun lain 2 §:ssä. Sotilaallinen päätöksenteko edellyttää oikea-aikaista ja faktoihin perustuvaa sotilasstrategista tilannekuvaa, jonka luomiseksi sotilastiedustelun on 1) seurattava Suomen turvallisuusympäristössä tapahtuvaa kehitystä, 2) määritettävä ympäristön muutokset ja 3) tuotettava tietoa vallitsevasta tilanteesta.⁸⁰

Sotilastiedustelun tiedonhankintatoimivaltuuksista ei ole säädetty lailla, niistä on annettu erilliset määräykset ja ohjeet puolustusvoimien sisällä. Osa tarvittavasta sotilastiedustelutiedosta saadaan Suomen ulkomailla sijaitseviin edustustoihin sijoitetuilta puolustusasiamiehiltä, jotka hankkivat kaikin laillisin keinoin tietoa kohdevaltion oloista ja tapahtumista. Kuten suojelupoliisikin, tekee myös puolustusvoimat sotilastiedustelun vaatimaa yhteistyötä ulkomaisten tiedusteluviranomaisten kanssa, tarkoituksena saada puolustusvoimien käyttöön tarpeellista ulkomaista tiedustelutietoa.⁸¹

3.6 Kansainvälinen tiedusteluyhteistyö

Niin kauan kun ollut rajoja – erottaen kansoja, kulttuureja ja talouksia – on ollut myös yhteistyötä ja konflikteja, joilla toimijat ovat halunneet siirtää näitä rajoja. Kun kansallisvaltiosta tuli vallitseva poliittinen kokonaisuus ja toimija, joutuivat ne aika-ajoin sovittamaan omaa toimintaansa tavoitellakseen muiden valtioiden kanssa yhteisiä päämääriä, mikä synnytti kansainvälisen yhteistyön käsitteen.⁸²

⁷⁸ Tiedonhankintalakityöryhmän mietintö 2015, s. 31 – 32.

⁷⁹ Sisäministeriön julkaisu 28/2014, s. 29.

⁸⁰ Tiedonhankintalakityöryhmän mietintö 2015, s. 32.

⁸¹ Ibid. s. 32.

⁸² Fägersten 2010, s. 47.

Tiedustelu on kansainvälistä toimintaa, joka on integroitumassa ja verkostoitumassa muiden kansainvälisten toimintojen tapaan. Globalisoituvassa maailmassa ja varsinkin yhdentyvässä Euroopassa tiedustelupalvelujen toiminnan perustana ei enää voi olla vain kunkin valtion omat kansalliset intressit. Kansallisten tavoitteiden tulee palvella myös erilaisten liittoutumien etua. Laajentuvassa Euroopan unionissa jäsenmaat joutuvat vastaamaan turvallisuusympäristön muutoksiin ja organisoimaan tiedusteluelimensä uudelleen. Yhteistyö YK:n ja Etykin tiedustelu- ja analysointiyksiköiden kanssa asettaa tiedustelutoiminnalle myös uudenlaisia tavoitteita.⁸³

Vuosikymmenien saatossa suojelupoliisi on omasta mielestään onnistunut luomaan toimivan yhteistyön sellaisten kansainvälisten turvallisuus- ja tiedustelupalvelujen kanssa, joita voidaan pitää keskeisinä toimijoina tiedustelun saralla. Yhteistyötä tekee merkittävän se, että suojelupoliisi on ainoa siviili- ja poliisiviranomaisemme, jolla on toimivat kanavat yhteistyön ja tiedonvaihdon mahdollistamiseen ulkomaisten tiedustelu- ja turvallisuuspalveluiden kanssa. Kansainvälisellä yhteistyöllä ja tehokkaalla tiedonvaihdoilla on SUPO:n mukaan nykyisin erityisen merkittävä rooli tiedustelutoiminnassa, ja heidän mukaan sen merkitys tulee tulevaisuudessa vielä kasvamaan. Pelkästään kansainvälisen yhteistyön keinoin on SUPO:n mukaan kuitenkin vaikea puuttua yhteiskuntamme kehityskulkuihin. Turvallisuus- ja tiedustelupalveluiden työnjaon väliset erot maailmalla ovat hämärtyneet. Tämä muutos näkyy siten, että sisäisten uhkien torjunnasta vastaavat turvallisuuspalvelut tekevät lisääntyvässä määrin kansainvälistä yhteistyötä torjuakseen myös ulkomaisperäisiä uhkia. Ulkomaan tiedustelusta vastaavat tiedustelupalvelut toisaalta nykyään keräävät ulkomailta myös valtion sisäisiä turvallisuusuhkia koskevia tietoja.⁸⁴

Pienten maiden kuten Suomen tiedustelusta vastaavat organisaatiot eivät enää nykymaailmassa kykene toimimaan täysin itsenäisesti. Syitä tähän on useita, mutta suurin syy on tehokkuus. Kaikkea tietoa ei yksinkertaisesti pystytä itse edes hankkimaan ja saatikka analysoimaan: sähköisen viestinnän yleistyttyä myös tiedon määrä on kasvanut merkittävästi. Koska mikään kansainvälinen tiedusteluelin ei voi enää toimia ilman liittolaisia, lisääntyy kansainvälinen yhteistyö jatkuvasti ja edelleen.⁸⁵

⁸³ Paul 2005, s. 67.

⁸⁴ SUPO:n vuosikirja 2015, s. 5, 13, 9 ja 17.

⁸⁵ Paul 2005, s. 67.

Jan-Peter Paul'in näkemys yhteistyön suurimmasta syystä – tehokkuuden vaatimuksesta - pitänee ainakin osaltaan paikkaansa, mutta nykyhetken suurimpana tiedusteluyhteistyön syynä ainakin itse näkisin olevan kansallisvaltioihin ja niiden kansalaisiin kohdistuvien uhkien yhä kansainvälistyvä ja rajat ylittävä luonne. Varsinkin kansainvälinen terrorismi ja terrori-iskuissa on ollut viime vuosina nähtävissä valtioiden rajat ylittäviä piirteitä niin iskujen toteuttajien, valmisteluiden ja kohteiden valinnan osalta. Useista eri kansalaisuuksista koostuvat iskujen tekijät värvätään valtiossa A. Heidät koulutetaan (yleensä) sodan runteleman ja vailla toimivaa hallintoa olevan valtion B alueella, jonka jälkeen terrori-isku toteutetaan kohdemaassa C. Lisänä tähän kuvioon voidaan ottaa - korostamaan toiminnan rajat ylittävää luonnetta - kaikkien edellä lueteltujen vaiheiden rahoittajatahot, joita voi olla useita yksilöitä eri lähdemaista tai esimerkiksi yksi erillinen järjestö tai valtio. Näin ollen tiedusteluyhteistyön kautta saatavan tiedon varassa eivät ole pelkästään Suomen kaltaiset pienet ja rajallisilla tiedusteluresursseilla toimivat valtiot, tätä yhteistyötä tarvitsevat yhtäläillä myös tiedustelun suurvallat kuten Yhdysvallat, Britannia ja Ranska.

Kuten aiemmin viittasin *professori Richard J. Aldrich*'in näkemykseen, jonka mukaan on toistuvasti voitu havaita, että tiedustelu on 2000-luvun alusta lukien ollut merkittävämmässä roolissa maailman politiikassa kuin se on koskaan aiemmin ollut. Globaalin epävarmuuden ympäristössä tehokas tiedustelu on keskeistä varsinkin terrorismin, organisoituneen rikollisuuden, separatististen uhkien ja laittoman asekaupan vastaisessa toiminnassa. Yleisesti onkin tiedostettu, että tämä toiminta vaatii laajempaa konsensusta. Kiihtyvää ja kasvavaa kansainvälistä tiedusteluyhteistyötä onkin pidetty tiedustelualan tärkeimpänä muutoksena viime vuosikymmeninä. Usein muutosta perustellaan yksittäisillä tapahtumilla kuten 9/11 –terrori-iskulla New Yorkissa vuonna 2001, mutta kasvavan yhteistyön taustalla on myös laajempi ilmiö – globalisaatio. Pidemmälle meneväksi syyksi on esitetty turvallisuusuhkien muuttunut ja yhä muuttuva luonne kahden viimeisten vuosikymmenten aikana. Uhkakuvien muutos on vaatinut laajempaa jakamisen toimintamallia, vaikka se ei olekaan vaivattomasti sopinut perinteiseen tiedustelukäytäntöön, jossa korostetaan varovaisuutta jaettaessa arkaluonteista tietoa.⁸⁶

Mitä tahansa yhteistyötä suunniteltaessa tulee osapuolten aina punnita yhteistyön tuomia etuja ja siitä mahdollisesti syntyviä haittoja tai riskejä sekä sitä ketkä ovat tulevan yhteistyön osapuolia. Tämä punninta on syytä suorittaa huolimatta siitä, mitä yhteistyö koskee ja missä toimintaympäristössä sitä on ajateltu tehtäväksi. Edellä oleva punninta koskee myös tiedusteluyhteistyötä.

⁸⁶ Aldrich 2011, s. 18 – 19.

Vaikka kansainvälisestä tiedusteluyhteistyöstä on lukuisia erilaisia näkemyksiä, ovat valtioiden intressit kuitenkin perusteellisimmin käsitelty alue asiaa koskevassa kirjallisuudessa. Yksi tapa muodostaa itselleen käsitys tästä diskurssista, on valtioiden motiivien ryhmittely yleisimpiin kategorioihin. Valtioiden tiedusteluyhteistyöhön liittyvät pääasialliset intressit voidaan esittää lyhyesti vaihtokaupan yksinkertaisella kaavalla: hyötyjen tavoittelu (tiedustelu ja poliittinen intressi) samanaikaisesti haittoja minimoiden (autonomia, suvereniteetti ja haavoittuvuus).⁸⁷

Tavoiteltaessa yhteistyön kautta hyötyjä tiedustelutoiminnassa (”tiedusteluhyöty”), keskeinen motivaatio mille tahansa valtiolle on tiedustelukapasiteetin lisääminen tai saman kapasiteetin tuottaminen alemmilla kustannuksilla. Tyypillisiä tiedusteluhyötyjä ovat; pääsy sellaisiin lähteisiin, joihin ei muuten ole pääsyä, menet, teknologia tai informaatio.⁸⁸

Vaikka useimmat yhteistyön muodot perustellaan kapasiteetin lisäämisellä, ei tämä aina kuitenkaan ole peruste kaikissa tapauksissa. Tiedusteluhyötyjen sijaan valtioilla voi olla yhteistyön motiivina enemmänkin se, mitä yhteistyö merkitsee instituutioille, joissa yhteistyö tapahtuu tai niille toimijoille, jotka ottavat osaa yhteistyöhön. Tiedusteluammattilaisten preferenssit yhteistyölle voivat olla toissijaisia poliittisille tai sotilaallisille välttämättömyyksille, jos tiedusteluyhteistyön tavoitteena on vahvistaa tai panna alulle poliittista tai sotilaallista yhteistyötä. Tällaisia yhteistyön tavoitteita Fägersten kutsuu ”poliittisiksi intresseiksi”. Yhteistyön tavoitteena voi olla esimerkiksi poliittisten tai taloudellisten etujen saaminen vastineeksi tiedustelutietojen jakamisesta. Tiedustelutietojen jakamisen tarkoituksena voi olla myös pyrkimys vaikuttaa sotilaalliseen konfliktiin tai liittolaisen puolustuksen ryhmitäksen ja aseman parantaminen. Joissain tapauksissa tiedusteluyhteistyöllä voidaan korvata poliittisia ja diplomaattisia suhteita, mikäli sellaisia ei ole tai niitä ei jostain syystä voida ylläpitää. Joskus tiedusteluyhteistyöllä voi olla vain symbolinen tarkoitus (poliittinen intressi): kahden välisellä yhteistyösopimuksella halutaan esimerkiksi parantaa tai korjata maiden välisiä suhteita, vaikka sopimuksella käytännössä on tietojenvaihdon kannalta vain hyvin vähäinen merkitys.⁸⁹

Jos valtiot Suomi mukaan lukien voivat lisätä tiedustelukapasiteettiaan yhteistyöllä, miksei tiedusteluyhteistyö ole sitten riittävä toimintamuoto tiedustelualalla? Fägerstenin mukaan tähän on

⁸⁷ Fägersten 2010, s. 83 – 84.

⁸⁸ Ibid, s. 84.

⁸⁹ Ibid, s. 84 – 85.

kaksi ilmeistä vastausta. Valtiot ensinnäkin puolustavat vankkumattomasti *autonomiaan ja suvereniteettiaan*, ja ne vastustavat kiihkeästi kaikkea, joka voi heikentää niiden valtaa. Autonomian ja suvereniteetin heikkenemisen lisäksi kaikilla valtiolla on suuri intressi välttää *haavoittuvuutta*.⁹⁰

Autonomian ja suvereniteetin nimissä valtiot suojelevat niiden sisäistä määräysvaltaa ja kontrollia sisä- ja ulkopolitiikkaan. Valtiot ovat epäluuloisia toisiaan kohtaan ja pelkäävät oikeudenloukkauksia, joten ne vastustavat voimakkaasti suvereniteettinsa vähäistäkin siirtymistä omista käsistään. Suvereniteettia heikentävät tapaukset ovat ilmeisiä tiedustelualalla, jos valtioiden välinen voimatasapaino on epäsuhtainen ja suhde perustuu pitkälle ulottuvaan yhteistyöhön. Näissä tapauksissa autonomian ja suvereniteetin vähentyminen koskee omistusta tai kontrollia tiedusteluaineistoon, joka liittyy valtion strategiaan intresseihin. Toisena esteenä tiedusteluyhteistyölle on autonomia tai paremminkin sen puute, toisin sanoen rasite pakollisesta osallistumisesta toimenpiteisiin, jotka eivät kuulu toimijan omiin intresseihin. Tiedusteluyhteistyön muodosta ja osapuolista siis riippuu kuinka paljon kumppanit (tai toinen niistä) menettävät suvereniteettiaan ja autonomiaansa. Tiedustelutiedon kerääminen ja sen jakaminen ovat vähinten menetyksiä ja vahinkoja aiheuttavia toimia yhteistyön saralla.⁹¹ Näin ollen eniten negatiivisia vaikutuksia yhteistyöstä voi syntyä siis yhteisestä tiedustelutoimien suunnittelusta, tietojen käsittelystä ja sen analysoinnista.

Valtion *haavoittuvuudella* tässä kontekstissa tarkoitetaan todennäköisyyttä ja seurauksia sen metodien ja lähteiden paljastumisesta tai pelkoa yhteistyökumppanin kuuliaisuuden ja luottamuksen pettämisestä tai pahimmassa tapauksessa loikkaamista niin sanotusti toiseen leiriin. Tiedustelualaan perehtyneet tutkijat ovat listanneet useita erilaisia skenaarioita, joissa valtioiden haavoittuvuus lisääntyy tiedusteluyhteistyön seurauksena. Ensiksikin, yhteistyöjärjestelyiden paljastuminen voi olla poliittisesti kiusallista varsinkin, jos yhteistyöllä ”ulkoistetaan” tiedustelutehtäviä, jotka eivät ole sallittuja kotimaassa. Toiseksi, yhteistyö voi saada aikaan ”kierrätysongelman”, jossa tiettyä tiedustelutietoa jaetaan useiden kumppanien välillä niin pitkään kunnes, jokin valtio pitää sitä luotettavampana ja uskottavampana kuin se muutoin olisi, vain siksi, että tietoa tukevat useat riippumattomat tahot. Kolmanneksi, yhteistyö voi aiheuttaa hankitun tiedustelutiedon kontrollin menettämisen. Toisin sanoen, kumppanille jaettu tiedustelutieto voi välittyä kolmannelle osapuolelle tai sitä voidaan käyttää tavoilla, jotka eivät ole sen alkuperäisen lähteen intressissä. Tiedustelutiedon kontrollinen menettäminen ei pelkästään tarkoita sen substanssia, vaan myös sen lähteet ja käytetyt

⁹⁰ Fägersten 2010, s. 85, 87.

⁹¹ Ibid, s. 85 – 86.

menetysmetodit sen saamiseksi voivat olla loukkauksen kohteena. Lisäksi korkeantason riippuvuussuhteessa yhteistyökumppanit oppivat tuntemaan toistensa vahvuudet ja heikkoudet, mikä saattaa vaikuttaa valtion strategiseen tilanteeseen negatiivisesti.⁹²

Yhteistyöstä mahdollisesti aiheutuvista riskeistä ja haitoista tai menetyksistä huolimatta tiedusteluyhteistyötä kuitenkin harjoitetaan, koska negatiivisia vaikutuksia ei aina voida ennakoinnista huolimatta kokonaan poistaa. Mikään valtio ei tämän päivän muuttuvassa ja globalisoituneessa maailmassa ole myöskään täysin omavarainen ja riippumaton tiedustelun kaikilla osa-alueilla. Edellä olevan perusteella voidaankin todeta tiedusteluyhteistyön valtioiden turvallisuus- ja tiedusteluorganisaatioiden välillä olevan ainakin jollain tasolla tarpeellista ellei välttämätöntä, ja se onkin lisääntynyt mahdollisista negatiivisista vaikutuksista huolimatta.

4 Turvallisuuden takaaminen tiedustelun keinoin ja perusoikeuksien vaatimukset

4.1 Turvallisuus ja sitä uhkaavat tekijät muuttuvassa ympäristössä

Kuten edellä on todettu kansallisen turvallisuuden osalta sen määrittelyn vaikeus, sama vaikeus koskee myös turvallisuutta, jota on monenlaista ja se voidaan määrittellä monesta näkökulmasta. Turvallisuutta voidaan tarkastella subjektiivisesti, koska sen voidaan ajatella olevan henkilökohtainen tunnetila. Virran mukaan turvallisuuden ”määritelmät ovat usein dikotomioita (kuten subjektiivinen/objektiivinen), toimijan tai kohteen mukaisia (mikä, minkä, kenen), vastakohtien kautta esitettyjä (uhka, riski, vaara, onnettomuus, katastrofi, turvattomuus) tai hallinnon ja politiikan funktionaalisia määritelmiä (sisäinen, ulkoinen, kansallinen, globaali turvallisuus)”.⁹³ Turvallisuuden määrittelemisen vaikeus perustuu juuri siis määrittelynäkökulmien tarjoamiin lähes loputtomiin mahdollisuuksiin sen sisällöstä, eikä oikeaa ja yhtä määritelmää voida ajatella olevan olemassa.

Limnellin mukaan turvallisuutta käsitteenä voidaan lähestyä vaihtoehtoisilla tavoilla. *Turvallisuus* sisältää hänen mukaan runsaasti erilaisia merkityksiä ja mielikuvia niin siihen liittyvistä oloiloista kuin keinoista sen saavuttamiseksi. Turvallisuudesta onkin muodostunut eräänlainen yleiskäsite, jossa on jokaiselle jotain ja sen avulla voidaan tavoitella kaikkea tärkeää. Toisaalta turvallisuuskäsite

⁹² Fägersten 2010, s. 87.

⁹³ Virta 2012, s. 122.

on nähty käyttökelttomaksi kyseenalaistamalla koko sen olemassaolo. Nämä näkemykset Limnellin mukaan viittaavatkin käsitettä käyttävien eri tahojen kasvaneeseen haluun käyttää ”turvallisuuatta” omien intressiensä ajamiseen. Vaikka turvallisuuden sisällöstä onkin lähes mahdotonta päästä yhteisymmärrykseen, mahdollistaa turvallisuuden käsitteen kiistanalaisuus sen eri ulottuvuuksien huomioon ottamisen, eikä turvallisuudesta näin ollen muodostu liian hallitsevaa vain tietyn katsantokannan mukaista toimintamallia. On ymmärrettävä, että turvallisuusdiskurssin tulee olla sisällöllisesti avointa ja prosessisina jatkuvaa, jotta sen on mahdollista uusiutua ajan hengen mukaisesti. Limnellin mukaan juuri turvallisuuden epämääräisyys ja suhteellisuus mahdollistaa sen tehokkaan käytön politiikan teon välineenä toimintaympäristössä, jossa tulisi käsitteen määrittelyn sijaan keskittyä niihin tulkintoihin ja tavoitteisiin, joita toimijat esittävät turvallisuuden nimissä. Tähän pitäisi keskittyä nykyään varsinkin siksi, että useat asiat helposti liitetään turvallisuuteen kuuluviksi.⁹⁴

Yhteiskunnassa yksilöiden turvallisuuden tunteeseen Limnellin mukaan voidaan ja pitääkin pyrkiä vaikuttamaan aktiivisesti, rehellisin ja oikein tiedoin. Kansalaisille on kerrottava avoimesti yhteiskunnan vahvuuksista ja heikkouksista kohdata erilaisia uhkia ja poikkeustilanteita. Kansalaisten luottamus yhteiskunnan selviytymiskykyyn ja tietoisuus omasta selviytymiskyvystä luo hänen mukaan turvallisuuden tunnetta ja synnyttää luottamusta kanssaihmiisiin ja koko yhteiskuntaan.⁹⁵ Turvallisuuatta horjuttaa siis *pelko* jostain olemassa olevasta tai kuvitellusta uhasta tai vaarasta, joka on riski turvallisuuden säilymiselle. Ilman tuota pelkoa voidaan ajatella olevan turvallista. Sellaista tilannetta ja ajanjaksoa ei varmaan ole koskaan ollutkaan, jossa joku ei pelkäisi jotain uhkaa, joka horjuttaa turvallisuuden tunnetta. Turvallisuus on siis tunne, mutta tähän tunteeseen vaikuttavat myös ympäröivät olosuhteet, jotka muuttuvat. Esimerkiksi ajasta ja paikasta johtuvat muuttuvat olosuhteet tekevätkin turvallisuuden määrittelemisestä vaikeaa ja ongelmallista.

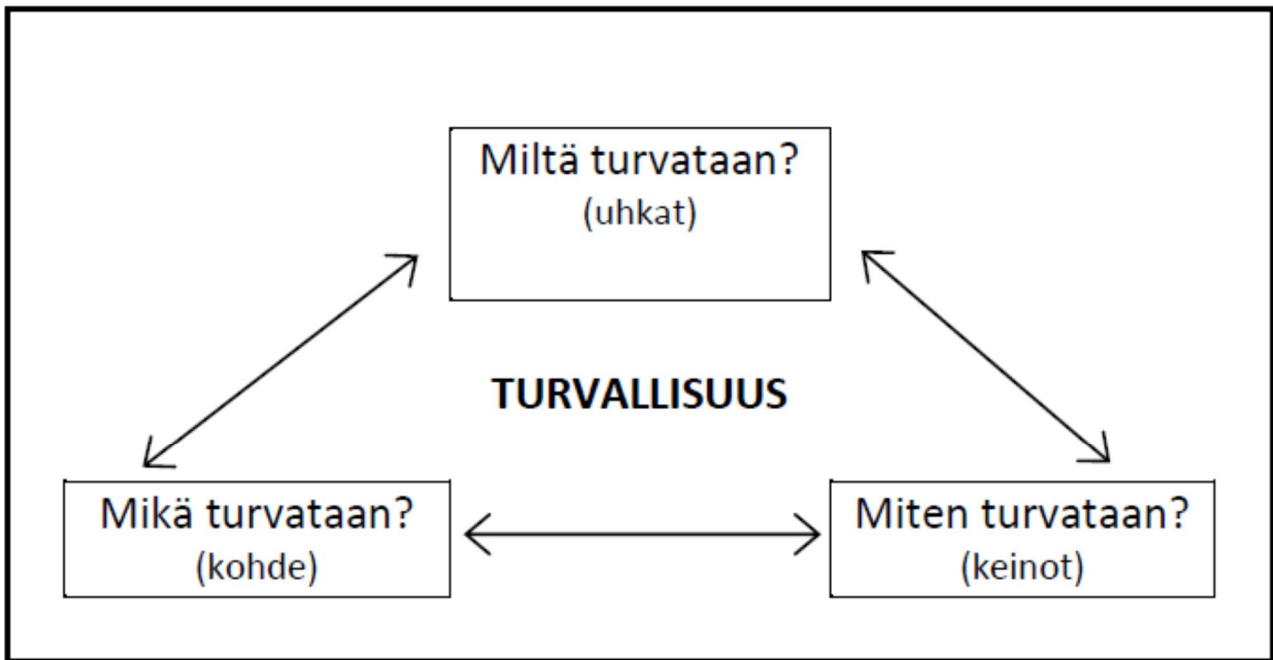
Turvallisuuden diskurssit ovat Limnellin mukaan historiallisten sosiaalisten prosessien ja rakenteiden tuotteita, joilla voidaan paikallistaa turvallisuuden käsitteellistämistä. Turvallisuuden määrittelyä ja muutosta koskevaa akateemista ja poliittista keskustelua on hallinnut 1980 –luvun alusta lukien pääasiassa kolme diskurssia.⁹⁶

⁹⁴ Limnell 2009, s. 43 – 44.

⁹⁵ Limnell 2011, s. 291.

⁹⁶ Limnell 2009, s. 45.

Kaavio 2. Turvallisuuden diskurssiulottuvuudet.⁹⁷



1) Ensimmäinen turvallisuuden määrittämisen edellytys koskee turvaamisen kohdetta – kenen turvallisuudesta on kysymys, *mikä / mitä pyritään ensisijaisesti turvaamaan?* Kohteen ytimessä ovat sen pääasialliset arvot, joiden turvaaminen nostetaan turvallisuuskurssissa kohteen turvallisuuden suhteen ensiarvoisimmiksi.

2) Toinen turvallisuuskurssin ulottuvuus koskee turvattavan kohteen turvallisuuden suhdetta johonkin – *mikä uhkaa* määritetyn kohteen turvallisuutta? Tässä korostuu turvallisuuden ymmärtämisen uhkakeskeisyys, jossa uhka nähdään turvallisuuden kontrastina ja välttämättömänä elementtinä määriteltäessä turvallisuutta.

3) Kolmas ulottuvuus liittyy keinoihin ja toimenpiteisiin, joita esitetään toimeenpantavaksi turvattavan kohteen suojelemiseksi niiltä uhkatekijöiltä, jotka vaarantavat kohteen turvallisuuden. *Miten (millä keinoin) turvattavan kohteen turvallisuus taataan?* Tämä lähtökohta edellyttää myös kysymään – *kuka vastaa turvallisuuden tuottamisesta?*⁹⁸

Turvallisuuden arviointiin liittyy kiinteästi sen vastineparina uhka ja riski. On siis arvioitava riskejä ja uhkia, jotka voivat muuttaa turvallisuuden tasoa. On selvää, että ihmiset ja sen muodostamat yhteisöt, sekä ihmiskunta kokonaisuutena, ovat aikojen alusta asti olleet alttiina erilaisille vaaroille,

⁹⁷ Linnéll 2009, s. 46.

⁹⁸ Ibid, s. 46.

uhkille ja riskeille. Absoluuttista turvaa ei voida ajatella olevan olemassa, vaan turvallisuudessa/turvattomuudessa on eri tasoja. Olemassa olevan senhetkisen turvallisuustilanteen kanssa pitää tulla toimeen. Voimme omilla toimilla pyrkiä vaikuttamaan turvallisuuden tilaan sitä parantaen, mutta huonoilla valinnoilla voimme myös heikentää sitä.

Turvallisuuskeskustelussa painottuvat eri asiat ja turvallisuutta uhkaavat tekijät nähdään eri tavalla. Toisen turvallisuus on jo toiselle turvattomuutta. Toiselle turvallisuutta lisäävät toimet voivat synnyttää toisessa turvattomuuden tunteen, esim. raskaasti aseistetut poliisit katukuvassa. Toinen ajattelee olevansa turvassa, koska poliisin pelkkä läsnäolo turvaa häntä, mutta toinen näkee tämän osoituksena turvallisuuden heikkenemisestä, joka synnyttää hänessä turvattomuuden tunteen. Turvallisuuden määrittelemisen vaikeus yhdistyy turvallisuuden suhteellisuuteen – milloin olemme turvassa ja miltä uhkalta?

Vaikka turvallisuus on perimmiltään tunnetila, tulisi sitä vaarantavia uhkia Eräsaaren mukaan kuitenkin pyrkiä mittaamaan ja asettamaan niille todennäköisyyksiä. Tähän arviointiin liittyy tietysti sellaisia muuttuvia tekijöitä, jotka eivät aina ole arvioitavissa. Epävarmuustekijät joudutaan kohtaamaan ja arvioinnin mahdottomuus johtaakin yleensä kysymykseen, kuinka paljon turvattomuutta olemme valmiita sietämään, jotta on riittävän turvallista. Edellä oleva ajatusmalli johtaa Eräsaaren mukaan rationaaliseen johtopäätökseen turvallisuuden suhteellisuudesta ja rajattomuudesta. Turvallisuus voidaan haluttaessa asettaa yhdessä sovittavassa olevalle ja hyväksyttävissä olevalle tasolle. Tämä kuitenkin edellyttää, että vaaroja ja uhkia osataan arvioida ja niiden toteutumisen todennäköisyydet tiedostetaan. Lisäksi tulee ymmärtää arviointiin aina liittyvät epävarmuustekijät. Ilman perusteellista riskianalyysiä ei Eräsaaren mukaan voida saavuttaa yhdessä hyväksyttävissä olevaa turvallisuuden tasoa.⁹⁹

Edellä olevasta voidaan johtaa ajatus oikean ja oikea-aikaisen tiedon tarpeen tärkeydestä niille toimenpiteille, joilla synnytetään ja pyritään lisäämään turvallisuutta. Turvallisuuden nimissä ja sen turvaamiseksi tehtävien päätösten tulisikin perustua faktoihin, eikä mielikuviin tai pelkkiin tuntemuksiin. Mikäli riskianalyysi perustuu väärin tietoihin emmekä ymmärrä sen sisältävän epävarmuustekijöitä, voi tuloksena olla epärealistisen kuva turvallisuudesta tai sen puutteesta. Tässä yhteydessä tiedustelutoiminnan merkitys ja sen avulla saadut tiedot saavat merkityksensä. Aina pelkkä saatavissa oleva tieto ei edes riitä oikean suuntaiseen päätöstentekoon, tiedon pitää olla myös analysoitua ja se pitää saattaa päätöksentekijöiden käytettäväksi ymmärrettävässä muodossa.

⁹⁹ Eräsaari 2002, s. 21.

Turvallisuudesta on tullut tärkeä käsite, mutta se on Koskelan mukaan jäänyt jäsentymättömäksi. Kukaan ei tunnu tietävän mitä se lopulta on ja miten siihen päästään. Julkisessa keskustelussa turvallisuudesta onkin tullut retoriikkaa, jolla voidaan pyrkiä oikeuttamaan mitä tahansa yhteiskunnallisia muutoksia.¹⁰⁰ Tässä ilmiössä on kyse niin sanotusta turvallistamisesta, joka lyhyesti ilmaistuna tarkoittaa, että ”*erilaiset asiat ja ilmiöt sekä yhteiskunnalliset ongelmat nähdään turvallisuuskysymyksinä, mikä muuttaa poliittista suhtautumista niihin sekä niiden ratkaisemiseen käytettäviä keinoja*”.¹⁰¹

Tätä jäsentymättömyyttä on Riialin mukaan lisännyt niin maailmalla kuin Suomessakin käyttöön otettu laaja-alainen turvallisuuskäsitys sekä sotilaallisten ja siviiliuhkien välisen rajavedon hämärtyminen. Sotilaallisten uhkien ja rikollisuuden tuottamien uhkien lisäksi laaja turvallisuuskäsitys pitää sisällään myös taloudelliset uhat, yhteiskunnalliset ja sosiaaliset uhat, ympäristöuhat ja terveydelliset uhat.¹⁰² Sotilaallisten ja siviiliuhkien välisen rajan hämärtymisessä on kyse siitä, ettei uhan paljastuessa ole tietoa sen alkuperästä tai sen tarkoituksesta. Uhan tarkoituksen ja tavoitteen arviointia voi hämärtää myös se, että käytettävät keinot voivat olla siviililuonteisia kuten esimerkiksi informaatio sodan käynnin keinoja kyberhyökkäyksineen ja valeuutisineen.

Turvallisuuteen liittyy olennaisesti sitä uhkaava ja vaarantava taho, jonka yleensä ajatellaan olevan vastapuolella (vihollinen). Turvallisuus ja tiedustelu liittyvät toisiinsa ainakin siinä mielessä, että vastapuolesta saatavilla olevien tietojen perusteella voidaan tehdä parempia päätöksiä, joiden avulla turvallisuutta voidaan lisätä tai ainakin pitää yllä. Voidaan ajatella, että ilman tiedustelutietoa yhteisön päätöksentekijä vain arvelee yhteisöön kohdistuvan uhkan olemassaolon. Jos väärän tai puutteellisen informaation perusteella ryhdytään vastustamaan ja torjumaan uhkaa täysin perusteetta, johtaa se mitä todennäköisimmin myös vastapuolen vastareaktioon, joka sitten onkin todellinen uhka, eikä enää kuviteltu. Alkuperäisestä tilanteesta siis jouduttiin tiedon puutteen vuoksi tilanteeseen, jossa molempien osapuolten turvallisuustilanne heikkeni. Tilanne olisi voitu välttää hankkimalla tietoa oletetun uhkan olemassaolosta harjoittamalla aktiivista tiedon hankintaa.

Tässä tutkimuksessa ei varsinaisesti oteta kantaa siihen, miten turvallisuus tiedustelulakihankkeen tutkimuskohteena tulisi ymmärtää tai kuinka laajasti turvallisuus pitäisi nähdä. Koska tässä tutkimuksessa keskitytään olemassa olevien uhkien ja niiden torjumisen tarkasteluun, eikä niinkään

¹⁰⁰ Koskela 2009, s. 45.

¹⁰¹ Laitinen 2009, s. 40.

¹⁰² Riiali 2016, s. 2.

turvallisuuden tarkasteluun, ymmärretään turvallisuus molempien siviili- ja sotilastiedustelun näkökulmasta. Koska säädöspohjainen tiedustelutoiminta nykytilassa ja tulevaisuudessa on uskottu viranomaisten tehtäväksi, aihetta lähestytään valtiollisesta näkökulmasta, joka puolestaan luo tutkimuksen lähtökohdaksi perinteisen valtiokeskeisen turvallisuuskäsityksen. Perinteisessä kansallisen turvallisuuden määritelmässä Limnellin mukaan yleensä korostuu valtion turvallisuuden ja sotilaallisen uhkan ensisijaisuus. Perinteinen hänen mukaan viittaa turvallisuuskäsitteen pitkäaikaiseen kiinnittymiseen erityisesti valtion suvereniteetin periaatteelle. Tässä kontekstissa turvallisuutta onkin vaikea käsittää ilman valtiokytkentää ja valtiota uhkaavia tekijöitä. Kun turvallisuus ymmärretään valtion sekä sen alueen että perusarvojen suojaamisena, on valtion turvallisuus myös kansalaisten turvallisuutta. Tällä perusteella kansalaisten oikeuksia voidaan rajoittaa, jos valtion olemassaolo on vaarassa. Ajatuksena on Limnellin mukaan kansallisen turvallisuuden perimmäisyys ja valtion ensisijaisuus, jotka kansalaiset hyväksyvät, koska valtio kykenee suojaamaan heitä uhkatilanteissa.¹⁰³

Laitisen mukaan globalisaation myötä Suomi on nykyisin kiinteä osa varsinkin eurooppalaista, ellei jopa globaalia turvallisuusympäristöä, jonka laajentumisen johdosta turvallisuuteen liittyvät näkemyksemme sekä menettelytapamme ovat monilta osin muuttuneet. Globalisaatio on laajentanut merkittävästi myös turvallisuusympäristöömme vaikuttavia tekijöitä.¹⁰⁴ Tiedonhankintalakitöryhmän käsityksen mukaan nykyisin turvallisuuttamme uhkaavat sellaiset tekijät, jotka useimmiten liittyvät Suomen ulkopuolisiin tapahtumiin. Pääasiallisia siviililuontoisia turvallisuusuhkia ovat työryhmän mukaan ainakin kansainvälinen terrorismi, kyberhyökkäykset, tietoverkkorikollisuus, vieraiden valtioiden Suomeen ja sen etuihin kohdistama laiton tiedustelutoiminta ja kansainvälinen vakava järjestäytynyt rikollisuus. Vakavaksi kansainvälisen järjestäytyneen rikollisuuden tekee se, että rikollisten perimmäisenä tarkoituksena yhteiskunnalliseen päätöksentekoon vaikuttaminen tai soluttautuminen Suomen hallinnon rakenteisiin. Lisäksi kybertoimintaympäristössä tapahtuva rajat ylittävä laiton tiedustelu (vakoilu) on noussut viime vuosina huomionarvoiseksi uhaksi.¹⁰⁵ Työryhmän mukaan vakavimmat kansalliseen turvallisuuteemme kohdistuvat uhat ovatkin lähes poikkeuksetta kansainvälistä alkuperää tai ne ainakin linkittyvät ulkomaille.¹⁰⁶ Turvallisuusympäristöömme muutoksella perustellaankin vaatimusta tiedustelulakien ja sen mahdollistavien keinojen säätämisestä.

¹⁰³ Limnell 2009, s. 50 – 51.

¹⁰⁴ Laitinen 2009, s. 1.

¹⁰⁵ Tiedonhankintalakitöryhmän mietintö 2015, s. 18 – 19.

¹⁰⁶ Ibid, s. 73.

Muuttuvaa turvallisuusympäristöämme käsittelevässä artikkelissa Laitisen mukaan varsinkin poliisin osalta kansainvälistymiseen liittyvä kehitys ja erityisesti Suomen jäsenyys Euroopan unionissa ovat osaltaan vaikuttaneet poliisin tehtäväkentän muuttumiseen. Turvallisuuteen liittyviä toimintoja on pitänyt jäsentää uudelleen, koska rajat ylittävä toiminta niin EU:n sisällä kuin voimakkaasti kansainvälistyvä rikollisuus vaativat sitä. Esimerkiksi terrorismia koskeva tietoisuus suomalaisessa turvallisuushallinnossa on merkittävässä määrin seurausta EU-jäsenyydestämme ja siten EU:n piirissä tehtävät lainsäädäntötoimet heijastuvat meille paikoin voimakkaastikin. Nykymuotoinen ja -sisältöinen turvallisuus omaa linkin sotaan, maahanmuuttoon, terrorismiin ja esimerkiksi järjestäytyneeseen rikollisuuteen. Tässä mielessä Laitisen mukaan turvallisuus sisältää yhä kapeamman ja kovan ulottuvuuden huolimatta pitkään esillä olleesta laajan turvallisuuden ideasta. Turvallisuus palautuukin valvontaan, informaatioon ja pakottaviin toimiin tapauksissa, jotka uhkaavat valtion ja yhteisön haavoittuvuutta. Turvallisuuden viimeaikaisessa kehityksessä sisäinen turvallisuuden ulottuvuus on painottunut ulkoisen sijaa. Esimerkiksi terrorismin vastaisessa toiminnassa tämä muuttunut ajattelu näkyy resurssien ja huomion kiinnittämisenä kykyyn havaita ja ennalta ehkäistä sekä mahdollisen iskun sattuessa kykyyn hallita järjestystä rikkovia voimia.¹⁰⁷

Tiedustelun mahdollistavan lainsäädännön tarkoituksena olisi tiedonhankintalakityöryhmän mukaan *”hankkia kansallisen turvallisuuden kannalta välttämätöntä tietoa vakavista uhkista”*.¹⁰⁸ Suojelupoliisin mukaan tiedustelun keinovalikoimasta esimerkiksi tietoliikennetiedustelun avulla voitaisiin havaita, tunnistaa ja kartoittaa kansalliseen turvallisuuteemme kohdistuvia erityisen vakavia kansainvälistä alkuperää olevia uhkia.¹⁰⁹ Uhkien havaitsemisen ja tunnistamisen sekä niiden torjumisen lisäksi tiedustelulakihankkeen tavoitteena on parantaa ylimmän valtionjohdon tiedonsaantia uhista ja Suomen turvallisuusympäristössä tapahtuvista muutoksista. Turvallisuusviranomaisilla on työryhmän näkemyksen mukaan oltava kyky tuottaa valtion ylimmälle johdolle tietoa, joka puolueetonta ja luotettavaa, lisäksi tiedon oltava käytettävissä riittävän ajoissa ennen merkittävää päätöksentekoa. Toiminnalla tuettaisiin valtion ylimmän johdon päätöksentekoa ja varmistettaisiin sen perustuminen oikeaan, ajantasaiseen ja luotettavaan tietoon.¹¹⁰

¹⁰⁷ Laitinen 2009, s. 8 – 11.

¹⁰⁸ Tiedonhankintalakityöryhmän mietintö 2015, s. 80.

¹⁰⁹ Suojelupoliisi, lausunto s. 2.

¹¹⁰ Tiedonhankintalakityöryhmän mietintö 2015, s. 13 – 14.

4.2 Yksityiselämän suoja ja luottamuksellisen viestin salaisuuden suoja perustuslaissa

Keskustelu toimenpiteistä kansalaisten turvallisuuden lisäämiseksi viranomaistoimin, synnyttää yleensä pelkoa ja epäilyksiä perusoikeuksien, eteenkin yksityisyyden kaventumisesta. Epäily perusoikeuksien kaventumisesta syntyy varsinkin, jos turvallisuutta lisäämään esitetyt keinot ovat kansalaisten ja eri toimijoiden teknistä valvontaa, tarkkailua, tietojen keruuta (kohdennettua tai massatiedustelua) sekä tiedon tallentamista ja sen käyttöä. Keskustelussa osapuolet ei mielestäni aina edes ymmärrä, että vastakkain asettuvat kaksi perusoikeutta; perustuslain 7 §:ssä jokaiselle taattu oikeus turvallisuuteen ja oikeus yksityisyyteen (PL 10 §).

Suomessakin perus- ja ihmisoikeudet ovat saaneet yhä enemmän painoarvoa laajalti erilaisissa lainsäätämisen- ja käyttötilanteissa. Länsinevan mukaan perusoikeuksista muodostuu eräänlainen yhtenäinen kokonaisjärjestelmä, jonka ominaispiirteenä kuitenkin on, että sen sisältämät ainesosat (perusoikeudet) ovat usein kollisiossa tai ainakin jännitteisessä suhteessa toisiinsa nähden. Yleisimmin jännitetilanne syntyy siitä, että samanaikaisesti vaaditaan yksilöiden toimintavapauden kunnioittamisesta ja toisaalta toisten ihmisten turvallisuudesta huolehtimista.¹¹¹ Tiedustelulakihankkeessa kansalaisten yksityisyyden suojan ja heidän turvallisuuden takaamisen mahdollistavien keinojen välillä on löydettävä molempien oikeuksien toteutumisen mahdollistama tasapainoinen ratkaisu.

Vuoden 1995 elokuussa voimaan tulleiden perusoikeussäännösten uudistamisen taustalla (HE 309/1993) oli säännösten kokonaisuudistus ja niiden kokoaminen hallitusmuodon II lukuun. Hallituksen esityksen mukaan perusoikeuksia koskevissa säännöksissä määritellään julkisen vallan valtiosääntöiset tehtävät ja näissä säännöksissä myös rajoitetaan julkisen vallan käyttöä yksilön oikeuksien hyväksi. Niillä lisäksi luodaan lainsäätäjän ja muiden julkisen vallan käyttäjien toiminnan kehykset. Perusoikeusuudistuksella tavoiteltiin pääasiassa yksilön oikeuksien perustuslaintasoisien turvan laajentamista ja vahvistamista. Uudistuksen yhtenä pyrkimyksenä oli myös yksilön ja julkisen vallan suhteiden määrittäminen sekä suomalaisen yhteiskunnan sen hetkisten perustavanlaatuisten arvojen määrittely nyt ja lähitulevaisuudessa. Kaiken jo edellä lueteltujen uudistusten lisäksi perusoikeusuudistuksen tavoitteena oli lisätä perusoikeuksien suoraa soveltuvuutta tuomioistuimissa ja parantaa yksilöiden mahdollisuutta vedota perusoikeussäännöksiin oikeuksiensa välittömäksi

¹¹¹ Länsineva 1998, s. 113 – 114.

tueksi sekä vahvistamaan Suomea sitovien kansainvälisten ihmisoikeussopimusten asemaa oikeusjärjestelmässämme.¹¹²

Hallituksen esityksessä (HE 1/1998 vp.) perusoikeussäännökset ehdotettiin otettavaksi uuteen perustuslakiin sellaisina kuin ne olivat tuolloin voimassa ollessa hallitusmuodossa. Sisällöllisesti yksilön perusoikeudet eivät siis muuttuneet 1.3.2000 voimaan tullessa perustuslaissa (PL 731/1999) ja perustuslain yksityiselämän suojaa koskeva 10 § vastaakin sellaisenaan vuoden 1995 uudistuksessa uudistettua hallitusmuodon 8 §:ää.¹¹³ Merkittävimmät muutokset liittyivät poikkeuslakien käyttömahdollisuuden rajoittamiseen ja perustuslain etusijajärjestelmään.¹¹⁴

Yksityiselämän suojasta ja luottamuksellisen viestin salaisuudesta säädettiin perusoikeusuudistuksen yhteydessä vuonna 1995 hallituksen esityksen (HE 309/1993 vp.) pohjalta. Perustuslain 10 § mukaan:

”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.

Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton.

Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.”

Perusoikeusuudistuksen yhteydessä PL 10 §:n otsakkeeksi tuli ”Yksityiselämän suoja”, joka käsitteenä Viljasen mukaan perustuslaissa viittaa laajassa merkityksessä sen turvaamien oikeuksien kokonaisuuteen, mutta viittaa myös suppeammassa merkityksessä 10 §:n 1 ja 2 momenteissa turvattuihin erityisiin perusoikeuksiin. Pykälän 3 momentti sisältää erityiset kotirauhan piiriin ulottuvat toimenpiteet ja viestin salaisuutta koskevat rajoituslausekkeet, eli ns. kvalifioidut lakivaraukset.¹¹⁵

Ennen perusoikeussäännösten uudistamista voimassa olleessa hallitusmuodossa ei ollut yksityiselämän suojaa koskevaa yleislauseketta. Hallituksen esityksessä (HE 309/1993 vp.) tämä puute nähtiin ongelmallisena yksityiselämän perustuslainsuojan kattavuutta ajatellen, koska ennen uudistusta suojattiin erityisesti vain tiettyjä yksityiselämän osa-alueita (kunnia, kotirauha, kirje-,

¹¹² HE 309/1993 vp, s. 1, 15.

¹¹³ HE 1/1998 vp, s. 64.

¹¹⁴ Saraviita 2011, s. 116.

¹¹⁵ Viljanen 2011, s. 389.

lennätin- ja puhelinsalaisuus). Yleislausekkeen puuttumisesta aiheutui tilanteita, joissa suojan ulkopuolelle oli mahdollista jäädä yksilön kannalta tärkeitä osa-alueita.¹¹⁶ Perusoikeusuudistuksen yhteydessä henkilön yksityistä piiriä eri puolilta suojaavat perusoikeudet koottiin yhteen. Viljasen mukaan merkittävä perusoikeusjärjestelmän täydennys olikin yksityiselämän suojaa koskevan yleislausekkeen ottaminen PL 10 §:ään.¹¹⁷

Perusoikeusuudistuksen taustalla olevan hallituksen esityksen (HE 309/1993 vp.) mukaan ”yksityiselämä” käsitteenä ymmärretään henkilön yksityistä piiriä koskevana yleiskäsitteenä. Se ei kuitenkaan selväpiirteisesti eroa esimerkiksi henkilökohtaisen koskemattomuuden, kunnian tai kotirauhan suojasta. Nämä eri oikeudet toimivatkin usein tosiasiasa päällekkäisinä suhteessa toisiinsa. Puuttuminen kotirauhan piiriin yleisesti, on nähtävä Viljasen mukaan puuttumisena myös henkilön yksityiselämään. Yksityiselämän luonne henkilön yksityistä piiriä koskevana yleiskäsitteenä merkitseekin Viljasen mukaan sitä, että yksityiselämän suojaäännöksellä voidaan täyttää muiden henkilön yksityistä piiriä turvaavien perusoikeuksien useasti jättämiä suoja-aukkoja.¹¹⁸ Yksityiselämän suojan käsitteeseen on tarpeen vedota varsinkin silloin, kun kyse on tilanteista, joihin muut edellä mainitut perusoikeussäännökset eivät suoraan sovellu.¹¹⁹

Hallituksen esityksen (HE 309/1993 vp.) mukaan ”*yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämänsä*”. Lähtökohtamäärittelystä huolimatta HE:ssä todetaan yksityiselämän piirin määrittelyn olevan vaikeaa. Siihen katsotaan kuuluvan ”*muun muassa yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään ja ruumiistaan*”.¹²⁰ Myös suuriosa yksityiselämän suojaa perusoikeutena tutkineista ja siitä kirjoittaneista oikeusoppineista ovat todenneet yksityiselämän piirin olevan vaikeasti määriteltävissä.

Metsärannan mukaan yksityiselämän käsite tuli osaksi perustuslakia ensisijaisesti Euroopan ihmisoikeussopimuksen 8 artiklasta. Perusoikeussäännöksen käsitteen perustuessa ihmisoikeussopimuksen käsitteistöön, on sen sisällön tulkinnassa mahdollista hänen mukaansa tukeutua vastaavan ihmisoikeusmääräyksen tulkintakäytäntöön. Näin ollen Euroopan

¹¹⁶ HE 309/1993 vp, s. 53.

¹¹⁷ Viljanen 2011, s. 390.

¹¹⁸ Viljanen 2011, s. 391.

¹¹⁹ Nieminen 1999, s. 112.

¹²⁰ HE 309/1993 vp, s. 52 – 53.

ihmisoikeustuomioistuimen ratkaisuksista, jotka koskevat yksityiselämän suojaa, voidaan hakea tukea sille, mitä yksityiselämällä tarkoitetaan.¹²¹

Niemisen mielestä yksityiselämän ja yksityisyyden suojan käsitteitä käytetään välillä hyvin epätarkasti ja saatetaan puhua yksityisyyden suojasta silloinkin, kun itse asiassa tarkoitetaan jonkin verran laajempaa yksityiselämän suojan käsitettä. *Yksityisyyden suojasta* puhuttaessa tarkoitetaan usein jossain määrin suppeampaa käsitettä kuin yksityiselämän suoja. Se sisältyy kuitenkin osana laajempaan *yksityiselämän suoja* käsitteeseen. Käsitteenä yksityisyyden suoja liitetään lähinnä tietosuojaan, jossa yksityisyyttä suojellaan henkilötietoja kerätessä, käytettäessä ja luovutettaessa.¹²²

Yksityiselämän suojaan liittyvät perusoikeudet vuoden 1919 hallitusmuodossa vanhenivat Saraviidan mukaan merkittävilta osin vuosien saatossa teknisen kehityksen edetessä. Sähköiseen viestintään liittyvä teknologia kehittyi nopealla tahdilla, kuten myös erilaiset tekniset seurannan mahdollistavat keinot. Henkilöiden elämää ja liikkumista sekä puheitaan ja viestintää laajemmassakin mielessä voitiin valvoa ja tallentaa erilaisin teknisin välinein. Teknologinen kehitys mahdollisti myös henkilöiden liikkumisen ja toiminnan jäljittämisen.¹²³

Uuden teknologian ja rikostutkimusmenetelmien kehityksen seurauksena on vuoden 1995 perusoikeusuudistuksesta alkaen säädetty sarja yksityisyyden suojan rajoituksia. Myös käsitteistö uudistui. Vanhanaikainen ja kielletty (sala)kuuntelu korvattiin telekuuntelun ja teknisen tarkkailun käsitteillä, ja se sai rinnalleen uutena rikostutkimusmenetelmänä teknisen katselun ja teknisen seurannan. Teknisen tarkkailun rinnalle kehittyi lievemmin yksityisyyttä rajoittava televalvonta eli oikeus saada puhelimen soittotietojen, sijaintitietojen ja sähköpostiviestien osoitetiedot (teletunnistetiedot). Sääntelyn alkuvaiheessa toimivaltuudet televalvontaa annettiin poliisille, myöhemmin myös tullille, Puolustusvoimille ja Rajavartiolaitokselle.¹²⁴

PL 10.2 § mukaan ”*kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton*”. Viljasen mukaan tämä momentin tarkoituksena turvata jokaisen oikeus luottamukselliseen viestintään ilman, että kukaan ulkopuolinen saa oikeudettomasti tiedon lähetetyn tai vastaanotettavaksi tarkoitetun luottamuksellisen viestin *sisällöstä*. PL 10.2 § antaa suojan muun muassa kirjeiden tai

¹²¹ Metsäranta 2015, s. 19 – 20.

¹²² Nieminen 1999, s. 112 – 113.

¹²³ Saraviita 2011, s. 179.

¹²⁴ Ibid, s. 179.

muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan. Säännös suojaa molempien viestinnän osapuolten - lähettäjän ja vastaanottajan – oikeutta luottamukselliseen viestintään.¹²⁵

Hallituksen esityksessä ilmaistun kannan mukaan ennen perusoikeussäännösten uudistamista voimassa ollut hallitusmuodon 12 §:n suoja ei soveltunut kovinkaan hyvin luottamukselliseksi tarkoitetun viestinnän uusiin muotoihin. Alati kehittyvä viestintäteknologia oli tehnyt vain tiettyjä välineitä koskevan viestinnän suojan ongelmalliseksi.¹²⁶ Tämä hallituksen esityksen havainto teknisestä kehityksestä olikin Viljasen mukaan lähtökohtana, kun perusoikeusuudistuksen yhteydessä perustuslainsuojan piiriin saatettiin kaikki luottamuksellisiksi tarkoitetut viestit riippumatta viestin välittämisessä käytetystä menetelmästä. PL 10.2 §:ää voidaankin näin ollen pitää välineneutraalina säännöksenä, vaikka siinä edelleen viitataan vain kirje- ja puhelinsalaisuuteen käytännössä tavallisimpina luottamuksellisen viestinnän muotoina.¹²⁷

Viestisisällön salassa pitäminen oli Saraviidan mukaan aikoinaan teknisesti varsin yksinkertaista (esimerkiksi kirjeen luvattoman avaamisen kriminalisoimisella). Tekniset edellytykset sähköisen viestin sisällön avaamiseen ja purkamiseen, viestin palvelimilla olevien kulkureittien selvittämiseen sekä tällaisen viestin luvattomaan ja huomaamattomaan haltuunottoon paranevat jatkuvasti. Tehokkaan tietosuojan ja luottamuksellisen viestin suojan turvaamisesta onkin tullut hänen käsityksensä mukaan vakava yksityisyydensuojaongelma.¹²⁸

On huomioitava, ettei säännös ei anna suojaa normaaliksi katsottavalta etäisyydeltä käytävän keskustelun sisällön kuuntelulta. Jos luottamukselliseksi tarkoitettua keskustelua kuunnellaan teknisiä apuvälineinä käyttäen, olisi tällainen kuuntelu puuttumista säännöksessä turvattuihin oikeushyviin. Hallituksen esityksen mukaan säännöksellä ensisijaisesti pyritään suojaamaan luottamukselliseksi tarkoitettun *viestin sisältö* ulkopuolisilta. Toisekseen säännöksen tarkoituksena suojata muitakin tällaista viestiä koskevia tietoja, joilla on mahdollisesti merkitystä viestin luottamuksellisena säilymiselle. Tyypillisesti tällaisia ovat esimerkiksi puhelujen *tunnistamistiedot*.¹²⁹ Teleyhteyden liittyvien tunnistamistietojen avulla voidaan saada selville yhteyden osapuolet. Tunnistamistietojen luovuttaminen merkitsee Viljasen mukaan kuitenkin viestin

¹²⁵ Viljanen 2011, s. 406.

¹²⁶ HE 309/1993 vp, s. 53.

¹²⁷ Viljanen 2011, s. 405.

¹²⁸ Saraviita 2011, s. 179 – 180.

¹²⁹ HE 309/1993 vp, s. 53.

sisällön paljastumiseen verrattuna vähäisempää puuttumista luottamuksellisen viestin salaisuuteen, millä on merkitystä rajoituksen sallittavuuden arvioinnissa.¹³⁰

Oikeus luottamuksellisen viestin säilymiseen salaisena jakautuu siis kahteen alueeseen, jotka ovat yhtäältä viestin sisältö (ydinalue) sekä toisaalta tunnistamistietojen antama tieto viestinnän tapahtumisesta ja viestinnän osapuolista (reuna-alue). Yksityiselämän suojan ja poliisin salaisten tiedonhankintakeinojen suhdetta selvittäneessä väitöskirjassa Metsärannan mukaan luottamuksellisen viestin salaisuuden kategorista jakoa suojan ydin- ja reuna-alueeseen ei voida välttämättä pitää onnistuneena. Kategorinen jaottelu ei ole toimiva, koska yksistään viestin tunnistamistiedoilla voidaan saada sellaista tietoa, jolla voi olla varsin huomattava merkitys yksityiselämän suojan kannalta. Luottamuksellisen viestin sisällön selvittämiselläkään ei välttämättä hänen mukaan aina saada kovinkaan merkittävää tietoa. Tunnistamistietojen keräämisen tekee ongelmalliseksi se, että niitä hyväksikäyttäen on mahdollista esimerkiksi paikantaa henkilön sijainti ja liikkeet tietyllä alueella. Henkilön viestinnän tunnistamistietojen avulla saadut sijaintitiedot ja liikkuminen tietyllä alueella esimerkiksi mielenosoituksen tai uskonnollisen tapahtuman aikana paikoissa, joissa nämä ovat tapahtuneet, on näiden tietojen avulla mahdollista muodostaa käsitys henkilön mahdollisista poliittisista tai uskonnollisista kannoista.¹³¹

Perusoikeusuudistuksen yhteydessä antamassaan mietinnössä perustuslakivaliokunta on todennut, että tietyt perusoikeussäännökset sisältävät erityisiä rajoituslausekkeita, jotka valtuuttavat lainsäätäjän rajoittaa perusoikeuksia tavallisella lailla, rajoituslausekkeilla kuitenkin asetetaan lainsäätäjän rajoittamisen harkintavallalle lisäkriteerejä. Nämä rajoituslausekkeet ovat niin sanottuja lakivarauksia, joita kutsutaan kvalifioituiksi lakivarauksiksi. Niissä perusoikeuden rajoittamisen valtuutus kytkeytyy tiettyyn tarkoitukseen (esim. perusoikeuden turvaaminen) tai tiettyihin edellytyksiin (esim. oikeudenkäynnissä). Lisäksi niissä on voitu asettaa rajoitukselle nimenomainen välttämättömyysvaatimus. ”Kvalifioitujen lakivarausten tarkoituksena on määrittää tavallisen lain säätäjän rajoitusmahdollisuus mahdollisimman täsmällisesti ja tiukasti siten, ettei perustuslain tekstissä anneta avoimempaa perusoikeuden rajoitusvaltuutta kuin välttämättä on tarpeen”.¹³² PL 10 §:n 3 momenttiin on nimenomaisesti sisällytetty edellä mainitun kaltainen ns. ns. kvalifioitu lakivaraus.

¹³⁰ Viljanen 2011, s. 406 – 407.

¹³¹ Metsäranta 2015, s. 37.

¹³² PeVM 25/1994 vp, s. 5

PL 10.3 § sisältää luottamuksellisen viestin salaisuuden rajoituksia koskevan erityisen rajoituslausekkeen, jossa tyhjentävästi luetellaan hyväksyttävät edellytykset puuttua viestin salaisuuteen sekä asetetaan rajoituksille välttämättömyysvaatimus. Rajoituslausekkeen mukaan viestin salaisuuden lainsäädännöllinen rajoittaminen ”on mahdollista yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana”. Olennaista on Viljasen mukaan kuitenkin kaikissa tapauksissa rajoituksen välttämättömyysvaatimuksen täyttyminen.¹³³

Vaikka kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on ”loukkaamaton”, tarkoittaa se ehdottomalta vaikuttavasta sanamuodosta huolimatta kuitenkin sitä, että tätä perusoikeutta voidaan rajoittaa PL 10.3 sisältämän kvalifioidun lakivarauksen ja yleisten perusoikeuksien rajoitusedellytysten asettamien rajojen mukaisesti. Säädetävällä lailla voidaan siis määrätä välttämättömiä rajoituksia viestin salaisuuteen esimerkiksi yksilön tai yhteiskunnan turvallisuutta vaarantavien rikosten tutkinnassa.¹³⁴

Tietoliikennetiedustelutoiminnan mahdollistavan lain kannalta lailla säätämisen vaatimuksella ei käytännössä ole merkitystä, koska lain tasoista säädöstä mietinnössä ollaan esittämässäkin. Toisena rajoitusedellytyksenä on sen välttämättömyys ja kolmantena rajoitusedellytyksenä tulee olla yksilön tai yhteiskunnan turvallisuutta vaarantavan teon tutkinta.

Perustuslakivaliokunta on arvioinut perusoikeusrajoituksen välttämättömyysvaatimusta mm. lausunnossaan (PeVL 32/2013 vp.) koskien esitutkintalain ja pakkokeinolain muuttamista. Lausunnon mukaan rajoituksen välttämättömyysvaatimus edellyttää, ettei muilla keinoilla voida saavuttaa tavoiteltavaa tulosta, ja siten perusoikeusrajoitus on välttämätön halutun päämäärän toteuttamiseksi.¹³⁵

PL 10 §:n 3 momentin kvalifioidun lakivarauksen mukaan yksilön turvallisuus on hyväksyttävissä oleva perusoikeuden rajoitusperuste, jos on kyse tilanteesta, jossa yksilöitävän henkilön oikeus on konkreettisessa vaarassa. Hallituksen (HE 309/1993 vp.) esityksen mukaan yksilön tai yhteiskunnan turvallisuutta vaarantavia rikoksia ovat muun muassa huumausainerikokset, törkeät väkivaltarikokset sekä maan- ja valtiopetosrikokset. Hallituksen esityksissä ja perustuslakivaliokunnan kannanotoissa,

¹³³ Viljanen 2011, s. 407 – 408.

¹³⁴ Viljanen 2011, s. 405. Saraviita 2011, s. 180.

¹³⁵ PeVL 32/2013 vp, s. 4.

joissa on tarkasteltu kysymystä siitä, mitä yksilön turvallisuutta vaarantavilla rikoksilla tarkoitetaan, ei ole käytettävissä tyhjentävää vastausta. Metsärannan mukaan yksilön turvallisuuden voidaan katsoa pitävän sisällään ainakin kaikki senkaltaiset uhat, joiden kohteena on henkilön fyysinen selviytyminen. Yksilön turvallisuuteen voidaan hänen mukaan katsoa kuuluvan niin taloudellisia oikeuksia kuin myös yksilön henkeen tai henkilökohtaiseen koskemattomuuteen liittyviä oikeuksia.¹³⁶

Yhteiskunnan turvallisuuden käyttämisessä luottamuksellisen viestin salaisuuden rajoitusperusteena törmätään yhteiskunnan turvallisuuden määrittelyn ongelmiin, joita käsiteltiin luvussa 2.1. Hallituksen esityksissä ja perustuslakivaliokunnan kannanotoissa yhteiskunnan turvallisuutta vaarantavina rikoksina edellisessä kappaleessa lueteltujen lisäksi voidaan Metsärannan mukaan ainakin pitää:

- ”sellaisia liike- ja ammattitoiminnassa tehtyjä talousrikokset, jotka saattavat vaikuttaa hyvinkin haitallisesti yhteiskunnan toimintoihin tai vaarantaa niitä ja
- yhteiskunnan toimintojen kannalta merkityksellisenä on pidetty myös automaattisia tietojenkäsittelyjärjestelmiä koskevia rikoksia. Automaattiseen tietojenkäsittelyjärjestelmään kohdistuessaan tällaisilla rikoksilla on merkittäviä yhteiskunnan toimintaan ja etenkin yksilöiden yksityiselämän suojaan ja luottamuksellisen viestin salaisuuteen liittyviä haitallisia vaikutuksia”.¹³⁷

Metsärannan mukaan vaikuttaa siltä, että yhteiskunnan turvallisuus suojaa lähinnä yhteiskunnan perustavaa laatua olevia toimintoja. Koska näihin toimintoihin voi kohdistua monenlaisia uhkia, ei yhteiskunnan turvallisuutta hänen mukaan voi käsitteenä pitää kovin tarkkarajaisena. Arvioitaessa yhteiskunnan turvallisuutta hyväksyttävänä rajoitusperusteena luottamuksellisen viestin salaisuuden kannalta, on hänen mukaan pohdittava sitä, miten rajoitusperusteena oleva toiminta tosiasiallisesti nähdään uhkaavan yhteiskunnallista turvallisuutta.¹³⁸

Perusoikeuden rajoittamisen perusteena on oltava jokin hyväksyttävä intressi, mutta Metsärannan mukaan sekään ei sellaisenaan pelkästään riitä. Jotta rajoitusperuste intressinä olisi hyväksyttävä, tulee intressiin kohdistuvan uhkan olla konkreettinen ja yksilöitävässä. Lakivarauksessa tämä vaatimus tuodaan esille rikoksen tutkinnan käsitteen kautta; kyseessä tulee olla konkreettinen ja yksilöity rikosepäily. Samoin kuin yksilön turvallisuuden osalta, on myös yhteiskunnan

¹³⁶ Metsäranta 2015, s. 92 – 94.

¹³⁷ Ibid, s. 95 – 96.

¹³⁸ Ibid, s. 98.

turvallisuuden osalta varmistettava, että käsillä todella on konkreettinen uhka yhteiskunnan turvallisuudelle.¹³⁹

Digitalisaation vaikutuksesta yksityiselämän suojaan kohdistuu jatkuvasti uudenlaisia uhkia, eikä lainsäädäntö pysy mukana tässä kehityksessä. Lainsäädäntö se myöskään pysty ajoissa reagoimaan uusiin uhkatekijöihin, jotka kohdistuvat yksityiselämään. Tästä huolimatta perustuslain yksityiselämää turvaava säännös kuitenkin ulottaa Viljasen mukaan vaikutuksensa myös sellaisiin yksityiselämään puuttumisiin, joita ei ole voitu asianomaista säädöstä laadittaessa vielä osattu edes ennakoida. Varsinkin nykymuotoisessa vahvasti digitalisoituneessa yhteiskunnassa yksityiselämän suojan kohdalla perusoikeuksien horisontaalivaikutuksella, eli vaikutuksella yksityisten keskinäisissä suhteissa, on Viljasen mukaan erityistä merkitystä. Lisäksi hänen mukaan on huomioitava, ettei henkilön oikeutta yksityiselämään useinkaan uhkaa välttämättä aina julkisyhteisö, vaan ennemminkin toinen yksityinen toimija.¹⁴⁰

Yksityiselämän perustuslaillisella suojalla on oma merkityksensä esimerkiksi arvioitaessa yksityiselämään puuttumisia tilanteissa, joissa sosiaalisen median palveluntuottaja käyttää omiin tai sopimuskumppaninsa tarpeisiin sovellustaan käyttävän kuluttajan käyttäjäprofiilista syntyneitä tietoja. Hyvänä esimerkkinä tällaisesta toiminnasta on Facebookin ja Cambridge Analytica –yhtiön välinen yhteistyö, jossa jälkimmäinen sai sovelluksen avulla kerätä Facebook –käyttäjien tietoja poliittisen profiloinnin tarkoituksessa. Yhtiön keräämien tietojen avulla republikaanit pystyivät kohdistamaan vaalimainontansa yhdysvaltojen viimeisissä presidentin vaaleissa täsmällisille kohderyhmille.

On selvää, että tietoliikennetiedustelutoimilla puututtaisiin oleellisesti perusoikeuksien suojaamiin oikeuksiin yksityiselämän suojan ja luottamuksellisen viestin salaisuuden osalta. Tätä puuttumista ja perusoikeuksien kaventamista perustellaan yleisellä tai kansallisella turvallisuudella, jota ei kuitenkaan käsittäkseni voitaisi käyttää perusoikeuksien rajoitusperusteena. Tämä johtuu siitä, ettei kansallista turvallisuutta ole laintasolla määritelty ja kuten edellä on todettu sen olevan käsitteenä suhteellinen ja vaikeasti määriteltävissä.

*Yksityiselämän suoja*a koskeva PL 10 § ei sisällä erityistä rajoituslauseketta. Tästä johtuen on yksityiselämän suojaan puuttumisen sallittavuutta Viljasen mukaan arvioitava myös perusoikeuksien

¹³⁹ Ibid, s. 94 ja 98.

¹⁴⁰ Viljanen 2011, s. 394 – 395.

yleisten rajoitusedellytysten valossa.¹⁴¹ Tätä puuttumisen sallittavuutta arvioidaan myöhemmin käsiteltävien perusoikeuksien yleisten rajoitusedellytysten yhteydessä.

4.3 Perusoikeuksien yleiset rajoitusedellytykset

Tietoliikennetiedustelua koskevalle lainsäädännölle asettavat vaatimuksia myös perusoikeuksien yleiset rajoitusedellytykset. Perusoikeudet eivät ole yleisesti Viljasen mukaan niin ehdottomia, ettei niitä saisi rajoittaa missään olosuhteissa tai laajuudessa. Kuitenkin perusoikeuksien luonteen ja niiden antaman perusoikeusturvan kannalta on tärkeää pitää niiden rajoitukset mahdollisimman vähäisinä.¹⁴² Hänen mukaan perusoikeuksien rajoittaminen voi tulla kyseeseen, jotta esimerkiksi toisten ihmisten perusoikeudet toteutuu tai jonkin painavan yhteiskunnallisen intressin turvaamiseksi.¹⁴³

Arvioitaessa perusoikeuksien rajoittamista kansallisen turvallisuuden perusteella, vastakkain ovat viranomaisten velvollisuus huolehtia sekä valtion että kansalaistensa turvallisuudesta ja yksittäisten kansalaisten oikeus yksityisyyteen sekä luottamuksellisen viestin salaisuuden suoja.

Lakien perustuslainmukaisuuden valvonta Suomessa on ennakkollista, abstraktia ja parlamentaarista. Valvonnassa keskitytään lakien säätämisvaiheen ennakkovalvontaan, jossa vertailun kohteina ovat perustuslain ja lakiehdotuksen säännökset. Tässä valvonnassa eduskunnan perustuslakivaliokunnalla on keskeinen rooli.¹⁴⁴

Ensisijaisesti perusoikeussäätelyn lähtökohtana on perustuslakivaliokunnan mukaan suojata yksilön vapauspiiriä sellaisilta puuttumisilta, jotka tulevat valtiovallan taholta. Perusoikeuksilla on paikkansa kuitenkin myös yksityisten keskinäisissä suhteissa, joka korostaa niiden merkitystä yhteiskunnan perusarvoina.¹⁴⁵ Perusoikeuksien rajoitusedellytyksiä ei ole kirjattu perustuslakiin. Perusoikeuksien yleisiä rajoitusedellytyksiä koskeva luettelo on ensimmäisen kerran esitelty perustuslakivaliokunnan perusoikeusuudistusta koskevassa mietinnössä (PeVM 25/1994). Vuoden 2000 perustuslaista annetussa mietinnössä ohjeet vahvistettiin ja laajennettiin koskemaan koko perustuslakia.¹⁴⁶ Tämä mietintö onkin tärkein asiakirja perusoikeustulkinnan kannalta, ja siinä tiivistetään perusoikeusteorian keskeisimmät osat. Niitä ovat perusoikeussäännösten luonne, lakivaraus- ja

¹⁴¹ Viljanen 2011, s. 395.

¹⁴² HE 309/1993 vp, s. 29.

¹⁴³ Viljanen 2001, 12 – 13.

¹⁴⁴ Oikeusministeriön julkaisu37/ 2013, s. 35.

¹⁴⁵ PeVM 25/1994 vp, s. 3.

¹⁴⁶ Saraviita 2011, s. 135.

viittaustekniikka, säännöt perusoikeuksien rajoittamisesta tai yleisestä sääntelystä tavallisen lain tasolla sekä delegointiproblematiikka.¹⁴⁷

Perustuslakivaliokunnan mietinnössä (PeVM 25/1994) luetellaan oikeuden muotoon kirjoitettujen perusoikeuksien sallitut ja yleiset rajoitusedellytykset, joita ovat:

1. **”Lailla säätämisen vaatimus:** *Rajoitusten tulee perustua eduskuntalakiin.*
2. **Täsmällisyys ja tarkkarajaisuusvaatimus:** *Rajoitusten on oltava tarkkarajaisia ja riittävän täsmällisesti määriteltyjä.*
3. **Rajoitusperusteen hyväksyttävyysoikeusvaatimus:** *Rajoitusperusteiden tulee olla perusoikeusjärjestelmän kannalta hyväksyttäviä, painavan yhteiskunnallisen tarpeen vaatimia.*
4. **Ydinalueen koskemattomuuden vaatimus:** *Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvaa rajoitusta.*
5. **Suhteellisuusvaatimus:** *Rajoitusten tulee olla välttämättömiä tavoitteen saavuttamiseksi sekä laajuudeltaan oikeassa suhteessa perusoikeuksien suojaamaan oikeushyvään ja rajoituksen taustalla olevan yhteiskunnallisen intressin painoarvoon.*
6. **Oikeusturvavaatimus:** *Perusoikeutta rajoitettaessa on huolehdittava riittävästä oikeusturvajärjestelystä.*
7. **Ihmisoikeusvelvoitteiden noudattamisen vaatimus:** *Rajoitukset eivät saa olla ristiriidassa Suomen kansainvälisten ihmisoikeusvelvoitteiden kanssa.”¹⁴⁸*

Keskityn arvioimaan tiedustelulakihankkeen suhtautumista edellä luetelluista viiteen rajoitusedellytykseen; täsmällisyys ja tarkkarajaisuusvaatimukseen, hyväksyttävyysoikeusvaatimukseen, perusoikeuden ydinalueen koskemattomuusvaatimukseen, suhteellisuusvaatimukseen ja ihmisoikeusvelvoitteiden asettamiin vaatimuksiin. Lailla säätämisen vaatimusta ei ole syytä tarkastella, koska lain tasoista sääntelyä ollaan tiedustelun osalta esittämässä. Myös oikeusturvavaatimus rajautuu pois, koska en tarkastele tutkimuksessa tiedustelutoiminnan lupamenettelyyn ja valvontaan liittyviä seikkoja, joihin oikeusturvavaatimus liittyy.

Täsmällisyys ja tarkkarajaisuusvaatimus kiinnittyy Viljasen mukaan osaltaan lailla säätämisen vaatimukseen: *”täsmällisyys ja tarkkarajaisuusvaatimuksessa on kysymys itse asiassa siitä, milloin rajoitus on niin täsmällisesti lain tasolla muotoiltu, että sen voidaan sanoa perustuvan laintasoiseen säännökseen. Täsmällisyys ja tarkkarajaisuusvaatimuksen ydinajatuksena on, että rajoituksen keskeisen sisällön on ilmentävä itse laista, eikä se saa jäädä alemmanasteisen normin antajan tai lakia soveltavan harkintaan. Keskeiseen sisältöön kuuluvat ainakin (a) rajoituksen edellytykset ja (b)*

¹⁴⁷ Ibid, s. 116 – 117.

¹⁴⁸ Viljanen 2001, s. 37 – 38.

*rajoituksen laajuuteen vaikuttavat seikat. Lailla myönnetyt perusoikeuksien rajoitusvaltuudet tulee rajata sillä tavoin tarkasti, ettei käytännössä synny epäselvyyttä siitä, kenellä on asianomaiset valtuudet ja kuinka pitkälle ne ulottuvat. Täsmällisyyden ja tarkkarajaisuuden välistä eroa onkin vaikea hahmottaa. Asiallista merkitystä sillä, puhutaanko rajoituksen tarkkarajaisuudesta vai täsmällisyydestä, ei näyttäisi olevan”.*¹⁴⁹ Viljasen mukaan lähtökohtana tässä arvioinnissa perustuslakivaliokunnan käytännön valossa on, että laista tulee ilmetä riittävän selkeästi ainakin seuraavat seikat: (1) kuka on oikeutettu käyttämään rajoitusvaltuuksia, (2) mitä valtuuksia käytettäessä saadaan tehdä ja (3) miten silloin on meneteltävä. Täsmällisyys ja tarkkarajaisuusvaatimus hänen mukaan edellyttää, että lailla säädetyt perusoikeuksien rajoitustoimivaltuudet on kirjoitettu niin selkeästi, että niiden perusteella on mahdollista riittävän varmasti ennakoida, miten toimivaltuuksia voidaan käyttää.¹⁵⁰

Perustuslakivaliokunnan mietinnön mukaan ”*rajoitusperusteen hyväksyttävyyysvaatimus tarkoittaa, että rajoituksen tulee olla painavan yhteiskunnallisen tarpeen vaatimaa*”. Rajoitusperusteen hyväksyttävyyden arvioinnissa perustuslakivaliokunnan mukaan voidaan tukeutua Euroopan ihmisoikeussopimuksen vastaavanlaista oikeutta koskeviin määräyksiin niiltä osin kuin ne sisältävät tyhjentävän luettelon ihmisoikeuksien hyväksyttävistä rajoitusperusteista.¹⁵¹ Hyväksyttävyyysvaatimus koskee nimenomaisesti rajoitusperustetta eli sitä syytä, jonka vuoksi rajoituksesta halutaan säätää ja rajoitus toimeenpanna. Viljasen mukaan hyväksyttäviä rajoitusperusteita olisivat ainakin muiden perusoikeuksien turvaamistavoite tai jokin muu painava yhteiskunnallinen intressi. Tällaisessa intressissä olisi kyse jonkin painavan kollektiivisen hyvän turvaamisesta tai edistämisestä. Viljanen mukaan tällaisina kollektiivisinä intresseinä voidaan pitää esimerkiksi kansallista turvallisuutta ja vakavan rikollisuuden estämisen edistämistä.¹⁵²

Säätäessään perustuslakia on lainsäätäjä määritellyt määrättyjen perusoikeuksien osalta jo valmiiksi ja tyhjentävästi niiden hyväksyttävät rajoitusperusteet. Näiden kvalifioitujen lakivarausten tarkoituksena on nimenomaisesti supistaa sallittujen rajoitusperusteiden alaa ja tällä tavoin määritellä kyseisten perusoikeuksien rajoitusedellytykset mahdollisimman tyhjentävästi.¹⁵³ Koska tietoliikennetiedustelulla puututtaisiin luottamuksellisen viestin salaisuuteen, on otettava huomioon se, että tätä oikeutta koskevassa lakivaruksessa on lueteltu tyhjentävästi edellä tarkastellut hyväksyttävät perusteet luottamuksellisen viestin salaisuuden rajoittamiselle.

¹⁴⁹ Ibid, s. 115 – 117.

¹⁵⁰ Ibid, s. 120 – 123.

¹⁵¹ PeVM 25/1994 vp, s. 5.

¹⁵² Viljanen 2001, s. 126, 136 ja 185.

¹⁵³ Ibid, s. 200.

Perusoikeuden *ydinalueen koskemattomuuden vaatimus* tiedustelulakia ajatellen liittyy käsittääkseni kysymykseen lähetetyn tai vastaanotetun luottamuksellisen viestin varsinaisen sisällön suojasta. PL 10.2 § mukaan ”*kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton*”. Ensisijaisesti säännöksen tarkoituksena on antaa suojaa sille, ettei luottamukselliseksi tarkoitettun viestin sisältö päädy ulkopuolisten tahojen tietoon. Toisekseen säännöksen tarkoitus turvata tällaista viestiä koskevat muut tiedot, joilla on mahdollisesti merkitystä viestin säilymiselle luottamuksellisena. Tällaisia tietoja ovat tyypillisesti puhelujen tai muiden sähköissä muodossa olevien viestien *tunnistamistiedot*.¹⁵⁴

Perustuslakivaliokunta on muotoillut mietinnössään (PeVM 25/1994 vp, s. 5) perusoikeuden ydinalueen koskemattomuusvaatimuksen seuraavasti:

”Tavallisella lailla ei voida säätää perusoikeuden ytimeen ulottuvaa rajoitusta.”

Viljasen mukaan jokaisella perusoikeudella on siis eräänlainen sen ”olemukseen” liittyvä ydinalue, joka tulee jättää koskemattomaksi. Perusoikeuksien ydinalueen koskemattomuuden vaatimus merkitsee erityisesti sitä, ettei ydinalueellaan perusoikeuksia voida lainkaan rajoittaa. Kysymykseen ei enää tulekaan suoritettava punnintatilanne, kuten arvioitaessa esimerkiksi perusoikeusrajoituksen suhteellisuusvaatimuksen täyttymistä.¹⁵⁵ Koska oikeuden ydinalueella kyse ei ole enää punninnasta, toimiikin perusoikeus Metsärannan mukaan sellaisena sääntönä, joka automaattisesti sulkisi pois vastakkaisten intressien toteuttamisen, kuten esimerkiksi tietoliikennetiedustelun toimivaltuuksien käytön.¹⁵⁶ Ydinalueen käytännön merkitystä on hieman hankala arvioida, koska lainsäädäntökäytäntöön ja oikeuskirjallisuuteen perustuen ydinalueen määrittely näyttäytyy varsin ongelmallisena.

Metsärannan mukaan perustuslakivaliokunnan lausuntojen perusteella voitaisiin tehdä sellainen päätelmä, ettei perusoikeuksien ydinalue voi toimia perusoikeusrajoitusten viimekätisenä rajana ainakaan tiettyjen oikeuksien osalta. Tällainen oikeus on esimerkiksi luottamuksellisen viestin salaisuus. Telekuuntelua ja televalvontaa koskevissa perustuslakivaliokunnanlausunnoissa viestin sisältöä pidetään Metsärannan mukaan puhelinsalaisuuden ydinalueena, mutta siitä huolimatta viestin sisältöön on katsottu voitavan puuttua vaikka telekuuntelulla. Vaikeudet ydinalueen määrittelyssä on johtanut hänen mukaan siihen, että oikeuskirjallisuudessa on esitetty näkemyksiä siitä, että

¹⁵⁴ HE 309/1993 vp, s. 53.

¹⁵⁵ Viljanen 2001, s. 229.

¹⁵⁶ Metsäranta 2015, s. 107.

ydinalueen koskemattomuuden vaatimus palautuu suhteellisuusvaatimukseen. Vaikka joidenkin oikeuksien osalta olisikin vaikeaa tehdä eroa ydinalueen suojan ja suhteellisuusvaatimuksen välisen rajan suhteen, olisi hänen mukaan jo periaatteelliselta kannalta kuitenkin hyvä yrittää tehdä ero ydinalueen koskemattomuusvaatimuksen ja suhteellisuus-vaatimuksen välillä.¹⁵⁷

Hautamäen mukaan Suomessa ei ole käytetty tähän mennessä ydinalueargumentteja kovinkaan paljon, eikä myöskään keskustelu ydinalueargumentaation merkityksestä näytä olleen kovin voimallista. Yhtenä syynä ydinalueargumenttien vähyydelle hän esittää sen, ettei ydinalueen koskemattomuuden vaatimus saa itsenäistä merkitystä tavanomaisissa perusoikeuksien rajoitusten arviointitilanteissa. Itsenäisen merkityksen puuttuminen johtuu siitä, että rajoitukset, jotka ulottuisivat perusoikeuden ydinalueeseen, olisivat hänen mukaan lähes poikkeuksetta ainakin suhteellisuusvaatimuksen vastaisia.¹⁵⁸

Perusoikeuden ydinalueen olemassaolo on kuitenkin riidatonta, vaikkakin sen ytimen määrittely tuottaa ongelmia. Viimekätinen raja perusoikeuden ydinalueen koskemattomuudelle voidaan asettaa siten, ettei oikeuden rajoittaminen saa mennä pisteeseen, jossa rajoitus tekisi perusoikeuden tyhjäksi tai merkityksettömäksi. Metsärannan käsityksen mukaan *”luottamuksellisen viestin suojan voi katsoa tulevan merkityksettömäksi, viimeistään silloin, kun yksityisiä viestejä voidaan seurata niin usein, että yksilöt eivät uskalla enää käyttää viestintävälineitä yksityisiin viesteihin tai jos he eivät enää uskalla ilmaista itseään vapaasti ja omana itsenään. Tällainen tilanne syntyisi silloin, jos yksilöt eivät voisi riittävällä varmuudella olettaa, että heidän viestejään ei seurata ja kuunnella”*.¹⁵⁹ Täysin kohdentamattomana suoritettava tietoliikennetiedustelu massavalvontana tekisi todennäköisesti luottamuksellisen viestin suojan merkityksettömäksi. Tämän välttämiseksi tietoliikennetiedustelun olisi perustuttava salaisten pakkokeinojen käyttämisen tavoin tuomioistuimen myöntämään lupamenettelyyn ja sen mukana tuomiin rajoituksiin.

Huolimatta perusoikeuden ydinalueen määrittelyn ongelmista, takaa perusoikeuden suojan toteutumista onneksi muut rajoitusedellytykset. Yleiset rajoitusedellytykset käsitetään oikeuskirjallisuudessa kokonaisuutena, eräänlaisena testinä, jossa perusoikeusrajoitusten tulee täyttää samanaikaisesti kaikki yleisiä rajoitusedellytyksiä koskevassa luettelossa mainitut vaatimukset.¹⁶⁰

¹⁵⁷ Metsäranta 2015, s. 107 – 108.

¹⁵⁸ Hautamäki 2011, s. 86 – 87.

¹⁵⁹ Metsäranta 2015, s. 110 – 111.

¹⁶⁰ Hautamäki 2011, s. 83.

Perustuslakivaliokunnan mietinnössä perusoikeusrajoitusten *suhteellisuusvaatimus* on määritelty seuraavasti: ”rajoitusten tulee olla välttämättömiä hyväksyttävän tarkoituksen saavuttamiseksi ja rajoitus on sallittu ainoastaan, jos rajoituksen taustalla oleva tavoite ei ole saavutettavissa perusoikeuteen vähemmän puuttuvin keinoin. Rajoitus ei myöskään saa mennä pidemmälle kuin on perusteltua, kun otetaan huomioon rajoituksen taustalla olevan yhteiskunnallisen intressin painavuus suhteessa rajoitettavaan oikeushyvään”.¹⁶¹

Suhteellisuusvaatimuksen toteutumisen arvioinnissa on Viljasen mukaan punninta tehtävä perusoikeuden takaamien intressien ja perusoikeuden rajoittamisen taustalla olevien intressien välillä. Asetelmassa ovat vastakkain siis rajoitettavaksi aiotun yksilön perusoikeuteen kiinnittyvä intressi ja perusoikeuden rajoittamiseen oikeuttava intressi eli hyväksyttävä rajoitusperuste. Se kuinka suuren painoarvon vastakkaiset intressit saavat, määräytyy muun muassa sen mukaan kuinka vahvan tuen perusoikeus saa perustuslaista, sen esitöistä ja eduskunnan perustuslakivaliokunnan tulkintakäytännöstä.¹⁶² Tietoliikennetiedustelun sallimista perustellaan muun muassa kansallisen turvallisuuden takaamisella. Tämän intressin painoarvo tullaan näkemään tiedustelulakien säätämisen siinä vaiheessa, jossa pitää tehdä punninta yksilön perusoikeutta turvaavan intressin ja sitä rajoittavan intressin eli kansallisen turvallisuuden välillä.

Viljasen mukaan perusoikeusrajoituksia koskeva punnintasääntö voisi kuulua seuraavasti:

*”Mitä enemmän perusoikeutta A rajoitetaan tavoitteen B vuoksi, sitä tärkeämpää tulee olla B:n toteutuminen.”*¹⁶³

Suhteellisuusvaatimus sisältää myös perusoikeuksien rajoituksilta vaadittavan *välttämättömyysvaatimuksen* eli rajoitusperusteen on oltava välttämätön hyväksyttävän tarkoituksen saavuttamiseksi. Ollakseen välttämätöntä, perusoikeutta rajoittavalta sääntelyltä edellytetään sitä, ettei ole olemassa muuta yhtä tehokasta vaihtoehtoista keinoa, joka rajoittaisi perusoikeutta vähemmän verrattuna valittuun keinoon tai sitä ei rajoiteta lainkaan.¹⁶⁴ Kyse on siis perusoikeusrajoitusten minimoinnista, käsillä olevien vaihtoehtojen valinnassa ja vaihtoehtojen tehokkuuden arvioinnista.

¹⁶¹ PeVM 25/1994 vp. s. 5.

¹⁶² Viljanen 2001, s. 210 – 211.

¹⁶³ Ibid, s. 215 – 216.

¹⁶⁴ Ibid, s. 205 – 206, 212.

4.4 Kansainvälisten perus- ja ihmisoikeussopimusten vaatimukset

Mietinnössä käsitellään kansainvälisten ihmisoikeussopimusten asettamia vaatimuksia yksityiselämän suojan ja luottamuksellisen viestin salaisuuden osalta seuraavissa sopimuksissa: YK:n kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (ns. KP-sopimus; SopS 8/1976), Euroopan ihmisoikeussopimus (EIS; SopS 63/1999), Euroopan unionin perusoikeuskirja.

Luottamuksellisen viestinnän suojasta säädetään KP-sopimuksen artiklassa 17, jonka mukaan *”kenenkään yksityiselämään tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua”*. Artiklan 17 kieltoa ei ole määritelty ehdottomaksi, se koskee vain ”mielivaltaista” ja ”laitonta” oikeuksiin puuttumista. Puuttumisen oikeuttavista tilanteista ja puuttumisessa käytettävistä keinoista voidaan säätää kansallisessa lainsäädännössä, ja näin kaikki sopimusvaltiot ovat tehneetkin. Luottamuksellisen viestin suojaa rajoittava kansallinen laki ei saa olla sisällöltään eikä sovelluttavuudeltaan mielivaltainen. Lisäksi laissa on tarkasti yksilöitävä kaikki olosuhteet, joissa puuttuminen on sallittua. Pelkkä lailla säätäminen ei siis ole riittävää.¹⁶⁵

Arvioitaessa uusien tiedustelutoimivaltuuksien ja –menetelmien sallittavuutta, on em. KP-sopimusta suurempi merkitys Euroopan neuvoston ihmisoikeussopimuksella (EIS), jonka noudattamista valvoo Euroopan ihmisoikeustuomioistuin (EIT). EIS:n suurempi merkitys perustuu siihen, että sen noudattamista valvotaan tiukemmin ja siihen, että EIT:n ratkaisukäytäntö on muovannut sen säännösten tulkintakäytännöstä yksityiskohtaisempaa.¹⁶⁶

Euroopan ihmisoikeussopimuksen 8(1) artiklan mukaan *”[j]okaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.”* EIS 8(2) artiklan mukaan *” [v]iranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.”*

EIS 8(2) artikla Lohsen mukaan mahdollistaa yksityiselämään ja kirjeenvaihtoon puuttumisen silloin ”kun laki sen sallii”. Euroopan ihmisoikeustuomioistuimen (EIT) ratkaisukäytäntö on vakiintunut EIS 8 artiklassa turvattujen oikeuksien rajoittamisen osalta. Ratkaisukäytännön mukaan kansallisen

¹⁶⁵ Tiedonhankintalakityöryhmän mietintö 2015, s. 51.

¹⁶⁶ Metsäranta 2015, s. 23.

lain pitää kuitenkin täyttää kolme laatukriteeriä: 1) lain tulee olla yleisesti saatavilla, 2) vaikutuksiltaan ennakoitava ja 3) oikeusvaltioperiaatteen mukainen.¹⁶⁷ Aivan kuten KP-sopimuksen artiklan yksityiselämän suojaan puuttuminen, edellyttää EIS 8(2) artiklassa mainittuihin oikeuksiin puuttuminen muutakin kuin sen pelkkää lain olemassaoloa.

Edellä mainittujen laatukriteerien lisäksi EIS 8(1) artiklan takaamiin oikeuksiin saa puuttua vain, mikäli puuttumisella tavoitellaan hyväksyttävissä olevaa päämäärää, jotka on luetteloitu tyhjentävästi 8 artiklan 2 kappaleessa.¹⁶⁸ Kansallinen turvallisuus on yksi hyväksyttävistä päämääristä. Mikael Lohse luettelee kybervakoilua koskevassa artikkelissaan kansallisista turvallisuutta uhkaavina tekoina muun muassa aseellisen hyökkäyksen, terrorismin ja vakoilun. Käsityksensä näiden tekojen kuulumisesta kansallisen turvallisuuden käsitteen piiriin, hän perustaa viiteen¹⁶⁹ EIT:n ennakkotapaukseen.¹⁷⁰

Metsärannan mukaan viimeisin EIS 8 artiklan ehto sille, että viranomaisten sallitaan puuttua artiklan takaamiin oikeuksiin, on vaatimus siitä, että puuttuminen on *välttämätöntä demokraattisessa yhteiskunnassa*. Puuttumiselta edellytetään ensinnäkin sitä, että sitä vaatii painava yhteiskunnallinen tarve. Toiseksi sen tulee täyttää suhteellisuusperiaatteen vaatimukset: *”oikeuksia ei voi rajoittaa enempää kuin on välttämätöntä painavan yhteiskunnallisen tarpeen perusteella”*.¹⁷¹

Yhteenvedon voidaan todeta, että EIT:n ratkaisukäytännön perusteella EIS 8(1) artiklan takaamiin yksityiselämän suoja-oikeuksiin voidaan puuttua kansallisen turvallisuuden vuoksi, jos kansallinen laki täyttää määrättyt laatukriteerit ja kun puuttumisen katsotaan olevan välttämätöntä.

Vastapainona yksityiselämän suoja-oikeuksiin puuttumiseen kansallisen turvallisuuden nimissä, on EIT päätöksissään korostanut, että viranomaisten harjoittama salainen tarkkailu ja valvonta voivat vaarantaa demokraattisen yhteiskuntajärjestyksen. Tällaisen vaaran torjumiseksi valtioiden tulee järjestää viranomaisten salaisten tiedonhankintakeinojen käytön riippumaton valvonta ja kansalaisille tehokkaat oikeussuojakeinot. EIT päätösten mukaan salaisia tiedonhankintakeinoja koskevan laillisuusvalvonnan tulee olla muun muassa avointa ja läpinäkyvää sekä sääntelyltään riittävän täsmällistä, sen uskottavuuden takaamiseksi, kuitenkin vaarantamatta salaisen tiedonhankinnan

¹⁶⁷ Lohse DL 4/2015, s. 767.

¹⁶⁸ Metsäranta 2015, s. 25.

¹⁶⁹ *Klass and others v. Germany* (5029/71), Judgment of 6 September 1978 kohta 48, *Weber and Saravia v. Germany* kohta 27 ja 96 ja *Segerstedt-Wiberg and others v. Sweden* (62332/00), Judgment of 6 June 2006 kohdat 81 ja 87.

¹⁷⁰ Lohse DL 4/2015, s. 768.

¹⁷¹ Metsäranta 2015, s. 25.

tarkoitusta. Demokratian suojelemisen kannalta olisi lisäksi toivottavaa, että kunkin valtion kansanedustuslaitos osaltaan osallistuisi salaisten tiedonhankintavaltuuksien valvontaan.¹⁷²

EU-oikeuden osalta arvioitaessa tietoliikennetiedustelun lainmukaisuutta tarkasteltavaksi tulevat Euroopan unionin perusoikeuskirjan (myöh. perusoikeuskirja) artikkelit 7 ja 8. Yksityiselämän suojasta säädetään perusoikeuskirjan artiklassa 7, jonka mukaan ”[j]okaisella on oikeus siihen, että hänen yksityis- ja perhe-elämänsä, kotiaan sekä viestejään kunnioitetaan.”

Perusoikeuskirjan 8 artiklan mukainen oikeus henkilötietojen suojaan edellyttää, että:

1. *”Jokaisella on oikeus henkilötietojensa suojaan.*
2. *Tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.*
3. *Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.”*

Oikeutta yksityiselämän kunnioittamiseen ja henkilötietojen suojaan eivät ole perusoikeuskirjankaan mukaan absoluuttisia. Perusoikeuskirjan 52 artikla on niin sanottu yleinen rajoituslauseke, jonka tarkoituksena on kattaa kaikkien perusoikeuskirjan oikeuksien rajoitukset.¹⁷³ 52 artiklan 1. kohdan mukaan:

1. *”Tässä perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämisestä voidaan rajoittaa ainoastaan lailla sekä kyseisten oikeuksien ja vapauksien keskeistä sisältöä kunnioittaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan säätää ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.”*

Perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien rajoittamisen edellytyksiä ovat; lailla säätämisen vaatimus, perusoikeuden ydinalueen koskemattomuuden vaatimus sekä suhteellisuus- ja välttämättömyysvaatimukset. Sisällöllisesti rajoituslauseke vastaa hyvin pitkälle Euroopan ihmisoikeussopimuksen 8(2) artiklan rajoituslauseketta ja EIT:n ratkaisukäytäntöä sen tulkinnasta. Sisältöjen vastaavuuden taustalla on se, että perusoikeuskirjassa vahvistetut perus- ja ihmisoikeudet perustuvat sekä Euroopan ihmisoikeussopimukseen, että Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön.¹⁷⁴

¹⁷² Tiedonhankintalakiyöryhmän mietintö 2015, s. 56.

¹⁷³ Tiilikainen – Helander – Heliskoski 2005, s. 70.

¹⁷⁴ Tiedonhankintalakiyöryhmän mietintö 2015, s. 57.

Perusoikeuskirjassa säädettyjen perusoikeuksien kunnioittamisen valvonta kuuluu Euroopan unionin tuomioistuimelle (EUT) ja kansallisille tuomioistuimille. Yksityiselämän kunnioittamisen ja henkilötietojen suojan sekä tietoliikennetiedustelun kannalta merkittävä EUT:n tuomio annettiin huhtikuussa 2014. EUT katsoi tuomiossaan vuodelta 2006 olevan Data Retention –direktiivin (2006/24/EY) olevan pätemätön. Direktiivi muun muassa velvoitti unionin jäsenvaltiota säilyttämään kattavasti teletunnistamistietoja vakavien rikosten torjunnan ja tutkinnan tarpeita varten.¹⁷⁵

Direktiivillä velvoitettiin sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen tarjoajia säilyttämään muun muassa viestin lähettäjän ja vastaanottajan jäljittämiseen ja tunnistamiseen tarvittavat tiedot. EUT toteaa tuomiossaan, että direktiivin vaatimalla tavalla säilytettävien tietojen avulla on mahdollista tehdä hyvin tarkkoja päätelmiä viestintäpalveluja ja –verkoja käyttäneiden henkilöiden yksityiselämästä, elämäntavoista, oleskelupaikoista, päivittäisistä liikkeistä, tekemisistä ja tätä kautta heidän sosiaalisesta ympäristöstään.¹⁷⁶

EUT käsitteli tapauksessa ennakkoratkaisukysymyksinä kaikkia neljää edellytystä, joilla perusoikeuskirjassa tunnustettuja oikeuksia ja vapauksia voidaan rajoittaa. Rajoitusedellytysten on 1) perustuttava lakiin, 2) kunnioitettava kyseisten oikeuksien keskeistä sisältöä, 3) vastattava unionin tunnustamia yleisen edun mukaisia tavoitteita tai suojella muiden henkilöiden oikeuksia ja 4) oltava suhteellisuusperiaatteen mukaisesti välttämättömiä. Tuomion perusteluissa EUT katsoi direktiivin täyttävän edellä mainituista kolme ensimmäistä rajoitusedellytystä, mutta ei suhteellisuusperiaatteen mukaista välttämättömyysvaatimusta sen tavoitteiden toteuttamiseksi.¹⁷⁷ EUT totesi tuomiossaan unionin lainsäätäjän ylittäneen säätämällään direktiivillä 2006/24 suhteellisuusperiaatteen rajat, joita perusoikeuskirjan 7 ja 8 artiklan ja 52 artiklan 1 kohdan noudattamiselta edellytetään.¹⁷⁸

Vaikka EUT katsoikin tietojen säilyttämisellä saavutettavan direktiivin 2006/24 tavoitteen - vakavan rikollisuuden, kuten järjestäytyneen rikollisuuden ja terrorismin, ehkäiseminen, tutkinta, selvittäminen ja syyteharkinta yleisen turvallisuuden takaamiseksi – ei tuo tavoite kuitenkaan voi yksin oikeuttaa katsomaan direktiivissä säädetyn kaltaista säilyttämistoimenpidettä välttämättömäksi. Puuttuessa perusoikeuskirjassa turvattuihin oikeuksiin vaaditaan niihin puuttuvilta toimenpiteiltä

¹⁷⁵ Tiedonhankintalakiyöryhmän mietintö 2015, s. 57.

¹⁷⁶ EUT:n tuomio C-293/12, kohta 26 – 27.

¹⁷⁷ Walkila 2015, s. 801.

¹⁷⁸ EUT:n tuomio C-293/12, kohta 69.

riittävää tarkkaraisuutta ja täsmällisyyttä. EUT totesi tuomiossaan, että direktiivin 2006/24 sisältämä puuttuminen koski kaikkia sähköisen viestinnän välineitä, joiden käyttäminen on nykyisin erittäin yleistä ja laajaa. Lisäksi tuomiossa todettiin, että näiden viestintävälineiden käyttö on nykyisin ja tulevaisuudessa merkittävässä asemassa meidän jokaisen arjessa, ja näin ollen direktiivillä puututtiin lähes kaikkien Euroopan asukkaiden perusoikeuksiin ilman minkäänlaista erottelua, rajoituksia tai poikkeuksia vakavan rikollisuuden torjunnan tavoitteen perusteella.¹⁷⁹

5 Tutkimusasetelma

5.1 Tutkimuskysymys

Tutkimuksen tarkoituksena on selvittää minkälaisilla uhkakuvilla tai muilla perusteilla tiedustelulakihanketta Suomeen vaaditaan sekä minkälaisia argumentteja lainvalmistelussa mukana olevat osapuolet esittävät niistä toimivaltuuksista ja keinoista, joilla tiedustelua olisi tarkoitus harjoittaa. Lisäksi pyrkimyksenä on saada selville mitkä perus- ja ihmisoikeudet ja miten niitä vaaditaan huomioonotettavaksi säädösprosessin valmisteluvaiheessa. Tutkimusongelma jakaantuu kolmeen alakysymykseen:

1. Mitkä ovat pääasialliset uhat, joita tiedustelulla pyritään torjumaan?
2. Minkälaisin argumentein tiedustelulakihanketta puolletaan tai vastustetaan? Minkälaisin reunaehdoin tietoliikennetiedustelu voitaisiin hyväksyä?
3. Mitä perus- ja ihmisoikeuskysymyksiä esitetään mietinnössä ja lausunnoissa sekä miten niitä vaaditaan huomioonotettavaksi lakihankkeessa?

5.2 Aineisto ja tutkimusmetodi

5.2.1 Aineisto

Tiedonhankintalakityöryhmän mietintö lähetettiin 9.2.2015 varsin laajalle lausuntokierrokselle ja lausuntoa pyydettiin eri ministeriöiltä, viranomaisilta, puolueilta, järjestöiltä, yrityksiltä ja yhteisöiltä, yhteensä 150:ltä eri taholta. Lisäksi lausunnot pyydettiin erikseen professori Martin Scheininiltä European University Institutesta, apulaisprofessori Juha Lavapuroilta Tampereen yliopistosta ja professori Tomi Voutilaiselta Itä-Suomen yliopistosta. Koska analysoitava lausuntoaineisto oli varsin

¹⁷⁹ EUT:n tuomio C-293/12, kohdat 24, 49, 54, 56 ja 57.

laaja, olen jakanut lausunnot niiden antajien organisaatiotyyppien ja niiden tehtävien sekä roolin mukaan eri ryhmiin, joista tarkemmin luvussa 5.2.4.

Tämän tutkimuksen aikana tiedustelulakihanke on luonnollisesti jatkunut ja edennyt. Hallituksen esitys (HE 202/2017 vp) eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi annettiin 25.1.2018. Tässä tutkimuksessa kuitenkin käytetään pääasiassa aineistoa, joka oli tiedustelulakihankkeesta saatavilla toukokuussa 2015 ja kohteena on lainsäädäntöprosessin ensimmäisen lausuntokierroksen valmisteluvaihe. Pääasiallisina virallislähteinä tässä vaiheessa - ennen hallituksen esityksen antoa – olivat;

- Tiedonhankintalakityöryhmän mietintö lausuntopyyntöineen,
- Liikenne- ja viestintäministeriön edustajan eriävä mielipide em. mietintöön,
- Tiedonhankintalakityöryhmän mietinnöstä annetut 74 erillistä lausuntoa (252 A4 –sivua).

Neljällä lausunnonantajalla ei ollut lausuttavaa asiassa ja 13:sta lausunnossa ei ollut tutkimuskysymyksiin liittyvää sisältöä. Lausuntoja käsitellään tarkemmin luvussa 7.

Tutkittavaan aineistoon ei mielestäni liity sellaisia tutkimuseettisiä seikkoja, jotka tulisi ottaa huomioon esimerkiksi yksityisyyden suojan kannalta, koska aineisto on kaikkien saatavilla ja se on kaikilta osin julkista.

Tiedonhankintalakityöryhmän mietintöä ei ole kirjoitettu hallituksen esityksen muotoon, dokumentin nimi on *Suomalaisen tiedustelulainsäädännön suuntaviivoja*.

Tässä vaiheessa on lukijalle hyvä muistuttaa, että säädöspolitiikka ja lainvalmistelun todellisuus tulee erottaa toisistaan. Lainvalmistelun laatua tutkineen Pakarisen mukaan on esimerkiksi havaittu, että sidosryhmien osallistumisen tärkeyden painottaminen on säädöspolitiikassa suhteellisen uutta. Hänen havainto ei kuitenkaan tarkoita siitä, että sidosryhmien mukaan ottaminen lainvalmisteluun olisi ilmiönä tuore, vaan että sen on vasta viime vuosina ymmärretty olevan yksi hyvän lainvalmistelun tärkeistä kriteereistä.¹⁸⁰

Ainakin tiedustelulakihankkeesta eri tahoilta pyydettyjen lausuntojen ja annettujen lausuntojen määrän perusteella voidaan ajatella, että tiedustelulakien säätämisen valmisteluvaiheessa sidosryhmien osallistumismahdollisuudet on toteutettu niin kutsutun paremman sääntelyn toimintaohjelman mukaisesti. Toinen asia on kuitenkin se, miten annetut lausunnot tulevat huomioonotetuksi valmistelun edetessä hallituksen esitysvaiheeseen.

¹⁸⁰ Pakarinen 2012, s. 30 – 31.

5.2.2 Laadullinen tutkimus

Jotta tutkija pystyy määrittelemään oman metodisen orientaationsa, tulee hänen Keinänen ja Väätsen mukaan tunnistaa oma tutkimusintressinsä. Lainopilliseen tutkimuskysymykseen ei voi vastata empiirisellä aineistolla (pääsääntöisesti) ja toisinpäin: empiirisen tutkimuksen kysymykseen ei voi vastata lainopillisella tutkimuksella. Koska tutkimuskysymyksiini liittyvät mm. lainsäätämisen taustalla olevien syiden (uhkien) tutkimiseen, edellyttää kysymyksiini vastaaminen empiiristä tutkimusotetta. Empiirisessä oikeustutkimuksessa tutkimusote voi olla määrällinen eli kvantitatiivinen tai laadullinen eli kvalitatiivinen. Tutkimusongelmasta ja tutkimuksen tarkoituksesta riippuu, kumpi lähestymistapa sopii paremmin.¹⁸¹

Laadullisen tutkimuksen aineisto on ilmiänsuhtaan tekstiä, jonka on kirjoittanut joko tutkija itse tai se on syntynyt tutkijasta riippumatta. Teksti voi olla valmista - olemassa olevaa – tekstimateriaalia, joka on tuetettu muuta tarkoitusta varten tai tutkijan esimerkiksi haastattelu- tai havainnointi menetelmällä hankkimaa aineistoa. Aineisto voi muodostua myös valmiista dokumenteista kuten eri viranomaisten tai muiden tahojen toimesta syntyneistä asiakirjoista (lainvalmistelumateriaali, viranomaispäätökset, tuomioistuinten ja laillisuusvalvojen ratkaisut, valitus- ja kanteluasiakirjat).¹⁸² Koska tutkimuskysymykset määrittävät hankittavan ja käytettävän aineiston, on tämän tutkimuksen käytettäväksi aineistoksi valikoitunut tiedustelulakien valmistelussa syntyneet valmiit dokumentit.

Tämän tutkimuksen pääasiallisena tutkimusmenetelmänä on kvalitatiivinen eli laadullinen, jonka tarkoituksena on sisällönanalyysin keinoin löytää ja eritellä aineistosta esiin nousevia teemoja ja argumentteja. Käytin tutkimuksessa myös kvantitatiivisen eli määrällisen tutkimuksen keinoja laskiessani lausunnoissa esitettyjen uhkien lukumääriä saadakseni selville mitkä uhat esiintyvät lausunnoissa suurimpina uhkina. Laskin myös puoltavien ja vastustavien argumenttien lukumäärällistä jakaantumista muodostamieni kategorioiden välillä. Myöskin perusoikeuksien osalta jouduin laskemaan niistä maininnat, saadakseni selville, mitkä perusoikeudet olivat lausunnonantajille tärkeimpiä.

Tuomen ja Sarajärven mukaan laadullisen aineiston sisällönanalyysi voi olla joko aineistolähtöistä, teoriaohjaava tai teorialähtöistä.¹⁸³ Tutkimuskysymyksistä johtuen tutkimusprosessia aloittaessani kävi jo selväksi, että aineistosta tulee etsiä tiedustelulakihanketta puoltavia ja vastustavia

¹⁸¹ Keinänen – Väätsen 2015, s. 6 – 7.

¹⁸² Keinänen – Väätsen 2015, s. 12.

¹⁸³ Tuomi – Sarajärvi 2009, s. 108.

argumentteja sekä lausunnoissa esiintuotuja perusoikeuskysymyksiä. Näin ollen tämän tutkimuksen sisällönanalyysi on aineistolähtöistä.

5.2.3 Aineistolähtöinen sisällönanalyysi

Tutkimuskysymysten analyysitavaksi valikoitui aineistolähtöinen sisällönanalyysi. Sisällönanalyysiä pidetään menettelytapana, jolla voidaan analysoida kirjalliseen muotoon saatettuja dokumentteja. Sisällönanalyysin tarkoituksena on saada kerätty aineisto järjestetyksi sellaiseen muotoon, että siitä voidaan tehdä tutkimuksen johtopäätökset. Useimmat laadulliset tutkimusmenetelmät perustuvat periaatteessa sisällönanalyysiin, vaikka näillä menetelmillä onkin useita nimiä. Sisällönanalyysin tarkoituksena on kuvata tutkittavaa ilmiötä sanallisesti ja luoda siitä selkeä kuva. Analyysin avulla tutkittava aineisto saa uuden muodon. Tavoitteena on, että muoto olisi tiivis ja selkeä, sisältäen kuitenkin aineiston alkuperäisen informaation. Tarkoituksena on aineiston informaatioarvon lisääminen, jolloin hajallaan olevasta ja mahdollisesti laajastakin aineistosta saadaan mielekästä, selkeää ja yhtenäistä informaatiota.¹⁸⁴

Sisällönanalyysi alkaa Tuomen ja Sarajärven mukaan valitsemalla analyysiyksikkö, joka voi olla yksittäinen sana, lause, lauseen osa tai ajatuskokonaisuus, joka voi koostua useista lauseista. Heidän mukaan aineistolähtöinen laadullinen analyysi on kolmivaiheinen prosessi. 1) Ensimmäisessä vaiheessa analysoitava informaatio esim. asiakirjassa redusoidaan eli pelkistetään siten, että siitä karsitaan tutkimuskysymysten kannalta epäolennainen pois. Jäljelle jää alkuperäiset tai pelkistetyt ilmaukset osina kokonaisinformaatiosta. 2) Seuraavana vaiheena on pelkistetyn aineiston klusterointi eli ryhmittely, jossa alkuperäiset tai pelkistetyt ilmaukset kootaan niiden sisällön mukaisesti omiksi teemoiksi. Teemoittelun yksikkönä toimii esimerkiksi tutkittavan ilmiön ominaisuus, piirre tai käsitys niiden sisällön mukaan. Teemoittelun avulla tutkija luo pohjan tutkimuksen perusrakenteelle ja alustavia kuvauksia tutkittavasta ilmiöstä. 3) Viimeisensä vaiheena on abstrahointi, jossa erotetaan tutkimuksen kannalta olennainen tieto ja valikoidun tiedon perusteella tuloksissa esitetään empiiristä aineistoa kuvaavat teemat.¹⁸⁵

Tekstin analysointia aloittaessani minulla ei ollut tarkkaa ajatusta siitä miten sen tekisin. Koska analysoitava lausuntoaineisto oli varsin laaja, päätin jakaa lausunnot niiden antajien organisaatiotyyppien ja niiden tehtävien sekä roolin mukaan eri ryhmiin seuraavasti;

¹⁸⁴ Ibid, s. 103 ja 108.

¹⁸⁵ Ibid, s. 108 – 113.

1) asiantuntijat,

Martin Scheinin, kansainvälisen oikeuden ja ihmisoikeuksien professori, Eurooppalainen yliopistollinen instituutti EUI.

Juha Lavapuro, julkisoikeuden apulaisprofessori, Tampereen yliopisto.

Tomi Voutilainen, julkisoikeuden professori ja IT-oikeuden dosentti, Itä-Suomen yliopisto.

2) etujärjestöt,

ammattiyhdistykset ja –liitot:

Maanpuolustuksen Insinöörit MPI ry, Puolustusvoimien Diplomi-Insinöörit ry, Palkansaajajärjestö Pardia ry, Suomen Journalistiliitto ry.

Kansalaisjärjestöt:

Amcham Finland ry, Electronic Frontier Finland - Effi ry, Suomen Sadankomitea ry, Internet käyttäjät ikuisesti IKI ry ja Suomen rauhanturvaajaliitto ry.

Yritysten etu- ja yhteistyöjärjestöt:

Teknologiaeollisuus ry ja Ohjelmistoyrittäjät ry, Viestinnän keskusliitto ry, Tietoturvaklusteri FISC ry, FICIX ry, Elinkeinoelämän keskusliitto ry, Tieto- ja viestintätekniikan ammattilaiset TIVIA ry, Suomen puolustus- ja ilmailuteollisuusyhdistys PIA ry, Keskuskauppakamari, Suomen Asianajajaliitto, Finnet-liitto ry, Suomen Microsoft osaajakumppaneiden yhdistys ry ja Tietoliikenteen ja tietotekniikan keskusliitto, FiCom ry.

3) laillisuusvalvojat,

oikeuskanslerinvirasto, eduskunnan oikeusasiamies ja tietosuojavaltuutettu.

4) ministeriöt ja niiden yhteydessä tai alaisuudessa toimivat viranomaistahot,

Viestintävirasto, Tulli, Rajavartiolaitos, Turvallisuuskomitea, Huoltovarmuuskeskus, valtioneuvoston kanslia, Huoltovarmuuskeskus, työ- ja elinkeinoministeriö, sisäministeriö, opetus- ja kulttuuriministeriö, liikenne- ja viestintäministeriö, puolustusministeriön viestintäyksikkö, maa- ja metsätalousministeriö, puolustusministeriön hallintopoliittinen osasto, oikeusministeriö, sosiaali- ja terveysministeriö ja valtionvarainministeriö.

5) poliisiorganisaatiot ja valtakunnansyyttäjävirasto,

suojelupoliisi, Poliisihallitus, Poliisiammattikorkeakoulu ja keskusrikospoliisi.

6) puolueet,

Vasemmistoliitto, Suomen ruotsalainen kansanpuolue, Vihreä liitto, Suomen Sosialidemokraattinen puolue, Suomen Keskusta, Suomen Kristillisdemokraatit ja Piraattipuolue.

Mielenkiintoinen havainto tutkimuksen tässä vaiheessa oli, ettei Suomen kahdeksasta pääpuolueesta Kansallinen kokoomus eikä Perussuomalaiset olleet antaneet lainkaan lausuntoa työryhmän mietintöön lakihankkeen tässä vaiheessa. Kokoomuksen osalta tätä voisi selittää sen valikoituminen 2015 hallitukseen vaalituloksensa perusteella ja tieto siitä, että tuo hallitus tulee esittämään tiedustelulakien säätämistä.

7) vrtvket.

Finnvera Oyj, TeliaSonera Finland Oyj, Cinia Group Oy, Suomen Erillisverkot Oy, Patria Oyj, Nixu Oyj, Dna Oy, Fujitsu Finland Oy, BaseN Oy, Prof-Tel Oy, CSC - Tieteen tietotekniikan keskus Oy, Nokia Oyj, SSH Communication Security Oyj, Tieto Oyj ja Microsoft Oy.

Työn helpottamiseksi tein lausunnonantajista ja lausunnoista excel –taulukon, johon lausunnot koottiin ja numeroitiin. Koska annettujen lausuntojen määrä (72 kpl) oli melko suuri, helpotti taulukko työtä, kun jouduin jostain syystä palaamaan alkuperäisiin lausuntoihin.

Aloitin varsinaisen analyysin lukemalla lausunnot ja kahden eriävän mielipiteen (72 kpl, sivuja 252) ryhmittäin useaan kertaan. Vähitellen lukuprosessin edetessä alkoi aineistosta hahmottua tutkimuskysymysten kannalta keskeisiä teemoja. Aineistoa lukiessani erittelin ja keräsin lausunnoista tutkimuskysymyksiin liittyviä alkuperäisiä ilmaisuja excel –taulukoihin lausunnonantajaryhmittäin. Lausuntojen luokittelu antajaryhmiin mielestäni helpotti minua muodostamaan yhteisiä aihealueita, koska ilmeni, että ryhmien sisällä näkemykset tiedustelulakihankkeesta ja käytetyt argumentit jonkin verran vastasivat toisiaan.

Aineistolähtöisen analyysin perusteella aloitin lausuntojen osalta selvittämällä mitä kaikkea tutkimuskysymyksiin liittyvää niistä löytyi. Lausunnoista kävi hyvin pian selville, että lausunnonantajat rajoittuvat lausumaan vain heille merkityksellisistä asioista jättäen pois keskustelusta heille mahdollisesti epämieluisia tai heille vähemmän tärkeitä näkökulmia.

Aineiston redusointi vaiheesta tein jokaisesta lausunnosta excel –taulukoon (kaavio 3.) oman rivin, johon koottiin argumentit, joilla mietinnössä esitettyjä tiedustelua koskevan lainsäädännön kehittämissuhteita ja johtopäätöksiä puollettiin tai vastustettiin. Tässäkin vaiheessa käsittelemäni lausuntoja edellä olevan ryhmittelyn mukaisesti aina yhden ryhmän kerrallaan, joten kaikille ryhmille tehtiin oma taulukko. Samassa yhteydessä poimin taulukkoon lausunnonantajan kannan tietoliikennetiedustelun suhteesta perustuslakiin ja ne perusoikeudet, joita lausunnonantaja katsoi mietinnössä esitettyjen tiedustelumenetelmien rajoittavan.

Kaavio 3. Redusointi vaiheen taulukko

Lausunnonantaja	Uhat	Perusoikeuskysymykset	Argumentit vastaan	Argumentit puolesta
XXX	Mainitut uhat	Alkuperäinen ilmaus	Alkuperäinen ilmaus	Alkuperäinen ilmaus
YYY	Mainitut uhat	Alkuperäinen ilmaus	Alkuperäinen ilmaus	Alkuperäinen ilmaus

Lausunnoista poimittiin niin ikään niissä mainitut uhkat, joita tiedustelulla pyrittäisiin tunnistamaan ja torjumaan. Kaikista lausunnoista yhteen koottu dokumentti helpotti jatkossa tekstianalyysin tekoa, koska alkuperäisiin lausuntoihin ei enää tarvinnut palata kuin satunnaisesti tarkistusmielessä.

Tämän jälkeen jaoin perusoikeuskysymykset, argumentit puolesta ja vastaan omiin taulukoihin (kaavio 4.). Sijoitin kaikkien lausuntojen tutkimuskysymyksiin liittyvät alkuperäiset ilmaisut taulukkoon ja pelkistin ilmaisuja, jonka jälkeen erittelin niistä yksinkertaistetut ydinargumentit.

Kaavio 4. Esimerkki vastustavien lausuntojen taulukosta

Lausunnonantaja	Argumentit vastaan	Pelkistetty ilmaus	Argumentti 1	Argumentti 2
XXX	Alkuperäinen ilmaus	Pelkistetty ilmaus	Tietoverkkotiedustelu ei ole tehokasta, koska viestien salausta on yleistynyt.	”Rajat ylittävä tietoliikenne” sisältää myös suomalaisten välistä kommunikaatiota.
YYY	Alkuperäinen ilmaus	Pelkistetty ilmaus	Verkkovalvonta heikentäisi tietoturvaa.	Kansalaisten luottamus yhteiskuntaan heikkenee.

Edellä olevassa esimerkissä on vain kaksi vastustavaa argumenttia, mutta useissa lausunnoissa niitä oli tietysti useampiakin, jotka kaikki sijoitin lausunnonantajakohtaisesti taulukkoon. Tätä samaa menetelmää käytin siis myös perusoikeuskysymysten ja puolesta olevien argumenttien tiivistämisessä.

Etsiessäni lausunnoista perusoikeuskysymyksiä sijoitin ne lausujakohtaisesti laatimaani taulukkoon. Tämän jälkeen ryhdyin erittelemään lausuntokohtaisesti esiintyneet perusoikeuskysymykset toisistaan. Mitä pidemmälle perusoikeuskysymysten pilkkominen ja teemoittelu eteni, sitä selvemmäksi kävi, että lausunnonantajat käyttivät perusoikeusargumenteissaan melko usein ainakin yhtä, ellei useampaa yleisistä perusoikeusrajoituksista. Tähän havaintoon perustuen laadin työtä helpottaakseni ja asian hahmottamista parantaakseni taulukon perusoikeusrajoituksista. Näistä muotoutui eräänlaisen analyysirunko (kaavio 5.), johon sijoitin lausunnoissa esiintyvät erilliset huomiot kustakin rajoitusedellytyksen huomioonottamisesta.

Yleisistä perusoikeuksien rajoitusedellytyksistä jouduin jättämään pois oikeusturvavaatimuksen, koska olin tutkimuskysymysteni perusteella rajannut tutkimuksen ulkopuolelle tiedustelutoiminnan lupamenettelyn ja valvonnan, jotka osaksi liittyvät kansalaisten oikeusturvan toteutumiseen. Lailla

säätämisen vaatimuksen jätin myös pois analyysirungosta, koska perusoikeuksien toteutumisen kannalta lausunnoissa vaadittiin sitä huomattavasti merkityksellisempiä perusoikeuksien rajoitusedellytyksiä huomioonotettavaksi.

Kaavio 5. Perusoikeuksien rajoitusedellytysten analyysirunko

Teema 1	Teema 2	Teema 3	Teema 4	Teema 5
Suhteellisuus- ja välttämättömyys	Ydinalueen koskemattomuus	Täsmällisyys- ja tarkkarajaisuus	Ihmisoikeusvelvoitteiden noudattaminen	Hyväksyttävä tarkoitus

6 Tiedonhankintalakiyöryhmän mietintö

Suomen turvallisuusympäristön muutokset perustuvat yhä useammin kansainvälisen toimintaympäristön kehityskulkuihin ja globalisoituneisiin turvallisuuskysymyksiin. Globalisaation myötä valtioiden toiminnot ja maailmantalous ovat enenevässä määrin riippuvaisempia toisistaan. Yhdessä globalisaation tuomien muutoksien ja toimintaympäristömme voimakkaan teknistymisen kanssa nyky-yhteiskunnat ovat haavoittuvia aivan uudella tavalla, jonka huomioonottaminen edellyttää laaja-alaista turvallisuuskäsitettä. Yhteiskunnan kriittiset toiminnot ja palvelut perustuvat teknisten, erityisesti sähkön ja tietoliikenteen varassa toimivien digitaalisten järjestelmien käyttöön. Tämä on aiheuttanut yhteiskuntaan vaikuttavien laajojen häiriöiden riskin kasvun. Meidän olisi kaikissa oloissa kyettävä takaamaan yhteiskunnan elintärkeiden toimintojen jatkuvuus. Turvallisuusviranomaisten näkökulmasta tähän haasteeseen vastaaminen tiedonhankintalakiyöryhmän mukaan edellyttää, että kansalliseen turvallisuuteen kohdistuvat uhat voidaan havaita ja tunnistaa riittävän varhaisessa vaiheessa.¹⁸⁶

Tiedonhankintalakiyöryhmän asetettiin puolustusministeriön toimesta 13.12.2013. Sen tehtävänä oli kehittää lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristössä. Lisäksi työryhmän tuli arvioida Suomen kykyä torjua tietoverkoissa esiintyviä sellaisia uhkia, jotka uhkaavat meidän kansallista turvallisuutta.¹⁸⁷

Nykyisen kaltaisissa tietoyhteiskunnissa informaatio on tietoverkoissa ja henkilöiden välinen kanssakäyminenkin tapahtuu tuossa samassa tietoverkkoverkkojen kyberympäristössä. Kahden henkilön välinen yhteydenpito voi olla rajat ylittävää, vaikka he fyysisesti ovatkin samassa maassa. Tämä johtuu siitä, että heidän välinen yhteydenpito voi reitittyä ulkomailla sijaitsevien

¹⁸⁶ Tiedonhankintalakiyöryhmän mietintö 2015, s. 18.

¹⁸⁷ Ibid, s. 7.

yhteyspisteiden kautta. Samalla tavalla myöskään ns. pilvipalvelut eivät tunne fyysisiä valtioiden välisiä rajoja. Pilvipalvelun palvelimet voivat sijaita useamman valtion alueella, ja niihin tallennettu tieto on sen haltijan käytettävissä mistä fyysisestä sijainnista tahansa, kunhan haltijalla on yhteys tietoverkkoon. Kansalliseen turvallisuuteen kohdistuvien uhkien taustalla olevat toimijat käyttävät sisäisen yhteydenpitonsa välineenä tietoverkoissa tarjottavia erilaisia yhteydenpitopalveluita. Tällaista yhteydenpitoa ovat esimerkiksi tehtävänannot, niistä raportointi, tehtävien suunnittelu ja tiedonhankinta valikoiduista kohteista. Näiden uhkien torjumiseksi kansallisesta turvallisuudesta vastaavien viranomaisten onnistunut toiminta edellyttää tällaisen yhteydenpidon selville saamista. Tiedonsaanti parantaa kykyä estää tai torjua uhkien toteutumisen.¹⁸⁸

Tiedonhankintalakitöryhmän mietinnössä esitetyn näkemyksen mukaan tietoverkoissa tapahtuva kansallista turvallisuutta uhkaavien toimijoiden verkostoituminen tulee edelleen kasvamaan ja verkostoitumisen tavat tulevat monimuotoistumaan sosiaalisen median palveluiden kehittyessä. Terroristi- ja muut radikaalijärjestöt ovat olleet aktiivisia modernien mediaorganisaatioidensa kehittämisessä propagandan levittämisessä. Nämä järjestöt käyttävät laajenevassa määrin toiminnassaan sosiaalista mediaa, kuten pikaviestipalveluita (esim. WhatsApp, Facebook, Messenger), sekä ylläpitävät avoimia ja suljettuja keskusteluryhmiä. NykYTEknologia tarjoaa näille järjestöille helppokäyttöiset viestintäkanavat kahden- ja monenväliseen viestintään, toiminnan suunnitteluun ja operaatioiden reaaliaikaiseen koordinointiin.¹⁸⁹

Tietoverkkoja käytetään myös välineenä luotaessa uhkia kansalliselle turvallisuudelle. Tällaisia uhkia ovat muun muassa kybervakoilu ja kyberoperaatit. Myös näiden tietoverkkojen avulla toteutettavien uhkien merkitys tulee työryhmän näkemyksen mukaan kasvamaan tulevaisuudessa. Verkostoitumisen ja uhkien merkityksen kasvun syynä ovat tekojen alhaiset kustannukset, suojautumisen vaikeus ja kalleus sekä kiinnijäämisriskin vähäisyys. Lisäksi yhtenä kasvun syynä mietinnössä on huomioitu, että ne ulkovaltat, jotka todennäköisimmin kohdentavat Suomeen em. toimia, panostavat määrätietoisesti ja mittavasti offensiivisen kyberkapasiteettinsa rakentamiseen. Suomen kansallista turvallisuutta uhkaavien toimijoiden ja tiedustelutoimien lisääntyminen on voitu todeta konkreettisesti suojelupoliisin ylimmälle valtiojohdolle laadittujen raporttien määrän kasvuna, näiden raporttien määrä on kymmenkertaistunut vuoden 2008 jälkeen. Tiedonhankintalakitöryhmän käsityksen mukaan Suomeen kohdistuva tiedustelutoiminta tulee jatkossa lisääntymään, lisäksi turvallisuusuhkat tulevat monimutkaistumaan ja kansainvälistymään. Tästä johtuen työryhmän

¹⁸⁸ Ibid, s. 19 – 20.

¹⁸⁹ Tiedonhankintalakitöryhmän mietintö 2015, s. 20.

mukaan Suomessa tullaan tarvitsemaan yhä enemmän ja yhä laadukkaampaa tiedustelutietoa poliittisen päätöksenteon tueksi.¹⁹⁰

Tiedonhankintalakityöryhmän näkemyksen mukaan muutokset Suomen ulkoisessa turvallisuusympäristössä ja sodankäynnin luonteessa edellyttävät viranomaisten tiedonhankintamenetelmien kehittämistä, koska nykyiset toimivaltuudet eivät mahdollista uhkien havaitsemista riittävän tehokkaasti ja aikaisessa vaiheessa. Riittämättömillä toimivaltuuksilla ei kyetä ryhtymään uhkien edellyttämiin toimenpiteisiin ja ennakkovaroituksen antamiseen ajoissa. Tiedonhankintalakityöryhmä esittää kolme erillistä tiedustelumenetelmää, joilla voitaisiin tuottaa erityisen merkityksellistä tietoa Suomen kansallisen turvallisuuden näkökulmasta. Nämä ovat tietoliikennetiedustelu, ulkomaan henkilötiedustelu sekä ulkomaan tietojärjestelmätiedustelu.¹⁹¹

Viestintään kohdistuvalla tiedustelulla on työryhmän käsityksen mukaan keskeinen rooli kansalliseen turvallisuuteen kohdistuvien uhkien havaitsemisessa, koska lähes kaikki globaalista yhteydenpidosta yksityisten henkilöiden, yritysten ja julkisten toimijoiden välillä tapahtuu nykyisin kiinteässä tietoliikenneverkossa.¹⁹² Tässä tutkimuksessa keskitytään esitetyistä uusista tiedustelumenetelmistä vain tietoliikennetiedusteluun, koska mietinnössäkkin ja annetuissa lausunnoissa pääpaino on sen mahdollistamisen edellytyksissä.

Tiedonhankintalakityöryhmän mietinnössä pääasiassa käsitellään tietoverkkoympäristössä tapahtuvaa tiedustelua ja siitä aiheutuvia uhkia kansalliselle turvallisuudelle. Jotta tietoliikennetiedustelu voitaisiin hyväksyä laajalti kansalaisten ja yhteiskunnan muiden toimijoiden taholta, tulisi ne uhat, joita tiedonhankinta koskee, olla määritelty mahdollisimman selkeästi ja suppeasti. Lisäksi tietoliikennetiedustelun avulla tunnistettavien uhkien tulisi olla riittävän vakavia ja kohdistua kansallisen turvallisuuden kannalta keskeisiin turvallisuusintresseihin.¹⁹³

Kansalliseen turvallisuuteen kohdistuvat uhat jaetaan tiedonhankintalakityöryhmän mietinnössä karkeasti siviililuonteisiin ja sotilaallisiin. Keskeisiä siviililuonteisia uhkia ovat kansainvälinen terrorismi ja siihen vaikutuksiltaan vertautuva toiminta, Suomeen ja sen etuihin kohdistuva ulkovaltojen vakoilu sekä sellainen kansainvälinen järjestäytynyt rikollisuus, joka pyrkii soluttautumaan valtiorakenteisiin tai muuten pyrkii vaikuttamaan yhteiskunnalliseen

¹⁹⁰ Ibid, s. 21, 23.

¹⁹¹ Ibid, s. 50.

¹⁹² Ibid, s. 50.

¹⁹³ Tiedonhankintalakityöryhmän mietintö 2015, s. 62 – 63.

päätöksentekoon. Erityisen maininnan mietinnössä saa viime vuosina esiinnoussut tietoverkkoympäristössä tapahtuva rajat ylittävä vakoilu, joka voi suuressa mittakaavassa toteutettuna aiheuttaa mittavaa vahinkoa kohdevaltion turvallisuudelle.¹⁹⁴

Tietoliikennetiedustelun avulla havaittavina uhkina työryhmä mainitsee vielä edellä mainittujen lisäksi seuraavat: joukkotuhoaseiden päätyminen väärin käsiin, vieraiden valtioiden suunnitelmat ja toimet, jotka voivat vaarantaa Suomen ulko- ja turvallisuuspoliittisia etuja ja valtion sisäiset vaikutuksiltaan vakavat uhat (esim. joukko- ja koulusurmat), joista voitaisiin saada tietoa rajat ylittävän tietoliikennetiedustelun avulla.¹⁹⁵ Uhkista huomiotta ei voi jättää vakavia tietoverkkouhkia, joita tuottavat valtiolliset vakoilu- ja haittaohjelmat, ja joiden kansallista turvallisuutta vahingoittava vaikutus on merkittävä. Tietoliikennetiedustelu täydentäisi merkittävästi Suomen suojautumista näiltä uhkilta, koska valtiollisesti tuotettuja ohjelmia ei voida havaita nykyisillä tietoturva- ja suojaohjelmilla.¹⁹⁶

Sotilaallisten uhkien luonteessa on myös tapahtunut muutoksia. Modernit sotilasoperaatiot sisältävät nykyään erilaisia ns. epäsymmetrisiä keinoja. Ennen perinteisten ja varsinaisten sotilaallisten toimien aloittamista, käynnistetään sotilasoperaatiot nykyään hybridisodankäynnin keinoin erilaisilla painostus- ja disinformaatio-operaatioilla sekä tietoverkkohyökkäyksillä.¹⁹⁷

Siviililuonteisten ja sotilaallisten uhkien yhteisenä nimittäjänä voidaan nähdä olevan kaiken kattavat ja lävistävät toimintojamme kannattelevat tietoverkot. Selvästi on havaittavissa, että nykyisin yhteiskunnan turvallisuutta uhkaavat toimet tapahtuvat kyberympäristössä ja toteutetaan sitä hyväksikäyttäen. Sisäisten ja ulkoistenuhkien raja on lisäksi hämärtynyt. Yhteiskunnan turvallisuutta uhkaavat toimet ovat hyvin usein rajat ylittäviä, eikä niiden toteuttajaa aina voida tunnistaa valtiolliseksi tai ei-valtiolliseksi toimijaksi. Näin ollen verkossa tapahtuva tiedustelutoiminta olisi työryhmän mukaan tarpeellinen lisäkeino viranomaisille kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitsemiseksi ja tunnistamiseksi.

¹⁹⁴ Ibid, s. 19.

¹⁹⁵ Ibid, s. 63.

¹⁹⁶ Ibid, s. 63 ja 69.

¹⁹⁷ Tiedonhankintalaki työryhmän mietintö 2015, s. 19.

7 Mietinnöstä annettujen lausuntojen analyysi

7.1 Lausunnoissa esiin tulleet uhat

Kysymys siitä minkälaisia uhkia tiedustelullailla pyritään torjumaan, on itsessään yksinkertainen niin tämänhetkisessä turvallisuuspolitiikkaa koskevassa diskurssissa kuin arkielämän keskusteluissa. Tieteen keinoin kysymykseen voidaan hakea vastausta lähestymällä kysymystä vaihtoehtoisista näkökulmista ja erilaisin tavoin. Poliitiikan saralla ja arkielämässä kysymykseen on saatavissa suuri määrä toisistaan poikkeavia ja erilaisiin mielipiteisiin perustuvia vastauksia. Todellisuus hahmottuu ihmisille erilaisten käsitysten ja sosiaalisten prosessien kautta, koska luomme olettamuksia ympäröivästä todellisuudesta ja siihen vaikuttavista tekijöistä.¹⁹⁸

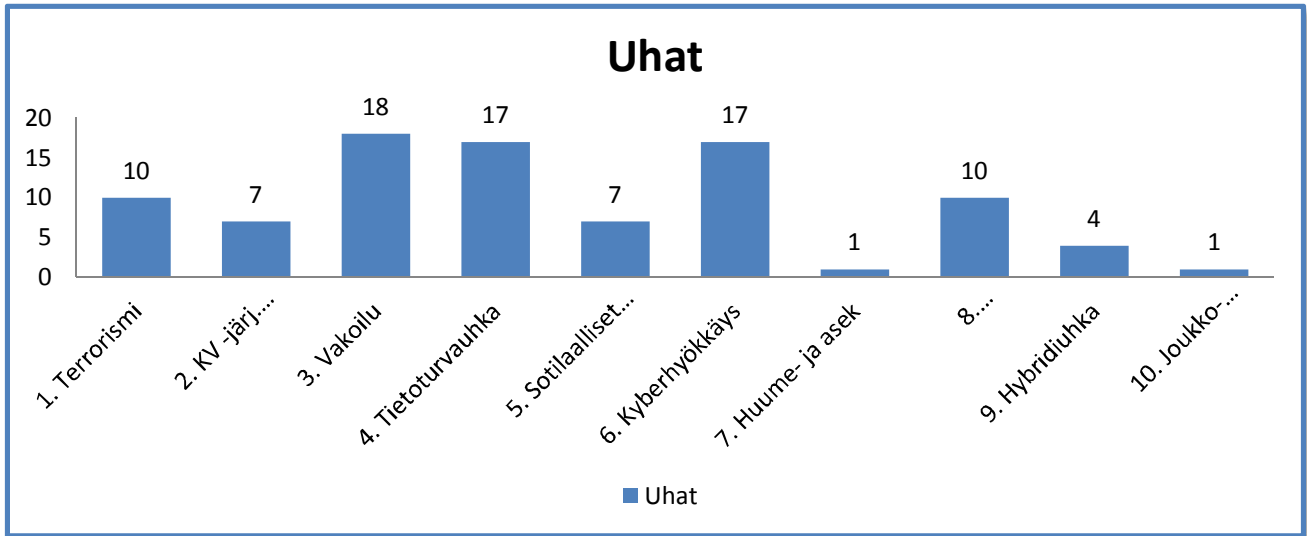
Uhkien kohdistuessa kansalliseen turvallisuuteen, on uhka ymmärrettävä lähtökohtaisesti sekä kiistanalaisena että neuvottelunvaraisena politiikan teon instrumenttina. Uhkaa ei ole olemassa yhtenä vakioituna olotilana eikä yhtenä ainoana määritelmänä, koska sen ”todellista todellisuutta” on mahdotonta verifioida objektiivisesti. Voidaankin sanoa, että turvallisuus ja uhka ovat sitä mitä niistä tehdään. Uhkakuvista voidaan hyvin harvoin jos koskaan saavuttaa yksimielisyyttä, koska erilaiset näkemykset turvallisuudesta ja uhkista perustuvat erilaisiin arvioihin, maailmankatsomuksellisiin näkemyksiin ja arvoihin sekä poliittisiin tavoitteisiin.¹⁹⁹ Tämän tutkimuksen kannalta lukijan on hyvä ymmärtää edellä oleva turvallisuuden ja uhkien kiistanalaisuus.

Luokittelin lausunnoissa esiin tulleet uhat (kaavio 6.) vastaten mietinnössä esitettyä jakoa siviililuonteisiin ja sotilaallisiin. Keskeisimmät lausunnoissa esiintuodut siviililuontoiset turvallisuusuhat olivat; ulkovaltojen Suomeen ja sen etuihin kohdistamaa vakoilu, tietoturva-uhat, kyberhyökkäykset, tietoverkkorikollisuus, kansainvälinen terrorismi ja kansainvälinen järjestäytynyt rikollisuus. Kaavion 6. luvut ovat kappalemääriä, siitä monessako lausunnossa vedottiin kyseiseen uhkaan, esim. kansainväliseen terrorismin uhka tuotiin esille 10:ssä lausunnossa.

¹⁹⁸ Limnell 2009, s. 2.

¹⁹⁹ Limnell 2009, s. 3.

Kaavio 6.²⁰⁰



Lausunnoissa puhuttiin yllätyksekseni melko vähän uhkista, vaikka niillä nimenomaan perustellaan esimerkiksi tietoliikennetiedustelun tarvetta. Uhkien esiin tuomisella lausunnonantajat tietysti perustelevat tiedustelulakien tarvetta ja lakihanketta yleisesti tai tarkemmin esimerkiksi tietoliikennetiedustelun tarvetta. 36:sta erilaisia uhkia maininneista lausunnonantajista 22 puolsi tiedustelulakihanketta. Myös sellaisissa lausunnoissa, joissa ei otettu selkeää kantaa puolesta eikä vastaan mainittiin, joitakin em. uhkista. Yksittäinen lausunnonantaja yleensä luetteli useamman kuin yhden uhkan, keskimäärin 2,5 uhkaa/lausunto. Lähes poikkeuksetta lausunnonantajat käyttivät kaaviossa käyttämiäni termejä, jotka ovat melko vakiintuneita uhkista puhuttaessa. Vain muutamassa tapauksessa oli suoritettava tulkintaa mitä uhkaa lausunnonantaja tarkoittaa.

Tietoturva-uhat, kyberhyökkäykset ja tietoverkkorikollisuus kaikki sijoittuvat digitaaliseen toimintaympäristöön, mutta niitä ei voi kuitenkaan niputtaa yhdeksi kategoriaksi, koska niissä on kuitenkin eronsa. Digitaalinen toimintaympäristö itse asiassa liittyy myös kaikkiin muihinkin edellä oleviin kymmeneen erilaiseen uhkaan. Yhteiskunnan toiminnan kannalta kriittisten toimintojen ja palveluiden perustuessa yhä suuremmin tietoverkkojen toimintaan on selvää, että näitä uhkaavat toimet sijoittuvat myös tähän ympäristöön. Toisaalta vaikka terroristiset teot tapahtuvat reaali maailmassa, käyttävät tekijät hyväkseen tietoverkkoja propagandan levittämiseen, yhteydenpitoon ja sen palveluita suunnitellessaan tekoja, tämä sama digitaalisen toimintaympäristön hyväksikäyttö liittyy myös kansainvälisen järjestäytyneen rikollisuuden toimintoihin.

²⁰⁰ 1. Kansainvälinen terrorismi, 2. Kansainvälinen järjestäytynyt rikollisuus, 3. Ulkovaltojen oikeudeton ja laiton tiedustelutoiminta sis. teollisuusvakoiluun, 4. Tietoturvauhka, 5. Elektroninen häirintä ja digitaalinen hyökkäys, 7. Verkossa tapahtuva huumausaine-, lääke- ja asekauppa, 8. Tietoverkkorikollisuus, 9. Hybridiuhka sis. disinformaation, 10. Joukkotuhoaseiden, kaksikäyttötuotteiden ja radioaktiivisten tuotteiden levittämispyrkimykset.

Osa lausunnonantajista käsittelee uhkia vain luettelemalla niitä viittaamalla mietinnön kansallista turvallisuutta vaarantaviin uhkiin. Esimerkiksi suojelupoliisi luettelee kansalliseen turvallisuuteen kohdistuvia useita uhkia, joita tietoliikennetiedustelulla olisi tarkoitus havaita. Suojelupoliisi viittaa lausunnossaan Euroopan ja Suomen lähialueiden viimeaikaisiin tapahtumiin muistutuksena siviili- ja sotilaallisten uhkien todellisesta olemassaolosta.²⁰¹

Toinen tapa käsitellä uhkia, on puhuminen niistä lausunnonantajan tehtävien tai hallinnonalan näkökulmasta. Esimerkiksi oikeuskansleri lähestyy uhkia aluevalvontalain 34 §:n kautta. Kyseisien pykälän mukaan puolustusvoimien ja rajavartiolaitoksen tehtävänä on valtakunnan turvallisuutta vaarantavan vihamielisen toiminnan torjuminen. Säännöksen mukaan vihamielisellä toiminnalla tarkoitetaan vieraan valtion aseellisen toiminnan lisäksi myös vieraan valtion turvallisuutemme kannalta tärkeisiin kohteisiin kohdistamaa oikeudetonta tiedustelua (vakoilu) ja elektronista häirintää.²⁰²

Uhkista puhuttaessa lausunnoissa korostuivat uhkien luonteen osalta seuraavat huomiot:

1. *”Suomen muuttuneessa turvallisuuspoliittisessa ympäristössä turvallisuusuhkien kirjo ja niiden toteutumisen mahdollisuus kasvanut ja niiden ennustettavuus on vaikeutunut”.*²⁰³
2. *”Kansalliseen turvallisuutemme kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä ulkomaille”.*²⁰⁴
3. *”Suomen kansalliseen turvallisuuteen kohdistuvat uhkat voivat olla toisiinsa kytköksissä, vaikeasti ennustettavia ja varoitusajaltaan lyhyitä”.*²⁰⁵
4. *”Poliittisen vaikuttamisen ja sodankäynnin rajan hämärtymiseen”.*²⁰⁶
5. *”Siviililuonteisten ja sotilaallisten uhkien sekä sisäisten ja ulkoisten uhkien rajan hämärtyminen”.*²⁰⁷

Uhkien olemassaoloa ei lausunnoissa kiistetä, joka kertoo nähdäkseni siitä, että ne ovat todellisia ja kiistattomia. Poikkeuksena oli kylläkin Piraattipuolue, jonka mukaan verkkovalvonnan tarvetta perustellaan mietinnössä epämääräisillä uhkakuvilla. Vaikka useissa lausunnoissa ei uhkia mainittukaan, esitti useat lausunnonantajat kuitenkin vaatimuksen siitä, että uhkat on määriteltävä ja niistä on säädettävä selkeärajaisemmin kuin mietinnössä on esitetty.

²⁰¹ Suojelupoliisi, lausunto s. 2.

²⁰² Oikeuskanslerinvirasto, lausunto s. 2.

²⁰³ Puolustusvoimien puolustuspoliittinen osasto, lausunto s. 1.

²⁰⁴ Suomen rauhanturvaajaliitto ry, lausunto s. 2, 1.

²⁰⁵ Valtionneuvoston kanslia, lausunto s. 1.

²⁰⁶ Ibid, s. 1.

²⁰⁷ Oikeuskanslerinvirasto, lausunto s. 2.

7.2 Lausunnoissa esiintyvät puoltavat argumentit

Tässä alaluvussa tarkastellaan lausunnoissa esiintyneitä puoltavia argumentteja lakihankkeesta. Sisällön analyysi on tehty havainnoimalla sisällöllisesti mietinnöstä annettuja puoltavia sisällöllisiä lausuntoja.

Osa puoltavista lausunnonantajista esitti yhden tai useampia argumentteja lakihankkeen puolesta, joten esitettyjen teemojen lukumäärää ja puoltavien lausunnonantajien määrää ei lukijan kannata ryhtyä vertaamaan.

Lausunnoista 46:ssa kannatettiin erilaisilla perusteilla tiedustelulakihanketta 157:llä erillisellä argumentilla. Puoltavien lausuntojen antajista 13 oli etujärjestöjä, yksi tiedonhankintalakityöryhmän nimeämä asiantuntija, 16 eri ministeriön (mukaan lukien ministeriöt) alaista laitosta tai yksikköä, viisi puoluetta, 10 yritystä ja Pääesikunta.

Puoltavista argumenteista syntyi niiden sisällön perusteella viisi kategoriaa, jotka ovat: 1) tiedustelutieto turvallisuuden takaamiseksi, 2) turvallisuus digitalisaation ja kybertoimintaympäristön viitekehyksessä, 3) tiedustelutieto tilannekuvan muodostamisessa ja rikostorjunnassa, 4) tiedustelu ja viranomaisten tiedustelutoimivaltuudet lainsäädännön piiriin ja 5) muuttunut turvallisuus- ja toimintaympäristö.

Tiedustelutieto turvallisuuden takaamiseksi

Ensimmäisen kategorian ytimessä ovat turvallisuus ja siihen kohdistuvat uhat, joita käsiteltiin yhteensä 28:ssa lausunnossa 39:llä argumentilla (osuus kaikista argumenteista 24,8 %), jotka sopivat tähän kategoriaan. Näiden lausuntojen mukaan kansallisen turvallisuuden varmistamiseksi on luotava säädöspohja Suomeen kohdistuvien vakavien kansainvälisten ja ulkoisten turvallisuusuhkien torjumiseksi. Tiedustelutoiminnalla tuotetaan turvallisuusuhkien torjunnan kannalta välttämätöntä tietoa. Tähän kategoriaan sijoittuvissa argumenteissa korostettiin turvallisuusviranomaisten tehtäviensä hoitamiseen tarvittavien toimivaltuuksien riittävyttä ja kykyä turvata yhteiskuntamme turvallisuutta. *Kansallista turvallisuutta* suojattavana etuna ja käsitteenä sellaisenaan käytettiin seitsemässä argumentissa. Epäsuorasti kansalliseen turvallisuuteen viittaavia yleisluonteisimpia turvallisuuteen ja viranomaisten kykyyn uhkien havaitsemiseksi ja

torjumiseksi käytettiin 11:ssä lausunnossa, esimerkkejä tällaista argumenteista seuraavassa:

- *”Tiedustelutiedon avulla turvataan kansalaisten henkeä ja terveyttä”*²⁰⁸,
- *”[..tietoyhteiskunnan toimivuutta ja turvallisuutta varantavat uhat on pystyttävä havaitsemaan..]”*²⁰⁹
- *”[.. viranomaisilla ja valtionjohdolla tulee olla edellytykset tietojen hankintaan vakavista kansainvälisistä uhkista..]”*²¹⁰
- *”Tiedustelutoiminta parantaa kykyä uhkien torjumiseen.”*²¹¹
- *”Turvallisuusviranomaisten on saatava tiedustelun avulla tietoa toimialaansa kuuluvien uhkien torjumiseksi.”*²¹²
- *”Tiedonhankintalailla luotavat toimivaltuudet mahdollistavat ennakkovaroituksen antamisen uhkista.”*²¹³

Kansallisen turvallisuuteen kohdistuvien uhkien havaitsemista, tunnistamista ja torjumista voidaan siis pitää ensimmäisen kategorian pääasiallisena teemana. Nämä toimet ovat proaktiivisia toimia, jotka sijoittuvat aikaan ennen uhkien realisoitumista. Toiseksi merkittävin teema (9 mainintaa) puoltavien lausuntojen ensimmäisessä kategoriassa koskevat vaatimuksia toimivaltuuksista kyberuhkien ja -rikollisuuden havaitsemiseen ja torjumiseen sekä kybervaikuttamiseen poikkeusoloissa.

Turvallisuus digitalisaation ja kybertoimintaympäristön viitekehyksessä

Toisen kategorian lausunnoissa kantavana teemana oli huoli viranomaisten toimivaltuuksien ja menetelmien riittävydestä vastata nimenomaan *digitalisoitumisen* tuomiin turvallisuusuhkiin. On myönnettävä, että ensimmäisen ja toisen kategorian raja on häilyvä, koska molemmissa on kyse turvallisuudesta ja että niissä päällekkäisyyttä. Pääasiallinen ero on kuitenkin se, että jälkimmäisessä digitalisaatio itse voidaan nähdä uhkana ja uhkia synnyttävänä ilmiönä.

Tähän kategoriaan sijoittui 23 eri lausuntoa ja 28 erillistä puoltavaa argumenttia (osuus puoltavista argumenteista 17,8 %). Näistä lausunnoista 15:ssä mainitaan digitalisaatio ja kybertoimintaympäristö haasteellisena viitekehystenä osana laajempaa turvallisyyttä, johon kansallinen turvallisuuskin kuuluu. Näissä lausunnoissa ei eritellä mitkä tällaiset uhat ovat, ne vain generoituvat digitalisaatiosta

²⁰⁸ Suomen Journalistiliitto, lausunto, s. 1.

²⁰⁹ Suomen Erillisverkot Oy, lausunto, s. 1.

²¹⁰ Keskuskauppakamari, lausunto, s. 1.

²¹¹ Suomen ruotsalainen kansanpuolue, lausunto, s. 1.

²¹² Rajavartiolaitoksen esikunta, lausunto, s. 1

²¹³ Pääesikunta, lausunto, s. 1.

ja kybertoimintaympäristöstä, yhteisenä tekijänä lausunnoissa kuitenkin on uhkien vakavuus, niiden määrän kasvu ja todenperäisyys.

Keskuskauppakamarin lausunnon tähän kategoriaan sijoittuva argumentti kuvaa hyvin edellä mainittuja lausuntoja. Heidän näkemyksen mukaan viranomaisilla on oltava valtuudet toimia digitaalisessa ympäristössä ja niiden on pystyttävä vastaamaan digitalisoitumisen tuomiin turvallisuusuhkiin.²¹⁴

Toisen merkittävän ryhmän (8 lausuntoa) tässä kategoriassa muodostivat lausunnot, joissa erikseen nimetään toimintaympäristö ja rikollisuuden luonne, jotka tulevat kysymykseen tässä viitekehysessä. Professori *Voutilaisen* mukaan kyberuhat uhkaavat muun muassa yhteiskunnan toiminnan kannalta kriittisiä peruspalveluja ja -toimintoja, koska ne perustuvat nykyään informaatio- ja viestintäteknologian (ICT) hyödyntämiseen.²¹⁵ *Poliisihallitus* puoltavia argumentteja tässä kategoriassa ovat; 1) yhteiskuntien digitalisoitumisen johdosta osa rikollisuudesta on siirtynyt tietoverkkoympäristöön, 2) yhteiskuntaan, yritystoimintaan ja kansalaisiin kohdistuva tietoverkkorikollisuus on kasvava uhka, 3) tietoverkkoja joko käytetään rikosentekovälineenä tai niitä hyödynnetään rikosten suunnittelussa tai rikollisten välisessä yhteydenpidossa, 4) kyberrikollisuus on globaalia rikollista toimintaa, jossa valtioiden rajat eivätkä viranomaisten perinteiset valvontamenetelmät enää muodosta estettä rikolliselle toiminnalle.²¹⁶

Tiedustelutieto tilannekuvan muodostamisessa ja rikostorjunnassa

Kolmannessa kategoriassa on siirrytty turvallisuuden takaamisesta ja uhkien havainnoimisesta konkreettisempiin käyttötarkoituksiin, joihin tiedustelutietoa käytetään. Tähän puoltavien lausuntojen kategoriaan sijoittuu 12 lausuntoa, joista kahdeksassa teemana oli, että valtionjohdon ja viranomaisten päätöksenteon on perustuttava oikeaan, ajantasaiseen ja luotettavaan tietoon ja tilannekuvaan uhkista. Näiden lausuntojen keskiössä olivat tilannetietoisuus ja tilannekuva välineenä, joka mahdollistaa oikea-aikaisen päätöksenteon ja toiminnan. Tällöin on mahdollista arvioida toiminnan seuraukset, miten muut siihen reagoivat ja mitä riskejä päätöksiin sisältyy.²¹⁷ Tällä perusteella tiedustelulakihanketta kannattivat; Suomen Rauhanturvaajaliitto ry, Suomen

²¹⁴ Keskuskauppakamari, lausunto s. 1.

²¹⁵ Voutilainen, lausunto s. 1.

²¹⁶ Poliisihallitus, lausunto s. 1.

²¹⁷ Yhteiskunnan turvallisuusstrategia 2010, s.54

Asianajajaliitto, valtionneuvoston kanslia, valtionvarainministeriö, suojelupoliisi, Suomen ruotsalainen kansanpuolue, Pääesikunta ja Prof-Tel Oy.

Kolmessa tämän kategorian lausunnoissa puoltavana perusteena oli, että hankittua tiedustelutietoa voitaisiin hyödyntää rikostorjunnassa ja -tutkinnan suuntaamisessa sekä toteutuneiden rikosten tutkinnassa.

Tiedustelu ja viranomaisten toimivaltuudet lainsäädännön piiriin

Neljänteen kategoriaan sijoittui 25 lausuntoa sisältäen 32 erillistä perustetta (osuus puoltavista argumenteista 17,8 %). 17:ssä näistä perusteluista esitettiin vaatimus siitä, että tiedustelun ja sen harjoittamisen mahdollistavien viranomaisten toimivaltuuksien on perustuttava laintasolla säädettyyn normistoon, mikä on oikeusvaltioperiaatteen yksi keskeinen elementti julkisen vallan käytölle. Lisäksi useassa perustelussa viitattiin mietinnössä tehtyyn kansainväliseen lainsäädäntövertailuun. Vertailun perusteella esitettiin huomioita, että tiedustelulakien puuttuminen on kansainvälisesti hyvin poikkeavaa. Teeman ilmaukset olivat seuraavanlaisia:

- Turvallisuusviranomaisten lakisäätteisten tehtävien täyttäminen edellyttäisi täsmällisiä lakisäätteisiä tiedustelu-oikeuksia. Tiedustelua koskevan lainsäädännön puuttuminen poikkeaa yleisestä länsimaisesta käytännöstä, ja vallitseva tilanne on oikeusvarmuuden ja oikeusvaltioperiaatteen kannalta epätydyttävä.²¹⁸
- Tiedustelutoimintaa koskeva lainsäädäntö on tarpeellinen vain siksi, että toiminta tulee lailla säädellyksi ja valvotuksi.²¹⁹
- *”[T]iedustelulainsäädännön puute on selvä epäkohta lainsäädännössämme, kun otetaan huomioon muuten tiedustelutoiminnan laaja-alaisuus muualla eri valtioissa.”*²²⁰
- *”[K]annattaa tiedonhankintalain säätämistä ja sitä kautta oikeuksien ja vastuiden määrittelyä lain tasolla. Mahdollisen tiedonhankintalain keinot on kuitenkin harkittava tarkkaan.”*²²¹

Lisäksi tässä kategoriassa puollettiin tiedustelun lainsäädännön piiriin saattamista kahdeksassa lausunnossa 11:llä samankaltaisella perusteella, joiden teemana oli viranomaisten nykyisten hajaantuneiden toimivaltasuhteiden selkeyttäminen ja tiedonvaihdon mahdollistaminen. Toimivaltasuhteiden epäselvyys ja hajanaisuus johtuu lausuntojenantajien näkemyksen mukaan tiedustelua koskevan lain puutteesta ja ulkoisten ja sisäisten turvallisuusuhkien torjunnan ja rikostorjunnan välisen raja hämärtymisestä.

²¹⁸ Suomen Asianajajaliitto, lausunto, s. 3 – 4.

²¹⁹ Vihreä liitto, lausunto, s. 1.

²²⁰ Voutilainen, lausunto, s. 5.

²²¹ Nokia Oyj, lausunto, s. 1.

Muuttunut turvallisuus- ja toimintaympäristö

Viidennen ja viimeisen kategorian puoltavina argumentteina oli, että Suomen turvallisuus- ja toimintaympäristössä tapahtuneet muutokset edellyttävät tiedustelulakien säätämistä. Tätä teemaa käytti vain kuusi lausunnonantajaa ja kaikissa niissä oli kyse nimenomaan ulkoisen turvallisuus- ja toimintaympäristön muutoksista. Vain kahdessa niistä tarkennettiin meihin vaikuttavia muutoksia ja niistä aiheutuvien haasteiden luonnetta. Niissä todettiin:

- ”Suomen muuttuneen toimintaympäristön ennustettavuus on vaikeutunut ja turvallisuusuhkien kirjo ja niiden toteutumisen mahdollisuus on kasvanut”.²²²
- ”Kansainvälinen turvallisuustilanne on heikentynyt ja sen muutokset ovat vaikeasti ennustettavia”.²²³

Yhdistävänä tekijänä näissä argumenteissa oli nykyisten turvallisuusuhkien laajakirjo ja niiden toteutumisen mahdollisuuden kasvu yhdistettynä vaikeasti ennustettavuuteen. On selvää, että tällaisilla kiistattomilla ja yleisesti eri foorumeilla hyväksytyillä perusteilla haetaan kannatusta tiedustelulakien säätämiseksi.

7.3 Lausunnoissa esiintyvät vastustavat argumentit

Tässä luvussa käsitelen lausuntoja, joissa vastustetaan tiedustelulakihanketta sellaisilla perusteilla, jotka eivät perusta vastustusta perusoikeuksien toteutumiseen tai niiden loukkaamiseen. Niitä käsitelen erikseen seuraavassa luvussa.

Tähän lukuun sijoittuvia lakihanketta vastustavia lausunnonantajia oli 11 kappaletta, joista kolme oli kansalaisjärjestöjä, yksi ministeriö, kolme puoluetta ja neljä yritystä. Lausunnoissa vastustettiin tiedustelulakihanketta 44:llä erillisellä argumentilla.

Vastustavien argumenttien teemoista syntyi niiden sisällön mukaan seitsemän kategoriaa, jotka ovat: 1) tietoliikennetiedustelun tehottomuus, 2) uhka väärinkäytöksistä, 3) kansalaisten luottamuksen vaarantuminen, 4) vaikutukset tietoturvaan, 5) tiedustelun kohdentamattomuus, 6) nykyiset tiedonhankintakeinot riittäviä, 7) toimivaltuuksien lakisidonnaisuus. Selvyiden vuoksi totean, että lausunnonantajat käyttivät kaikki useampaa kuin yhtä kategorioiden teemaa, keskimäärin jokaisella oli lausunnossa 3 – 5 erillistä teemaa.

²²² Puolustusministeriön puolustuspoliittinen osasto, lausunto s. 1.

²²³ Suojelupoliisi, lausunto s. 1.

Viisi ensimmäistä kategoriata liittyvät pääasiallisesti tietoliikennetiedusteluun, josta Liikenne- ja viestintäministeriö ja useimmat muutkin hanketta vastustavat käyttävät lausunnoissaan käsitettä verkko- tai massavalvonta, koska se heidän mukaan kuvaa todenmukaisemmin toimintaa, jossa olisi kyse teknisestä pääsystä kaikkeen tietoliikenteeseen.

Tietoliikennetiedustelun tehottomuus

Ensimmäiseen kategoriata sijoittui 10 (osuus vastustavista argumenteista 22,7 %) lausunnonantajan ilmausta, jotka kohdistivat tietoliikennetiedustelun tehokkuuteen vakavia epäilyjä ja he kyseenalaistivat sen tehokkuuden, koska siitä ei ole esitetty riittävää ja luotettavaa näyttöä. Vastustajien pääasiallinen viesti on, ettei tietoliikennetiedustelu nykyisellään välttämättä tuottaisi kaikkea sitä tietoa, jota sillä joskus aikaisemmin on voitu saada, koska viestien salaustekniikat ovat kehittyneet ja niiden käyttö on lisääntynyt sekä tietoliikenteen määrä on kasvanut. Lisäksi tässä yhteydessä huoleksi esitettiin, että viestien lisääntynyt salaaminen, johtaa tiedustelutoimien kohdentamiseen viestiliikenteen sijaan jatkossa itse päätelaitteisiin ja taustapalvelujärjestelmiin.

Tämän kategorian argumentein tiedustelulakihanketta vastustivat Electronic Frontier Finland - Effi ry, Suomen Sadankomitea ry, Internet -käyttäjät ikuisesti - IKI ry, Liikenne- ja viestintäministeriö, Vihreä liitto, Piraattipuolue, Fujitsu Finland Oy ja CSC - Tieteen tietotekniikan keskus Oy.

Uhka väärinkäytöksistä

Toinen kategoriata kuvastaa lausunnonantajien epäluottamusta viranomaistoimiin ja virkatehtäviä hoitavia henkilöitä kohtaan yleisesti, ajatuksena annettujen toimivaltuuksien ylittäminen ja väärinkäyttö sekä tiedustelulla hankittujen tietojen vuotaminen julkisuuteen. Tällaista vastustavaa teemaa käytti viisi lausunnonantajaa (osuus 11,4 %). Lausunnonantajien epäluottamusta ei hälvennä edes mietinnössä esitetty tiedusteluviranomaisten toimien lupa- ja valvontamekanismi. Esimerkiksi Piraattipuolue pitää viranomaisille perusoikeusloukkauksista määrättyjä seuraamuksia nimellisinä ja riittämättöminä ehkäisemään toimivaltuuksien väärinkäytöksiä.²²⁴

Tämän kategorian argumentein tiedustelulakihanketta vastustivat Electronic Frontier Finland - Effi ry, Suomen Sadankomitea ry, Internet -käyttäjät ikuisesti - IKI ry, Vasemmistoliitto, Piraattipuolue,

²²⁴ Piraattipuolue, lausunto s. 5.

Kansalaisten luottamuksen vaarantuminen

Kolmanteen kategoriaan sijoittuvien ilmausten huolena on, että viranomaisten pääsy kaikkeen tietoliikenteeseen synnyttää kansalaisissa tunteen jatkuvasta seurannasta²²⁵, joka heikentää kansalaisten luottamusta yhteiskuntaa ja viranomaisia kohtaan.²²⁶ Tätä vastustavaa teemaa käytti viisi (osuus 11,4 %) lausunnonantajaa.

Tämän kategorian argumentein tiedustelulakihanketta vastustivat Electronic Frontier Finland - Effi ry, Internet -käyttäjät ikuisesti - IKI ry, Vasemmistoliitto, Piraattipuolue ja CSC - Tieteen tietotekniikan keskus Oy.

Vaikutukset tietoturvaan

Neljännän kategorian lausunnoissa oli huoli tietoliikennetiedustelun negatiivisista vaikutuksista tietoturvaan. Tähän kategoriaan sijoittui kuudessa (osuus 13,6 %) launnossa käytetyt ilmaisut. Liikenne- ja viestintäministeriön eriävän mielipiteen mukaan ”*verkkovalvonta tarkoittaisi sitä, että tiedonhankinnan kohteeksi valikoidun viestinnän suojaukset yritettäisiin ohittaa tai murtaa, mikä heikentäisi niiden henkilöiden tietoturvallisuutta, joiden viestejä välitettäisiin niissä viestintäverkoissa, joissa verkkovalvontaa suoritettaisiin*”.²²⁷ Tähän eriävään mielipiteeseen yhtyi neljä lausunnonantajaa. Toisena teemana tässä kategoriassa oli uhka kerättyjen luottamuksellisten tietojen joutumisesta väriin käsiin esimerkiksi tietovuotojen tai hakkeroinnin seurauksena.

Tämän kategorian argumentein tiedustelulakihanketta vastustivat Electronic Frontier Finland - Effi ry, Internet -käyttäjät ikuisesti - IKI ry, Liikenne- ja viestintäministeriö, Fujitsu Finland Oy, CSC - Tieteen tietotekniikan keskus Oy ja Nokia Oyj.

Tiedustelun kohdentamattomuus

Viidennessä kategoriassa tiedustelulakihanketta vastustettiin hyvin moninaisin ilmauksin. Tähän kategoriaan sijoittui kahdeksan ilmaisua (osuus 18,2 %), joiden yhteiseksi teemaksi muodostui tietoliikennetiedustelun kohdentamattomuus. Kaikissa niissä esitettiin epäily mietinnössä esitettyyn mahdollisuuteen, että tiedusteluviranomaisemme voisivat kohdistaa tietoliikennetiedustelun vain Suomen rajat ylittävään tietoliikenteeseen, jolloin sen kohteeksi ei joutuisi suomalaisten

²²⁵ Electronic Frontier Finland - Effi ry, lausunto s. 2.

²²⁶ Internet käyttäjät ikuisesti IKI ry, lausunto s. 4.

²²⁷ Liikenne- ja viestintäministeriö, eriävä mielipide, s. 2.

viestiliikenne.²²⁸ Tarkemmin ottaen näissä ilmaisuissa oli kyse siitä, ettei ulkomaista ja kotimaista tietoliikennettä voi käytännössä erottaa toisistaan, jonka johdosta myös suomalaiset joutuvat verkkovalvonnan kohteeksi.

Liikenne- ja viestintäministeriö (LVM) katsoo eriävässä mielipiteessään, että tietoliikennetiedustelu on verkkovalvontaa, jonka he nimeävät massavalvonnaksi. Tällaisessa kohdentamattomassa massavalvonnassa valvojalla on tekninen pääsy kaikkeen tietoliikenteeseen.²²⁹ LVM pitää mietinnössä tietoliikennetiedustelun yhteydessä käytettyä etuliitettä ”rajat ylittävä” tarkoitushakuisena, koska sen käyttäminen hämärtää käsitystämme siitä, mihin viestintään verkkovalvonta voisi kohdistua. LVM:n mukaan käytännössä verkkovalvonnan kohdentaminen vain ”rajat ylittävään” tietoliikenteeseen on vaikeaa, ellei jopa mahdotonta. Käytettäessä esimerkiksi pilvipalvelusähköposteja (Gmail, MS Outlook) tietoliikenne reitittyy kohteeseensa lyhintä tai nopeinta reittiä ja tietoa tallentuu sattumanvaraisesti usealle palvelimelle, jotka voivat sijaita missä tahansa maassa. Käyttäjä ei siis voi vaikuttaa siihen, mitä reittiä tieto kulkee tai mihin sitä tallentuu.²³⁰

Tämän kategorian argumentein tiedustelulakihanketta vastustivat Internet -käyttäjät ikuisesti - IKI ry, Liikenne- ja viestintäministeriö, Vasemmistoliitto, Vihreä Liitto, Piraattipuolue, Fujitsu Finland Oy ja CSC - Tieteen tietotekniikan keskus Oy.

Nykyiset tiedonhankintakeinot riittäviä

Kuudennessa yläkäsitekategoriassa tiedustelulakihanketta vastustettiin sillä perusteella, että nykyiset poliisin ja puolustusvoimien käytössä olevat salaiset tiedonhankintakeinot katsottiin olevan riittäviä niille määrättyjen tehtävien suorittamiseksi, eikä tietoliikennetiedustelulle näin ollen ole tarvetta. Tähän kategoriaan sijoittui seitsemän (osuus 15,9 %) lausunnonantajan lausuntoa.

Ainoana lausunnonantajista BaseN Oy perusteli näkemystään tässä kategoriassa tarkemmin. Heidän näkemyksen mukaan uusille tietoliikennetiedusteluvaltuuksille ei ole tarvetta, koska *”digitalisoituneesta ympäristöstämme voidaan jo tällä hetkellä muodostaa tosiaikainen ja kokonaisvaltainen tilannekuva ilman yksityisyyden suojan heikennyksiä, tukeutuen liikennevirtojen ja poikkeaminen jatkuvaan analyysiin”*.²³¹

²²⁸ Tiedonhankintalakiyöryhmän mietintö 2015, s. 70.

²²⁹ Liikenne- ja viestintäministeriö, eriävä mielipide, s. 1.

²³⁰ Ibid, s. 6.

²³¹ BaseN Oy, lausunto s. 2.

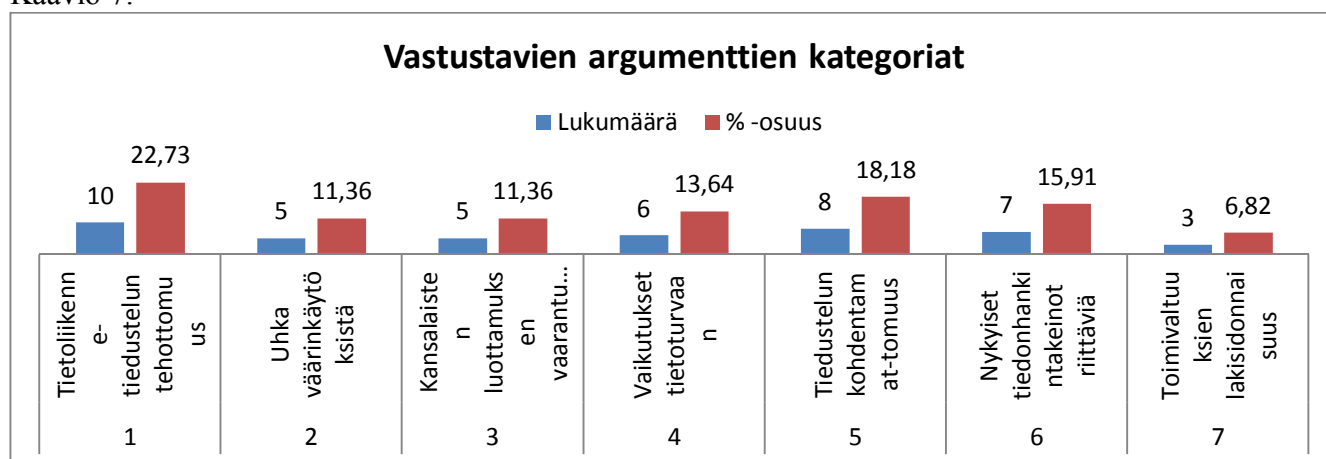
Tämän kategorian argumentein tiedustelulakihanketta vastustivat Internet -käyttäjät ikuisesti - IKI ry, Liikenne- ja viestintäministeriö, Vasemmistoliitto, Vihreä Liitto, Piraattipuolue, Fujitsu Finland Oy ja BaseN Oy.

Toimivaltuuksien lakisidonnaisuus

Seitsemänteen vastustavien lausuntojen kategoriaan sijoittui vain kolme lausunnonantajan vastustavaa ilmausta (osuus 6,8 %). Niiden teemana oli, että viranomaisten toimivaltuuksien on perustuttava niiden lakisääteisiin tehtäviin, eikä ”tiedustelua” tai ”uhkien torjuntaa” ole lailla säädetty puolustusvoimien tai poliisin tehtäviksi. Viranomaisten toimivaltuuksien on perustuttava vain ja ainoastaan niiden lakisääteisiin tehtäviin.²³² Tätä teemaa käytti lausunnossaan Liikenne- ja viestintäministeriö, jonka lausuntoon yhtyi kaksi muuta lausunnonantajaa.

Vastustavien argumenttien jakaantuminen seuraavassa kaaviossa 7. esitettynä ilmausten lukumäärien mukaan ja niiden jakaantuminen prosentuaalisesti eri kategorioiden kesken.

Kaavio 7.



7.4 Lausunnoissa esiintyvät huomioon otettavat perus- ja ihmisoikeuskysymykset

Tässä kappaleessa käsitellään lausunnoissa esitettyjä perus- ja ihmisoikeuskysymyksiä, jotka tulisi lausunnonantajien mielestä huomioida tiedustelulakihankkeessa. Perus- ja ihmisoikeuskysymyksinä käsitellin kaikkia lausunnoissa esiintyneitä ilmaisuja, joissa mainittiin jokin perusoikeus (esim. yksityisyyden suoja tai lähdesuoja) tai joissa sen sisältö viittasi perus- tai ihmisoikeuksiin tavalla tai toisella. Erilaisia vaatimuksia, huomioita ja kannanottoja perusoikeuskysymyksistä ovat esittäneet

²³² Liikenne- ja viestintäministeriö, eriävä mielipide, s. 7 – 10.

niin lakihanketta vastustavat kuin sitä puoltavatkin tahot, kuten myös ne, jotka eivät ole ottaneet kantaa puolesta tai vastaan. Pääasiallisesti näiden oikeuksien toteutumiseksi esitetyt vaatimukset, huomiot ja kannanotot liittyvät mietinnössä esitettyyn tietoliikennetiedustelun toteuttamiseen.

Näitä kaikkia lausunnoissa esiintyviä perus- ja ihmisoikeuskysymyksiä käsitellään tässä samassa luvussa tekemättä eroa mitä kantaa lausunnonantajat edustivat. Tässä yhteydessä argumenttien jaottelu puolesta tai vastaan ei ole tarkoituksenmukaista, koska lakihanketta puoltavat tai vastustavat tahot ovat käyttäneet samoja argumentteja huolimatta siitä mikä on heidän kanta tietoliikennetiedustelusta tai lakihankkeesta kokonaisuutena.

Yhtenä tämän tutkimuksen tarkoituksista oli selvittää mitkä ovat niitä perus- ja ihmisoikeuskysymyksiä, joita lausunnoissa tuodaan esiin ja mitä perusoikeuksia mietinnössä esitetyt tiedustelutoimet rajoittaisi tai vaarantaisi niiden toteutumista.

72:sta annetusta lausunnosta 51:ssä käsiteltiin tavalla tai toisella (70,83 %) perus- ja ihmisoikeuskysymyksiä, mikä osaltaan kertoo tiedustelulakihankkeen olevan perusoikeuksien osalta sensitiivinen.

Annettujen lausuntojen perusteella ehdotettujen tiedustelukeinojen vaarantamat keskeisimmät perusoikeudet ovat yksityiselämän suoja ja luottamuksellisen viestin salaisuuden suoja. Tiedustelulakihankkeen perusoikeuskysymyksiä käsittelevistä 51:stä lausunnosta 33:ssa (64,71 %) katsottiin olevan vaikutuksia yksityiselämän suojan toteutumiseen tai se ainakin tulee ottaa huomioon lakia säädettäessä. 26:ssa lausunnossa (50,98 %) lakihankkeella katsottiin olevan vaikutuksia luottamuksellisen viestin salaisuuden suojan toteutumiseen tai se ainakin tulee ottaa huomioon lakia säädettäessä. Muita huomioonotettavaksi vaadittuja perusoikeuksia lausunnoissa olivat henkilötietojen suoja (25,49 %), sananvapaus (11,76 %) ja lähdesuoja (9,80 %) sekä omaisuuden suoja (3,92 %).

Puhuttaessa yksityiselämän suojasta lausunnoissa käytettiin sen käsitettä epätarkasti. Pääasiassa niissä puhuttiin oikeudesta yksityisyyteen tai käytettiin termiä ”yksityisyyden suoja”. Yksityisyyden suojasta puhuttaessa tarkoitetaan usein jossain määrin suppeampaa käsitettä kuin yksityiselämän suoja. Se sisältyy kuitenkin osana laajempaan yksityiselämän suoja käsitteeseen.²³³

²³³ Nieminen 1999, s. 112 – 113.

Luottamuksellisen viestin salaisuuden suojan osalta vastaavaa epätarkkuutta ei lausunnoissa esiintynyt.

Edellä mainittujen perusoikeuksien lisäksi lausunnoissa mainittiin lisäksi yksittäisinä mainintoina oikeus turvallisuuteen (PL 7 §) ja perusoikeuksien turvaaminen (PL 22 §). Perustuslain 22 §:ssä on julkiselle vallalle säädetty velvollisuus perusoikeuksien toteutumisesta. Yksityiselämän suojan takaamiseksi valtion on itse pidättäydyttävä loukkaamasta kansalaisten yksityiselämää, lisäksi siltä edellytetään aktiivisia toimia yksityiselämän suojaamiseksi toisen yksilöiden loukkauksia vastaan.²³⁴ Yhteiskunnan peruspalvelujen ja -toimintojen digitalisoituessa viranomaisten on turvattava mm. tietoturvatoinenpitemillä tietojärjestelmien toimivuus PL 22 §:ään perustuen, joka saattaa johtaa ristiriitaan, jonkin toisen perusoikeuden kanssa.²³⁵

PL 22 §:ään liittyy myös suojelupoliisin lausunnossaan mainitsema valtion velvoite huolehtia ”kansalaistensa turvallisuudesta”²³⁶, toisin sanoen jokaisen oikeudesta henkilökohtaiseen turvallisuuteen. SUPO ei suoraan mainitse yksilön oikeutta turvallisuuteen perusoikeutena, josta on säädetty PL 7 §:ssä. Mutta viittaamisen kansalaisten turvallisuuteen huomioonotettavana valtion velvoitteena, voidaan ajatella tarkoitetun tässä yhteydessä turvallisuutta jokaiselle kuuluvana perusoikeutena. Laajemmin ajateltuna SUPO:n argumentin ajatuksena lienee se, että yleisen turvallisuuden takaamisen epäonnistuminen saattaa johtaa yksilön oikeuden laiminlyömiseen. SUPO ei kuitenkaan vetoa luottamuksellisen viestin suojan rajoittamisen perusteena PL 22 §:n velvoitteeseen eikä PL 7 §:n perusoikeuteen, vaan laissa määrittelemättömään kansalliseen turvallisuuteen.

7.4.1 Perusoikeuksien yleiset rajoitusedellytykset teemoina

Lausuntojen perus- ja ihmisoikeuksia koskevista argumenteista erottui selvästi niiden sisällön perusteella viisi teemaa, jotka ovat yhdenmukaisia yleisten rajoitusedellytyksien kanssa.

Teema 1	Teema 2	Teema 3	Teema 4	Teema 5
Suhteellisuus- ja välttämättömyys	Ydinalueen koskemattomuus	Täsmällisyys- ja tarkkarajaisuus	Ihmisoikeusvelvoitteiden noudattaminen	Hyväksyttävä tarkoitus

²³⁴ Liikenne- ja viestintäministeriö, eriävä mielipide s. 20.

²³⁵ Voutilainen, lausunto s. 2.

²³⁶ Suojelupoliisi, lausunto s. 2.

Suhteellisuus- ja välttämättömyysvaatimus

Arvioitaessa suhteellisuusvaatimuksen toteutumista Viljasen mukaan punninta tehdään perusoikeuden takaamien intressien ja perusoikeuden rajoittamisen taustalla olevien intressien välillä. Asetelmassa ovat vastakkain siis rajoitettavaan yksilön perusoikeuteen kytkeytyvä intressi ja perusoikeuden rajoittamiseen oikeuttava intressi eli hyväksyttävä rajoitusperuste.²³⁷

Perusoikeuskysymyksiä käsittelevistä 51:stä lausunnosta 25:ssä (49,02 %) esitettiin vaatimus suhteellisuusvaatimuksen huomioonottamisesta säädettäessä tiedustelulaeista. Vaatimus suhteellisuusvaatimuksen toteutumisen ja täyttymisen arvioinnin suorittamisesta esitettiin lausunnoissa käyttämällä esimerkiksi ilmaisuja *oikeasuhtaisuusvaatimus*, *suhteellisuusperiaate*, *oikeasuhtainen*, *suhteeton*, *tasapaino*. Lausunnoissa selkeimmin suhteellisuusvaatimuksen huomioonottamisen esittää professori *Scheinin* seuraavassa:

*”Perus- tai ihmisoikeuteen kohdistuvan rajoituksen on oltava oikeasuhtainen verrattuna siihen hyötyyn, mikä toimenpiteellä saavutetaan sen perusteena käytetyn hyväksyttävän tarkoitusperän toteuttamiseksi. Vain hyväksyttävän tarkoitusperän toteuttamiseksi välttämätön ja tehokas keino voi olla oikeasuhtainen siitä seuraavaan perusoikeusrajoitukseen verrattuna”.*²³⁸

Suojelupoliisi on myös ilmaissut suhteellisuusvaatimuksen huomioonottamisen lausunnossaan hyvin selkeästi. Suojelupoliisin mukaan luottamuksellisen viestin suoja voidaan rajoittaa kansallisen turvallisuuden nimissä yhteiskunnallisesti hyväksyttävällä ja tasapainoisella tavalla, sitä rajoitettaisiin vain mahdollisimman vähän ja sen verran kuin on välttämätöntä.²³⁹

Implisiittisesti suhteellisuusvaatimuksen huomioiminen ilmaistaan esimerkiksi Prof-Tel Oy:n ja Cinia Group Oy:n lausunnoissa:

*”Toisaalta nyt kyseessä olevan tiedustelulainsäädännön kehittämisen tavoitteet sekä toisaalta ihmisoikeussopimusten ja perusoikeuksien, tavoitteet eivät lähtökohtaisesti ole ristiriidassa keskenään. Molempien tavoitteet voidaan sovittaa tukemaan toisiaan”.*²⁴⁰

*”Yksityisyyden suojan rinnalla myös turvallisuus on nähtävä perusoikeutena, näiden molempien oikeuksien toteutuminen tulee olla tasapainossa tulevassa tiedustelulainsäädännössä”.*²⁴¹

²³⁷ Viljanen 2001, s. 210 – 211.

²³⁸ Scheinin, lausunto, s. 2, 11.

²³⁹ Suojelupoliisi, lausunto s. 2.

²⁴⁰ Prof-Tel Oy, lausunto, s. 5.

²⁴¹ Cinia Group Oy, lausunto s. 1.

Suhteellisuusvaatimuksen toteutumisen punninta-arviossa vastakkain olivat luottamuksellisen viestin salaisuuden suojan intressi ja sen hyväksyttävää rajoittamista perustelevat intressit, joita lausunnoissa kuvattiin muun muassa seuraavilla ilmaisuilla; *kansallinen turvallisuus, turvallisuuden takaamiseksi vaadittavan tiedonsaantitarve, kansalaisten ja yhteiskunnan turvallisuus, turvallisuus perusoikeutena ja turvallisuushyöty*.

Vain neljässä suhteellisuusvaatimusta koskevassa lausunnossa arvioitiin vastakkain asettuvien intressien painoarvoa. Näissä kaikissa kyseenalaistettiin rajoitusperusteena olevan intressin painoarvo. Perusteellisimman arvion esitti professori *Scheinin*, joka kyseenalaisti elektronisen ”verkkovalvonnan” hyödyn esimerkiksi terrorismin torjunnassa ja sen tehokkuuden ja kustannustehokkuuden johtamansa SURVEILLE –tutkimushankkeen tutkimustuloksiin perustuen. Tutkimushankkeen lopputuloksen mukaan työryhmän mietinnössä hahmotellun kaltainen tietoliikennetiedustelu saisi aikaan varsin vaatimatonta hyötyä potentiaalisten terroristien paljastamisessa, samalla kun sen negatiiviset vaikutukset perusoikeuksiin olisivat niin huomattavia, ettei suuremmatkaan hyödyt voisi sitä oikeuttaa.²⁴²

Kahdessa muussa lausunnossa myös kyseenalaistettiin tietoliikennetiedustelun tuottama turvallisuushyöty vedoten siihen, ettei sen tuottamia tuloksia tai hyötyjä ole esitetty lainkaan tai niitä ei ole riittävästi.²⁴³ Lisäksi yhdessä lausunnossa rajoitusperusteen painoarvo kyseenalaistettiin vetoamalla mietinnössä esitettyjen uhkakuvien epämääräisyyteen ja, että ”kansallisen turvallisuuden” käsite on liian epämääräinen voidakseen toimia perusoikeuden rajoitusperusteena.²⁴⁴

Suhteellisuusvaatimus sisältää myös perusoikeuksien rajoituksilta vaadittavan *välttämättömyysvaatimuksen* eli rajoitusperusteen on oltava välttämätön hyväksyttävän tarkoituksen saavuttamiseksi. Perusoikeutta rajoittavan sääntelyn on oltava välttämätöntä, joka tarkoittaa sitä, ettei käytettävissä ole muuta vastaavaan tehokkuuteen yltävää vaihtoehtoista keinoa, joka rajoittaisi perusoikeutta vähemmän verrattuna valittuun keinoon tai ei rajoittaisi sitä lainkaan.²⁴⁵ Kyse on siis perusoikeusrajoitusten minimoinnista, käsillä olevien vaihtoehtojen valinnassa ja vaihtoehtojen tehokkuuden arvioinnista.

Välttämättömyysvaatimuksen huomioonottamista vaadittiin 11:sta (19,61 %) lausunnossa, joissa käsiteltiin tiedustelulakihankkeeseen liittyviä perusoikeuskysymyksiä.

²⁴² Scheinin, lausunto s. 6 – 11.

²⁴³ Electronic Frontier Finland - Effi ry, lausunto s. 3. Voutilainen, lausunto s. 4.

²⁴⁴ Piraattipuolue, lausunto s.

²⁴⁵ Viljanen 2001, s. 205 – 206, 212.

Tietoliikennetiedustelun välttämättömyyttä perusteellisimmin arvio lausunnossaan professori *Scheinin*. Hänen mukaan vain tosiasiallisesti tehokas perusoikeusrajoitus voi olla välttämätön. Perusoikeutta rajoittavaa toimintaa ei voida pitää olla välttämättömänä, jollei se ole tehokasta, mukaan lukien kustannustehokasta. Scheinin mukaan elektronisen massavalvonnan tehokkuudesta ei ole esitetty luotettavaa eikä riittävää näyttöä sitä harjoittavien tiedusteluorganisaatioiden taholta. Näin ollen massavalvonnan tehokkuus onkin erittäin kiistanalainen kysymys. Hän osoittaa massavalvonnan tehottomuuden kolmella perustelulinjalla²⁴⁶. Scheinin näkee massavalvonnassa olevan resurssien kohdentamisen ongelma, eli voimavaroja käytetään lisätiedon hankintaan, vaikka painopisteen tulisi olla jo tiedossa olevien potentiaalisten tekijöiden seurannassa ja heidän mahdollisten tekojen estämisessä.²⁴⁷

Välttämättömyysvaatimuksen huomioonottamisen yhteydessä useimmissa sitä koskevissa lausunnoissa mietintöä kritisoidaan siitä, ettei tietoliikennetiedustelun tarpeellisuutta, käyttökohteita ja erityisesti sen tehokkuutta ole kuvattu riittävän tarkasti, minkä vuoksi jää epäselväksi, onko sen keinoin perusoikeuksiin puuttuminen todellakin välttämätöntä.

Välttämättömyysvaatimukseen liittyy myös liikenne- ja viestintäministeriön esittämä huomio työryhmän tapaan käsitellä tietoyhteiskuntakaaren 272 §:ää verkkovalvonnan yhteydessä. Tietoyhteiskuntakaaren 272 § mahdollistaa tietoliikenteen seulonnan, jotta voidaan huolehtia tietoturvasta. Tämä seulonta rinnastetaan mietinnössä ministeriön mukaan tarkoitushakuisesti ja harhaanjohtavasti verkkovalvontaan. Se, että tietoyhteiskuntakaaren 272 §:n tietoliikenteen seulontatoimenpiteet ovat teknisesti lähellä verkkovalvonnan toimenpiteitä, ei anna perustetta verkkovalvonnan vertaamiseen tietoyhteiskuntakaaren mahdollistamiin toimiin ja näin ollen verkkovalvonnasta säätämiseen. Tietoyhteiskuntakaaren 272 §:n tarkoituksena on nimenomaisesti edistää luottamuksellisen viestinnän suojan toteutumista. Sen sijaan verkkovalvontaa koskevaa sääntelyä ei ministeriön mukaan voida perustella luottamuksellisen viestinnän suojaamisella, eikä siinä toteutettaisi sellaista sääntelyä, joka olisi perusoikeuden toteutumisen kannalta *välttämätöntä*. Sen tarkoitus on päinvastaisesti tiedon luottamuksellisuuden murtaminen.²⁴⁸

²⁴⁶ 1. Taloudelliset ja henkilöstövaikutukset ovat selvittämättä, 2. SURVEILLE -tutkimushankkeen tulokset, 3. Oletettuihin todennäköisyyksiin perustuva ajatuskoe.

²⁴⁷ Scheinin, lausunto s. 5, 11.

²⁴⁸ Liikenne- ja viestintäministeriö, eriävä mielipide s.20.

Perusoikeuden ydinalueen koskemattomuus

Lausunnoissa todettiin, että tietoliikennetiedustelulla hankittaisiin tietoja yksityisyyden suojan ja luottamuksellisen viestin salaisuuden suojan ydinalueeseen kuuluvasta viestin sisällöstä ja viestinnän tunnistamistiedoista.

Perusoikeuskysymyksiä käsittelevistä lausunnoista 12:ssa (23,53 %) nähtiin tietoliikennetiedustelun keinot perustuslain vastaisina, koska tiedustelun kohdistuessa viestinnän sisältöön, loukataan yksityisyyden ja luottamuksellisen viestin salaisuuden suojan ydinaluetta. Lisäksi perusoikeuden ydinalueen koskemattomuuteen liittyvissä argumenteissa tuotiin esille näkemys, että perinteinen käsitys luottamuksellisen viestin *sisällön* ja *tunnistamistietojen* välisestä kategorisesta jaosta suojan ydin- ja reuna-alueeseen ei aina ole perusteltua, vaan huomiota olisi kiinnitettävä myös rajoituksen merkittävyyteen ja, että perusoikeusrajoituksen astetta on syytä arvioida kokonaisuutena.

Toisin sanoen yksityisyyden suoja ei lausunnonantajien mukaan välttämättä rajoitu ainoastaan viestin sisältöön ja että myös viestin tunnistetiedot voivat kuulua suojan piiriin. Tunnistamistietojen keräämistä ja tallentamista sekä niiden yhdistämistä muihin käytettävissä oleviin viestinnän tietoihin, ei voida enää pitää vain perusoikeussuojan reuna-alueelle kohdistuvana sallittuna perusoikeuden rajoittamisena.²⁴⁹

Tätä argumenttia perusteltiin perustuslakivaliokunnan tietoyhteiskuntakaarta koskevalla lausunnolla, jossa on lausunnonantajien mukaan viitteitä tulkintakäytännön muutoksesta. Tulkintakäytännön muutos voi johtaa ministeriön mukaan siihen, että perustuslakivaliokunta voi tulevaisuudessa ottaa sellaisen kannan, että myös tunnistamistiedoille on annettava viestinnän sisältöä vastaava suoja, mikäli perusoikeuden rajoitus arvioidaan merkittäväksi.²⁵⁰ Toisena perusteena käytettiin EU-tuomioistuimen ratkaisua koskien ns. Data Retention –direktiiviä, jota tuomioistuin piti perusoikeuksia loukkaavana pätemättömänä. Direktiivin pätemättömäksi julistamisesta huolimatta tuomioistuin kuitenkin katsoi, ettei direktiivi loukannut yksityisyyden suojan ja tietosuojan ydinsisältöä, koska sen määräykset rajoittuivat vain tunnistamistietoihin. Tästä huolimatta tuomioistuin kuitenkin katsoi kyseessä olleen *erittäin vakava* puuttuminen yksityisyyden suojaan ja tietosuojaan perusoikeuksina ja vahvisti niiden loukkauksen.²⁵¹

²⁴⁹ Liikenne- ja viestintäministeriö, eriävä mielipide s. 17.

²⁵⁰ Ibid, s. 17.

²⁵¹ Scheinin, lausunto s. 3.

Viestinnän tunnistamistietoihin kohdistuvan tiedustelun osalta sallivamman kannan otti Suomen Asianajajaliitto, jonka mukaan suhteellisuusperiaatteen puitteissa viestintään kohdistuva valvonta tulisi ensisijaisesti toteuttaa tietoliikenteen tunnistamistietoihin perustuvien toimien avulla. Tunnistamistietojen valvonta automaattisesti toteutettuna, soveltuvin osin tietoyhteiskuntakaassa luotuja oikeuksia noudattaen, Asianajajaliiton näkemyksen mukaan minimoisi yksityisyyden suojaan puuttumista.²⁵²

Rajoitusedellytyksen täsmällisyys- ja tarkkarajaisuusvaatimus

Täsmällisyys ja tarkkarajaisuusvaatimuksen toteutumisen ydinajatuksena on, että rajoituksen keskeisen sisällön tulee ilmetä itse laista, eikä sitä saa jättää alemmanasteisen normin antajan tai lain soveltajan harkinnan varaan.²⁵³

Vaatimus perusoikeuksia rajoittavien tiedustelutoimien täsmällisyydestä ja tarkkarajaisuudesta ilmaistiin lausunnoissa hyvin vaihtelevasti. Perusoikeuskysymyksiä käsittelevistä lausunnoista 18:ssä (35,29 %) vaadittiin täsmällisyys- ja tarkkarajaisuusvaatimuksen huomioonottamista ja pääasiassa vaatimus yhdistettiin mietinnössä esitettyyn tietoliikennetiedustelun sääntelyyn.

Microsoftin lausunnossa tämän rajoitusedellytyksen toteutumista vaadittiin niin, että viranomaisten toimivalta internetin käyttäjien tietojen keräämiseen tulee olla lailla säädettyä ja rajoitettua sekä tietojen keruun tulee tapahtua vain tarkoin *rajatuissa olosuhteissa*.²⁵⁴ Oikeuskanslerinviraston mukaan ”*yksityiselämän suojan näkökulmasta keskeistä olisi, kuinka täsmällisiä ja tarkkarajaisia tietoliikennetiedustelulla saatavien tietojen seulonnassa käytettävät hakuehdot käytännössä olisivat uhkien torjunnan osalta*”.²⁵⁵

Viestintävirasto edellyttää *kansallinen turvallisuuden* ja sitä uhkaavien *uhkien* määrittelemistä tiedustelulaissa mahdollisimman selkeästi, tarkasti ja suppeasti, koska niitä käytettäisiin tietoliikennetiedustelun automaattisen seulonnan hakuehtoina.²⁵⁶ Kansallisen turvallisuuden löyhän

²⁵² Suomen Asianajajaliitto, lausunto s. 4.

²⁵³ Viljanen 2001, s. 116.

²⁵⁴ Microsoft Oy, lausunto s. 4.

²⁵⁵ Oikeuskanslerinvirasto, lausunto s. 3.

²⁵⁶ Viestintävirasto, lausunto s. 3

määritelmän soveltumattomuuteen rajoitusperusteena ja sitä uhkaaviin epämääräisiin uhkiin vedotaan myös muissa lausunnoissa.²⁵⁷

Ei pelkästään tietoliikennetiedusteluun liittyen, mutta myös laajemmin ajateltuna tiedustelua koskevan *sääntelyn* tulee olla täsmällistä ja tarkkarajaista, lisäksi tiedusteluun liittyvät *käsitteet* tulee yksilöidä riittävän tarkasti. Poliisihallitus vaatii launnossaan, että yksityisyyden suojan turvaamiseksi tiedustelutoiminnalle on asetettava selkeästi ymmärrettävissä olevat rajat, koska tiedustelutiedon hankinta ajoittuu yleensä tilanteeseen, jossa ei vielä ole perusteltua epäilyä kenenkään syyllistymisestä tiettyyn rikokseen.²⁵⁸

Lausunnoissa esitetyt täsmällisyys- ja tarkkarajaisuusvaatimukset kohdistuvat erilaisiin kohteisiin. Osassa lausunnoista täsmällistä ja tarkkarajaista sääntelyä vaadittiin tietoliikennetiedustelun tiedonkeruun olosuhteilta ja siinä käytettäviltä hakuehdoilta. Joissakin vaatimus taasen kohdistui tiedustelun käsitteisiin ja kansallinen turvallisuuden sekä uhkien määrittelyyn. Riippumatta vaatimuksen kohteesta, kaikkien ilmaukset voitaneen yhdistää ajatukseen siitä, että laista on riittävän selvästi käytävä ilmi, ne olosuhteet ja edellytykset, joiden toteutuessa henkilö voi joutua viranomaisten toteuttaman elektronisen tarkkailun tai muiden tiedustelutoimien kohteeksi.²⁵⁹

Ihmisoikeusvelvoitteiden noudattaminen

Tähän kategoriaan sijoitin kaikki argumentit, jotka liittyvät ihmisoikeusvelvoitteiden noudattamiseen ja joissa mainittiin kansainväliset ihmisoikeussopimukset, Euroopan ihmisoikeustuomioistuimen ja EU-tuomioistuimen käytäntö sekä EU:n ja YK:n toimielinten päätökset. Ihmisoikeusvelvoitteita käytettiin argumenttina 18:ssä (35,29 %) launnossa, joissa käsiteltiin perus- ja ihmisoikeuskysymyksiä. Ihmisoikeusvelvoitteiden huomioonottamisen vaatimus liittyi kaikissa em. lausunnoissa nimenomaan tietoliikennetiedusteluun.

Viljasen mukaan ihmisoikeusvelvoitteiden noudattamisen vaatimus tarkoittaa sitä, että niitä koskevat rajoitukset eivät saa olla ristiriidassa Suomea velvoittavien kansainvälisten ihmisoikeussopimusten kanssa.²⁶⁰ Tämän kategorian osalta on huomionarvoista se, että osassa lausunnoista ei nähty olevan ristiriitaa ihmisoikeusvelvoitteiden kanssa. Suomen Asianajajaliitto, oikeusministeriö ja suojelupoliisi katsoivat lausunnoissaan Euroopan ihmisoikeustuomioistuimen oikeuskäytännön

²⁵⁷ Piraattipuolue, lausunto s. 3. Vasemmistoliitto, lausunto s. 2.

²⁵⁸ Poliisihallitus, lausunto s. 2.

²⁵⁹ Tiedonhankintalakiyöryhmän mietintö, s. 64.

²⁶⁰ Viljanen 2001, s. 37 – 38.

hyväksyvän verkkovalvonnan, jos sitä suoritetaan ”muun muassa kansallisen ja yleisen turvallisuuden intresseissä ja toiminnan ollessa riittävän oikeudellisen sääntelyn alaista”.²⁶¹

Kuitenkin yleisin tähän kategoriaan sijoittuvista argumenteista (7 kpl) käsitteli Euroopan Unionin tuomioistuimen ratkaisua, jolla ns. Data Retention –direktiivi julistettiin perusoikeuksia loukkaavana pätemättömäksi.²⁶² Direktiivin pätemättömäksi julistamisesta huolimatta tuomioistuin kuitenkin katsoi, ettei direktiivi loukannut yksityisyyden suojan ja tietosuojan ydinsisältöä, koska sen määräykset rajoittuivat vain tunnistamistietoihin. Tästä huolimatta tuomioistuin kuitenkin katsoi kyseessä olleen *erittäin vakava* puuttuminen yksityisyyden suojaan ja tietosuojaan perusoikeuksina ja vahvisti niiden loukkauksen.²⁶³ Lavapuron mukaan tämä EUT:n ratkaisu on tällä hetkellä auktoritatiivisin tulkintakannanotto siihen millaisia rajoituksia yksityiselämän suoja asettaa luottamuksellisten viestien kohdentamattomalle massavalvonnalle. Data Retention –tuomion perusteella professori Lavapuro pitää tietoliikennetiedustelua ehdotetulla tavalla toteutettuna em. ratkaisun vastaisena, koska siinä automaattiset hakuehdot kohdistuvat ennalta rajoittamattomaan joukkoon yksityistä viestintää, eivätkä hakuehdot lainkaan rajaa niitä olosuhteita ja edellytyksiä, joissa kansalaiset voivat joutua salaisesti toteutettavan tarkkailun kohteeksi.²⁶⁴

Edellä mainittujen kantojen väliin sijoittuu muissa lausunnoissa esiin tuotu velvoite noudattaa kansainvälisiä ihmisoikeusvelvoitteita yleisesti. Vaikka Euroopan ihmisoikeustuomioistuin on sallinut tietynasteisen verkkovalvonnan kansallisen turvallisuuden nimissä, ei sitä Piraattipuolueen mukaan kuitenkaan voida pitää suositeltavana.²⁶⁵

Hyväksyttävyyysvaatimus

Perusoikeuskysymyksiä käsittelevistä lausunnoista 11:ssä (35,29 %) vaadittiin, että perusoikeutta rajoittavalta perusteelta on edellytettävä hyväksyttävää tarkoitusta.

Kuten Scheinin lausunnossaan toteaa perustuslain 10.3 §:ssä yksityiselämän suojan hyväksyttävänä rajoitusperusteina kotirauhan piirissä mainitaan vain perusoikeuksien turvaaminen ja rikosten selvittäminen. Saman lainkohdan mukaan luottamuksellisen viestin salaisuutta saadaan hyväksyttävästi rajoittaa vain yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien

²⁶¹ Suomen Asianajajaliitto, lausunto, s. 3.

²⁶² Ratkaisussa yhdistetty asiat C-293/12 ja C594/12, Lavapuro käyttää ratkaisusta nimeä Digital Rights Ireland –tuomio.

²⁶³ Scheinin, lausunto s. 3.

²⁶⁴ Lavapuro, lausunto s. 1 ja 5.

²⁶⁵ Piraattipuolue, lausunto, s. 2.

rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.²⁶⁶

Oikeusministeriön mukaan PL 10 §:n 3 momentissa säädetty perusteet luottamuksellisen viestin suojan rajoittamiselle on tarkoitettu tyhjentäviksi, eikä perustuslaki siten tunnista viestin salaisuuden mahdollisena rajoitusperusteena kansallista turvallisuutta.²⁶⁷ Samoilla linjoilla lausunnossaan oli myös liikenne- ja viestintäministeriö, joka totesi, ”*ettei kansallista turvallisuutta ole mainittu perustuslain 10.3 §:ssä perusteena rajoittaa viestinnän luottamuksellisuutta*”. Puuttuvan hyväksyttävän tarkoituksiperän argumenttia liikenne- ja viestintäministeriö vahvistaa vetoamalla siihen, että Euroopan parlamentin näkemyksen mukaan edes terrorismin torjunta ei voi oikeuttaa kohdentamattomia ja salaisia laajamittaisen valvonnan ohjelmia, ja että tällaiset ohjelmat ovat ongelmallisia EU:n perusoikeuksien näkökulmasta.²⁶⁸

Samaan seikkaan kiinnittää lausunnossaan huomiota professori Lavapuro toteamalla, että ehdotetun kaltaiset tiedusteluvaltuudet eivät mahdu PL 10 §:n 3 momentin rajoitusedellytysten sisään. Lavapuro lisää vielä, että valtiosääntöoikeudelliset ongelmat eivät välttämättä poistuisi edes poistamalla nyt ongelmia aiheuttavat lakivaraukset tai lisäämällä PL 10 §:ään rajoitusperusteeksi kansallinen turvallisuus. Hänen mukaan pelkästään hyväksyttävän rajoitusperusteen käsillä olo ei riitä, vaan myös yleisten rajoitusedellytysten on täytyttävä.²⁶⁹ Edellä oleviin näkemyksiin yhtyy myös professori Scheinin, jonka mukaan mietinnössä esitetyt tarkoituksiperät tiedustelulle ”*ovat varsin kaukana PL 10 §:n 3 momentin sanamuodosta*”.²⁷⁰

8 Johtopäätökset

Turvallisuuden takaamiseksi yhteiskuntamme on kyettävä torjumaan erilaisia uhkia, näin ollen on selvää, että tiedustelulakeja puollettiin juuri uhkiin vetoamalla. Lausunnoista 46:ssa puollettiin tiedustelulakeja ja niistä 22 lausunnonantajaa käytti pontenaan muun muassa erilaisia uhkia. Varsinkin terrorismi, vakoilu ja kyberhyökkäysten nousivat esiin merkittävimpinä uhkina, jotka heikentävät kansallista turvallisuutta, tämä näkyikin selvästi noissa 22:ssa lausunnossa, joissa em. uhkia käytettiin perusteena 30 kertaa.

²⁶⁶ Scheinin, lausunto s. 4.

²⁶⁷ Oikeusministeriö, lausunto s. 2.

²⁶⁸ Liikenne- ja viestintäministeriö, eriävä mielipide, s. 5, 16.

²⁶⁹ Lavapuro, lausunto s. 9 – 10.

²⁷⁰ Scheinin, lausunto s. 4.

Vastustavien lausuntojen osalta määrällisesti suurimmiksi (27,7 %) ²⁷¹ kategorioiksi nousseiden tietoliikennetiedustelun tehottomuusväitteen ja sen kohdentamattomuuden (18,2 %) voidaan mielestäni perusoikeuskysymysten osalta yhdistää suhteellisuus- ja välttämättömyysvaatimukseen sekä hyväksyttävyyysvaatimukseen. Kohdentamaton massavalvonta olisi suhteeton keino oikeuttamaan perusoikeuksien rajoittamista. Vain tehokas perusoikeusrajoitus voidaan katsoa välttämättömäksi, eikä tietoliikennetiedustelun tehokuutta ole voitu osoittaa. Kohdentamattomana massavalvontana toteutettu tietoliikennetiedustelu terrorismin torjunnan tarkoituksessa ja kansallisen turvallisuuden nimissä eivät ole hyväksyttäviä perusteita rajoittaa yksityiselämän suojaa.

Koska tietoliikennetiedustelun tehokkuudesta ei ole esitetty kiistattomia eikä riittäviä tuloksia tai hyötyjä, on helppo yhtyä professori Scheinin'in näkemykseen, että *”vain tosiasiallisesti tehokas perusoikeusrajoitus voi olla välttämätön, ja että vain tehokas keino voi olla oikeasuhtainen siitä seuraavan perusoikeusrajoituksen verrattuna”*. ²⁷²

Mietinnöstä ja annetuista lausunnoista esiin tulleen kiistattomana tosiseikkana voidaan todeta, esitetyistä uusista tiedustelumenetelmistä yksilön perus- ja ihmisoikeuksiin vaikuttaisi eniten tietoliikennetiedustelun toimenpiteet, jotka toteutuessaan loukkaisivat ja rajoittaisivat luottamuksellisen viestin ja yksityisyyden suojaa.

Koska mietinnössä esitetyllä tietoliikennetiedustelulla puututtaisiin luottamuksellisen viestin salaisuuteen ja yksityisyyden suojaan, tulee tiedustelulakeja säädettäessä huomioida, että näitä oikeuksia koskevissa lakivarauksissa on tyhjentävästi mainittu ne hyväksyttävissä olevat perusteet, joilla näitä oikeuksia voidaan rajoittaa. Mikäli lainsäädännöllä halutaan puuttua luottamuksellisen viestin salaisuuteen tai yksityisyyden suojaan, ainoastaan sellaiset intressit, jotka kuuluvat näissä lakivarauksissa mainittujen intressien turvaamisen piiriin, voivat tulla kyseeseen hyväksyttävänä perusteina tietoliikennetiedustelun käytölle. ²⁷³ Perusoikeuden rajoitusperusteen hyväksyttävän tarkoituksen suhteen perustuslaki asettaa kansainvälisiin ihmisoikeussopimusvelvoitteisiin verrattuna tiukemmat ehdot, sillä esimerkiksi Euroopan ihmisoikeussopimuksen 8 artikla sallii kansallisen turvallisuuden mahdollisena perusteena luottamuksellisen viestin suojan rajoittamiselle.

Kansallinen turvallisuus ei sovellu luottamuksellisen viestin salaisuuden rajoitusperusteeksi, koska hyväksyttävät rajoitusperusteet on määritelty tyhjentävästi PL 10 §:ssä, eikä siinä mainita kansallista turvallisuutta. Oikeusministeriön asettama asiantuntijatyöryhmä selvitti luottamuksellisen viestin

²⁷¹ Kts. luku 7.3 s.

²⁷² Scheinin, lausunto s. 4 ja 11.

²⁷³ Metsäranta 2015, s. 103 – 104.

salaisuuden suojaa koskevan perustuslakisääntelyn tarkistamista 11.10.2016 julkaistussa mietinnössä. Työryhmän näkemyksen mukaan ”perustuslain sanamuodon ja sen nykyisen tulkintakäytännön mukaan ei olisi mahdollista säätää sellaisista rajoituksista luottamuksellisen viestin salaisuuteen, joiden tarkoituksena olisi laajemmalti kansallisen turvallisuuden kannalta välttämättömän tiedon hankkiminen vakavista uhkista, erityisesti uhkiin varautumiseksi ja niiden ennakoimiseksi sekä valtion ylimmän johdon päätöksenteon tueksi”.²⁷⁴

Kuten edellä on todettu, ei luottamuksellisen viestin suojan ydinalueen määrittely ole riidatonta, kiistaa ja näkemyseroja on siitä, kuuluuko viestin tunnistamistiedot perusoikeuden ytimeen. Vaikka luottamuksellisen viestin suojan ytimen sisällöstä ja tunnistamistietojen asemasta ytimessä vai reuna-alueella ei päästäisikään yhteisymmärrykseen, takaa suhteellisuusvaatimus sen, ettei luottamuksellisen viestin suoja perusoikeutena murene merkityksettömäksi. Vaatimus perusoikeusrajoituksen merkittävyyden huomioonottamisesta ja rajoituksen asteen kokonaisarvion tekemisestä palauttaa ydinalueen koskemattomuusvaatimuksen suhteellisuusvaatimukseen.²⁷⁵

Koska tietoliikennetiedustelulla puututtaisiin ainakin osaltaan perusoikeuden ydinalueeseen, tulisi ”kansallinen turvallisuus” säätää perustuslakiin yhdeksi suojattavaksi perusoikeudeksi, jotta päästäisiin suorittamaan perusoikeuksien kollisiotilanteen vaatima punninta niillä suojattavien intressien välillä.

Tiedustelulakeja ja tiedustelukeinoja säädettäessä haasteena on löytää hyväksyttävissä oleva tasapaino turvallisuuden takaamiseksi tehtävien toimien ja perusoikeuksien toteutumisen välillä. Mutta miten tähän päästään? Ääripäiden toteuttamisvaihtoehdot ovat; rajoittamaton kaiken tietoliikenteen valvominen ilman perusoikeussuojaa, toisena ääripäänä nykyiset salaiset tiedonhankintakeinot. Tasapaino pitäisi löytää siis näiden välimaastosta. Vastakkain tasapainon löytämisessä asettuu valtion kyky torjua kansallista turvallisuutta vakavasti uhkaavia toimia ja kansalaisten perusoikeuksien toteutuminen. Arvioitaessa jonkin toimen tarpeellisuutta, välttämättömyyttä ja suhteellisuutta tulisi arvioinnin osoittaa toimen olevan tehokas, eikä sillä ole kielteisiä vaikutuksia tai niitä on vain vähän, eikä toimelle ole olemassa muita vaihtoehtoja. Jotta

²⁷⁴ Oikeusministeriön julkaisu 41/2016, s. 12 – 13.

²⁷⁵ Metsäranta 2015, s. 111.

tietoliikennetiedustelu olisi hyväksyttävä keino viranomaisille turvallisuuden lisäämiseksi ja takaamiseksi, tulisi sen olla todistettavasti tehokas, saavuttaen tuloksia, joita ei kyetä muilla keinoin saavuttaa.

Ehdotettuja tiedustelutoimia voi hyvin verrata poliisin salaisiin tiedonhankintakeinoihin, joista ryhdyttiin säätämään toimivaltuuksia 1992 alkaen. Nykyisten voimassa olevien salaisten tiedonhankintakeinojen toimivaltuuksien säätäminen kesti yli 20 vuotta. Julkisessa keskustelussa puhelin- ja telekuuntelun sallivaa lakia tietysti niin vastustettiin kuin myös kannatettiin. Vastargumenteissa sitä pidettiin tarpeettomana, alttiina väärinkäytöksille ja perustuslaillisia oikeuksia loukkaavana. Lain kannattajat pitivät telekuuntelua erityisen tehokkaana keinona yhdyntävässä Euroopassa lisääntyvän suunnitelmallisen, organisoituneen ja kansainvälisen rikollisuuden tutkinnassa. Telekuuntelu rikosten selvittämiseksi mahdollistettiin Suomessa 1.6.1995 voimaan tulleella pakkokeinolain (402/95) muutoksella.²⁷⁶

Vuosikymmeniä jatkunut yhteiskunnallinen keskustelu poliisin telekuunteluoikeuksista osoittaa, kuinka vaikeaa on perustella ja päättää uusista salaisista tiedonhankintatoimivaltuuksista vakavien yhteiskuntaa uhkaavien toimien tai rikosten torjumiseksi.²⁷⁷ Valmisteilla olevia tiedustelulakeja vastustetaan ja puolletaan hyvin samanlaisin argumentein kuin aikanaan telekuuntelun sallivaa lakialoitetta. Mielenkiintoisena pidän havaintoani siitä, että kansalaiset suhtautuvat vähemmän kriittisesti heitä koskevien tietojen keräämiseen, analysointiin ja käyttöön, kun se tapahtuu yksityisten toimijoiden (Google, Facebook, kauppaketjut) toimesta. He suhtautuvat tällaisten tahojen tiedonkeruuseen arkipäiväisesti ja hyväksyvät sen ilman suurempaa kritiikkiä. Kun taas tietojen kerääminen tapahtuu viranomaisten toimesta, ovat kansalaiset hyvin kriittisiä ja huolissaan yksityisyyden suojastaan ja perusoikeuksiensa loukkaamisesta.

Yhdyn niiden lausunnonantajien näkemyksiin siitä, ettei perustuslain 10 §:n 3 momentin nykyinen sanamuoto eikä sen tulkintakäytäntö anna mahdollisuutta rajoittaa lainsäädännöllä luottamuksellisen viestin salaisuutta kansallisen turvallisuuden nimissä. Mielestäni kansallinen turvallisuus voitaisiin kuitenkin lisätä PL 10 §:ään perustuslain vaatimana välttämättömänä perusteena, jotta luottamuksellisen viestin salaisuutta voitaisiin rajoittaa sellaisen tiedon hankkimiseksi, jolla turvattaisiin kansallista turvallisuutta vakavilta uhkilta.

²⁷⁶ Hankilanoja 2014, s. 70 – 71 ja 77.

²⁷⁷ Hankilanoja 2014, s. 78.

Tämä kuitenkin edellyttää, että esimerkiksi tietoliikennetiedustelun mahdollistavan lain tulee olla riittävän tarkkarajainen ja edellyttävän salaisten pakkokeinojen käytön mukaista lupamenettelyä, riittäviä oikeussuojakeinoja tiedustelun kohteille, toiminnan harjoittavan sisäistä ja ulkoista valvontaa sekä harjoitetun tietoliikennetiedustelun määrästä ja tuloksista raportointia.

Kuten olen aiemminkin todennut, liittyy tiedustelutoiminnan ja –organisaatioiden akateemisen tutkimuksen vähyys – ainakin julkaistavan – käsittääkseni sen salaiseen ja salassa pidettävään perusolemukseen. Oikeudellisen lisätutkimuksen kohteena voisi kuitenkin jatkossa, tulla kyseeseen esimerkiksi tiedustelun kohteeksi joutuvien oikeussuojakeinojen riittävyyden ja tiedustelutoiminnan valvonnan toimivuuden arviointi.