Haaga-Helia
ammattikorkeakoulu Oy

Siviilitiedustelulainsäädännöllä kohti Orwellin maailmaa?

Pekka Seppänen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2019

Haaga-Helia ammattikorkeakoulu Oy

Tekijä(t)
Pekka Seppänen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön nimi
Siviilitiedustelulainsäädännöllä kohti Orwellin maailmaa?

Sivu- ja liitesivumäärä
37

Heinäkuussa 2019 Suomen lainsäädäntö muuttui oleellisesti tietoliikenteeseen kohdistuvan tiedonhankinnan osalta. Suojelupoliisille ja Puolustusvoimille tuli oikeus seurata verkkoliikennettä siviili- ja sotilastiedustelussa. Tämän opinnäytetyön tavoitteena on selvittää, miten siviilitiedustelulainsäädäntö muutti poliisin toimivaltuuksia hankkia tietoa tietoverkoista. Opinnäytetyö on toteutettu kirjallisuuskatsauksena ja pääasiallisena lähteenä on käytetty voimassaolevaa lainsäädäntöä sekä niihin liittyviä esitöitä.

Suojelupoliisi on ainoa viranomainen, joka voi tehdä tietoverkkoon kohdistuvaa siviilitiedustelua. Aikaisemmin tiedonhankinta kohdistui epäiltyyn tekijään tai rikokseen. Siviilitiedustelu taas kohdistuu sellaiseen toimintaan, jonka epäillään uhkaavan kansallista turvallisuutta. Toiminta ei välttämättä täytä rikoksen tunnusmerkistöä valmisteluvaiheessa eikä uhkan toteutuessakaan asiasta välttämättä voida aloittaa esitutkintaa. Tiedustelulainsäädännön myötä suojelupoliisin rooli muuttui niin, että se ei voi enää suorittaa esitutkintaa. Tämä oli edellytyksenä suojelupoliisin laajempien tiedonhankintaoikeuksien saamiseksi.

Teknisesti suurin muutos oli se, mistä kohdasta tietoverkkoa tietoa kerätään. Aikaisemmin tiedonhankinta kohdistui pelkästään tietoverkon reunaan ja tiettyyn kohteeseen, jolloin sivullista liikennettä ei päätynyt viranomaisen haltuun. Nyt tietoliikennetiedustelu tapahtuu tietoverkon keskellä, jolloin käsittelyyn tulee myös ulkopuolista viestiliikennettä. Liikennettä voidaan suodattaa vain ohjaus- ja välitystietojen perusteella eikä viestin sisältöä saa avata suodatusvaiheessa. Suojelupoliisi käsittelee suodatetun liikenteen ja voi avata tässä vaiheessa myös viestin sisällön.

Lainsäädäntöpaketin yhtenä tärkeänä osana oli myös tietoliikennetiedustelun laillisuusvalvonta ja sen seuranta. Lakipakettiin kuului laki tietoliikennetiedustelun valvonnasta, jossa määriteltiin kaksi uutta valvontaelintä aikaisempien lisäksi. Parlamentaarisesta valvonnasta vastaa tiedusteluvalvontavaliokunta ja tiedusteluvalvontavaltuutettu vastaa tiedustelutoiminnan laillisuusvalvonnasta ja seurannasta.

Asiasanat
Tiedustelulaki, tietoliikennetiedustelu, siviilitiedustelulainsäädäntö

Sisällys

1 Johdanto

1.1 Tutkimuksen tavoite

Yhdysvalloissa 9.11.2001 tapahtuneen terroriteon jälkeen verkossa tapahtuvaan valvontaan liittyvät viranomaisoikeudet ovat lisääntyneet kaikkialla maailmassa. Erilaisten kansallisten ja kansainvälisten uhkien perusteella viranomaisten oikeuksia valvoa verkkoliikennettä on muutettu niin paljon, että niiden on jopa katsottu puuttuvan ihmisten yksityisyydensuojaan. Missä menee raja yksityisen ja yhteiskunnan edun välillä? Onko George Orwellin kirjassaan Vuonna 1984 kuvaama tilanne kohta todellisuutta:

> Teleruutu oli sekä vastaanotin että lähetin. Se kuuli jokaisen Winstonin hiirenhienoa hiiskausta kovemman äännähdyksen, ja niin kauan kuin hän pysyi metallilevyn näkökentässä, häntä ei vain kuunneltu, hänet myös nähtiin siinä. Hän ei tietenkään koskaan tiennyt, millä hetkellä häntä tarkkailtiin. Saattoi vain arvata, kuinka usein tai minkä menetelmän avulla ajatuspoliisi kytkeytyi yksityisen ihmisen verkkoon. Oli jopa mahdollista että kaikkia valvottiin koko ajan. (Orwell 1999, 12.)

Hallitus jätti esityksen eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi 25.1.2018. Eduskuntakäsittelyn jälkeen hallituksen esitys hyväksyttiin 11.3.2019 ja se tuli voimaan 1.6.2019. Tiedustelulainsäädännöllä tarkoitetaan tässä tutkimuksessa tiedustelua, jonka päämääränä on ennalta estää suomalaisiin tai Suomen valtioon kohdistuvia uhkia. Tässä tutkimuksessa käsitellään verkkotiedusteluun liittyvää lainsäädäntöä. Tietoliikennetiedustelulla pyritään havaitsemaan sellaista toimintaa, joka ensisijaisesti uhkaa kansallista turvallisuutta. Myöhemmin tekstissä käytän lyhennettä TTST, kun viittaan lakiin Laki tietoliikennetiedustelusta siviilitiedustelussa. En ole toistaiseksi löytänyt laille mitään virallista lyhennettä.

Tutkimuksen tavoitteena on saada käsitys, miten lakiesitys muutti voimaan tullessaan viranomaisen oikeutta tehdä tiedonhankintaa verkossa ja mitä rajoituksia siinä on. Keskeisenä kysymyksenä on, minkälaisia toimivaltuuksia uusi laki toi viranomaisille verrattuna aikaisempaan lainsäädäntöön, kun kohteena on tietoliikenneverkkoon kohdistuva tiedonhankinta. Tutkimuksessa pyritään myös selvittämään, miten laillisuusvalvonta toteutetaan. Tutkimus toteutetaan kirjallisuuskatsauksena. Tärkeimpänä lähteenä on hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi, siviilitiedustelulainsäädäntö sekä tiedonhankintakeinoihin ja pakkokeinoihin liittyvä lainsäädäntö.

Aikaisempaa oikeuskäytäntöä aiheesta ei Suomessa ole, joten laki muutti monia viranomaiskäytäntöjä. Laajemmat oikeudet tuovat myös vastuuta. Miten voidaan varmistaa, että lakia käytetään niin kuin lainsäätäjä on halunnut sitä käytettävän? Viranomainenkin on ihminen, josta on osoituksena oikeudenkäynnit virkavelvollisuuden rikkomisista ja

henkilörekisteririkoksista. Näistä ehkä tunnetuin on Mika Myllylän kuolemaan liittyvien tietojen selailu poliisin rekisteristä ilman perusteltua syytä (Iltalehti 2014).

Tutkimuskysymykset:

- Miten uusi siviilitiedustelulainsäädäntö muuttaa viranomaisten oikeuksia tehdä tiedonhankintaa tietoverkoissa ja miksi lakiuudistukseen oli tarvetta?
- Miten siviilitiedustelulain perusteella tehtyä viranomaistoimintaa on rajoitettu ja miten sitä valvotaan?
- Miten kansalaisten oikeusturva taataan?

1.2 Käytetyt lyhenteet

Esitutkintalaki	ETL
Laki viranomaisten toiminnan julkisuudesta	JulkL
Laki tietoliikennetiedustelusta siviilitiedustelussa	TTST
Pakkokeinolaki	PKL
Poliisilaki	PolL
Suomen perustuslaki	PL

1.3 Verkossa tapahtuva rikollisuus

Teknologian nopea kehitys on muuttanut Suomeen kohdistuvien sisäisten ja ulkoisten uhkien luonnetta. Eri organisaatiot voivat toimia eri valtioiden alueella ja verkostoitua siitä huolimatta tehokkaasti. Viestintään käytettävän teknologian kehittymisen myötä turvallisuusuhkia pitää kyetä tunnistamaan myös Suomen rajojen ulkopuolella toimivien tahojen osalta. Rikostutkinnassa rikoksen tapahtuma-ajalla ja -paikalla on tärkeä rooli mm. määritettäessä sitä, voidaanko esitutkintaa suorittaa. Verkkorikollisuudessa voi olla jopa mahdotonta määrittää, mikä on rikoksen tekopaikka tai tarkka aika.

Turvallisuustilanne on muuttunut nopeasti maailmassa. Suomi on aikaisemmin ollut sivussa vakavimmilta terroriteoilta, mutta tilanne on muuttunut siltäkin osin. Samalla kun ihmisten liikkuvuus on lisääntynyt ja helpottunut, myös turvallisuusuhkat ovat lisääntyneet. Rikolliset ovat siirtyneet tietoverkkoihin ja myös turvallisuusuhkiin liittyvät toimijat käyttävät niitä värväys-, yhteydenpito- ja opetusvälineinään. Tekninen kehitys on mahdollistanut tehokkaan toiminnan aiempaa pienemmillä resursseilla eikä merkittävänkään uhkan taustalla tarvitse olla valtiollinen toimija. Koska verkossa on suhteellisen helppoa toimia anonyymisti, kiinnijäämisen riski on vähäinen.

Lähes kaikki tieto on siirtynyt tietoverkkoihin, myös valtioiden osalta. Vakoilu ja muu laiton tiedonhankinta on tehokkainta ja helpointa toteuttaa verkossa. Yleisesti tietoturva perustuu niin yksityisellä toimijalla kuin valtionhallinnossa kaupallisiin tietoturvaohjelmiin tai erilaisiin tietoturvapalveluihin. Valtiollisen toimijan vakoilua ei ole välttämättä mahdollista

havaita tavallisella kaupallisella tietoturvaohjelmistolla, koska ne voivat olla kehitetty yhtä tiettyä kohdetta varten ja voivat olla hyvin monimutkaisia. Ehkä kuuluisin tämäntyyppinen haittaohjelma on vuonna 2010 Iranissa uraania rikastavan laitoksen lamauttanut Stuxnet. Haittaohjelma oli suunniteltu niin, että se ei vaikuttanut saastuneisiin tavallisiin työasemiin, vaan se aktivoitui vasta kohteena olevassa ympäristössä (Suomen kuvalehti 2010). Vastaavanlainen haittaohjelma esimerkiksi Suomen sähkönsiirron kantaverkossa voisi aiheuttaa vakavaa vaaraa yhteiskunnalle. Verkkoliikenteen valvonnalla voidaan saada yksi työkalu lisää valikoimaan, kun estetään verkkovakoilua tai verkkoon kohdistuvia hyökkäyksiä.

Aikaisemmin lainsäädäntö on säädetty pelkästään sitä silmällä pitäen, että rikos on tapahtunut tai tapahtumassa, eli on olemassa jonkinlainen rikosepäily. Lainsäädäntöä, joka koskee tässä tutkimuksessa käsiteltävää tiedustelua, ei ole ollut aikaisemmin olemassa. Ennen tiedustelulainsäädännön voimaan tulemista tiedustelu käsitettiin rikostorjuntaan liittyvänä tiedonhankinnan toimenpiteenä eikä käsitteitä tiedustelu tai tiedusteluviranomainen ollut olemassa. Rikostorjunnassa verkkoliikenteestä saatavan tiedon hyväksikäyttö koski rikosten ennalta estämistä, rikosten paljastamista, esitutkintaa ja niihin liittyvää lainsäädäntöä.

1.4 Rajaukset

Käsittelen tässä tutkimuksessa vain tietoverkossa tapahtuvaa tiedonhankintaan siviilitiedustelulainsäädännön perusteella. Samassa yhteydessä säädettiin lakipaketti sotilastiedustelusta, mutta jätän sen osan pois tutkimuksestani. Poliisin lisäksi muita esitutkintaviranomaisia ovat rajavartio-, tulli- ja sotilasviranomaiset (ETL 2:1 § 2). Suomessa keskeisin rooli turvallisuusuhkia vastaan on suojelupoliisilla.

> Suojelupoliisin tehtävänä on ennaltaehkäistä ja torjua kaikkein vakavimpia kansallisen turvallisuuden uhkia, kuten terrorismia ja vieraiden valtioiden Suomeen kohdistamaa laitonta tiedustelua. Lisäksi teemme ennakoivaa tiedusteluanalyysiä kansallista turvallisuutta uhkaavista ilmiöistä valtiojohdon ja muiden viranomaisten päätöksenteon tueksi. Teemme myös ennaltaehkäisevää turvallisuustyötä, kuten turvallisuusselvityksiä. (Suojelupoliisi 2019.)

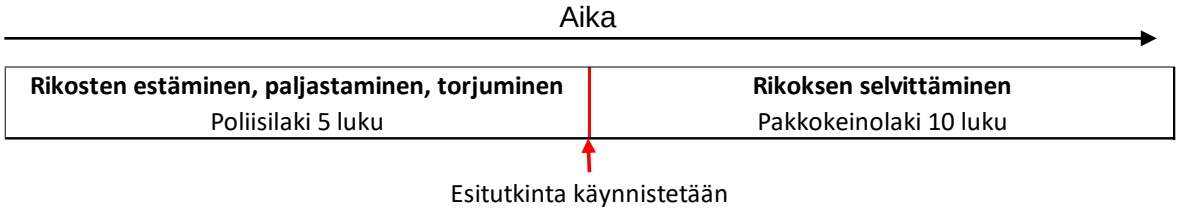
Tässä tutkimuksessa käsitellään vain poliisin ja etenkin suojelupoliisin tehtäviin liittyvää lainsäädäntöä, koska siviilitiedustelulainsäädäntö käsittelee vain suojelupoliisin toimivallan mukaista tiedonhankintaa.

Tutkimuksessa ei käsitellä käytännön toteutusta tai tekniikkaa verkkotiedustelun toteuttamisesta. Teknistä toteutusta ei ole mahdollista selvittää salassapitosäännösten vuoksi (JulkL 6:24 § 5).

2 Viranomaisten tiedonhankinta tietoverkosta poliisilain ja pakkokeinolain perusteella

2.1 Tiedonhankinnan perusteet

Ennen tiedustelulainsäädäntöä viranomaisten toimivaltuudet tulivat pelkästään rikostorjuntatehtäviin liittyvistä tehtävistä. Rikosten ennalta estämiseksi, paljastamiseksi sekä torjumiseksi käytettävistä salaisista tiedonhankintakeinoista säädetään poliisilaissa (PolL 5 luku). Kun rikosta selvitetään ja on aloitettu esitutkinta, salaisista pakkokeinoista säädetään pakkokeinolaissa (PKL 10 luku). Se kumpaa lainsäädäntöä sovelletaan, riippuu siitä missä vaiheessa tiedonhankinta on (Kuvio 1).



Kuvio 1

Rikoksen estämisellä ja torjumisella tarkoitetaan sitä, että rikosta ei ole vielä tapahtunut ja tiedonhankinnan avulla pyritään estämään rikos, rajoittamaan rikoksesta aiheutuvaa haittaa tai keskeyttämään rikoksen toteuttaminen. Rikoksen valmisteluun voidaan puuttua myös siinä tapauksessa, että itse suunnittelua ei ole kriminalisoitu (PolL 5:1 § 2). Tästä esimerkkinä voisi olla Liedossa tapahtunut pankkiryöstön yritys (MTV 2008). Poliisilla oli käytössään kaikki poliisilain keinot, vaikka törkeän ryöstön valmistelua ei ollut kriminalisoitu vuonna 2007.

Rikosten paljastaminen tarkoittaa taas sitä, että rikoksen epäillään tapahtuneen, mutta esitutkintaa ei voida aloittaa, koska esitutkinnan käynnistämisen edellytykset puuttuvat. Tiedonhankinnan avulla pyritään selvittämään, onko asiassa mahdollista aloittaa esitutkinta (PolL 5:1 § 3). Jos tiedonhankinnan perusteella voidaan riittävän perustellusti epäillä rikoksen tapahtuneen, aloitetaan esitutkinta ja tällöin sovelletaan pakkokeinolakia.

Esitutkinta, eli rikoksen selvittäminen aloitettava, kun esitutkintaviranomaisella on syytä epäillä rikoksen tapahtuneen (Esitutkintalaki 3:3 § 1). ”Syytä epäillä” -termiä ei avata lainsäädännössä juuri lainkaan. Asiaa on kuvattu hallituksen esityksessä esitutkintaa ja pakkokeinoja rikosasioissa koskevaksi lainsäädännöksi niin, että asioita huolellisesti harkitseva ihminen päätyy tällaiseen tulokseen (HE 14/1985, 16). Esitutkintakynnyksen ylittämiseen

tarvitaan yleensä jotain konkreettista näyttöä, eikä esimerkiksi pelkkä vihjetieto rikoksesta riitä aloittamaan esitutkintaa.

Yhteistä näissä tapauksissa on, että tiedonhankinnan perusteena on epäilys tietystä rikoksesta ja lopullisena tavoitteena on selvittää, kuka on rikoksen tekijä ja muut rikokseen liittyvät seikat. Lopullisena päämääränä on saattaa joku luonnollinen henkilö rikosvastuuseen. Sovellettava tiedonhankintakeino kohdistuu yleensä tiettyyn henkilöön tai yksilöityyn kohteeseen, joka voi olla myös verkko-osoite tai tietty laite.

2.2 Poliisitoiminnan yleiset periaatteet

Kun poliisi käyttää toimivaltuuksiaan hänen on noudatettava niin sanottuja poliisioikeudellisia periaatteita, eli on kunnioitettava perusoikeuksia ja ihmisoikeuksia. Vaihtoetoja punnittaessa on valittava perustellusti ne toimivaltuudet, jotka parhaiten edistävät näiden oikeuksien toteutumista. (PolL 1:2 §.)

Suhteellisuusperiaate (PolL1:3 §) tarkoittaa sitä, että toimivaltuuksista käytetään sitä keinoa, joka on kaikkein järkevin tavoiteltuun päämäärään nähden. Tämän lisäksi poliisilla on mahdollisuus luopua tai siirtää toimenpide, jos toimenpiteestä aiheutuu tulokseen verrattuna kohtuuttomia seurauksia (PolL 1:9 §).

Vähimmän haitan periaatteella (PolL1:4 §) tarkoitetaan sitä, että poliisi ei saa puuttua kenenkään oikeuksiin enemmän kuin on välttämätöntä tehtävän suorittamiseksi. Keinoista tulee käyttää sitä, josta aiheutuu vähiten haittaa toimenpiteen kohteelle. Käytettävä keino tai toimenpide valitaan aina tilanteen mukaan. Esimerkkinä tästä voisi olla voimankäyttötilanteet ja poliisilla käytössään olevat eritasoiset voimankäyttövälineet.

Tarkoitussidonnaisuuden periaate (PoL1:5 §) tarkoittaa sitä, että toimivaltuutta saa käyttää vain siihen tarkoitukseen kuin lainsäätäjä on sen kohdistanut. Tämä koskee myös tilannetta, jossa voitaisiin käyttää jotain pakkokeinoa, mutta jo etukäteen tiedetään, että kyseisellä pakkokeinolla ei saavuteta mitään.

2.3 Rikosten estäminen, paljastaminen ja torjuminen

Salaisesta tiedonhankinnasta ennen esitutkintaa säädetään PolL 5 luvussa. Tässä kappaleessa käsitellään vain niitä salaisia tiedonhankintakeinoja, jotka kohdistuvat tietoverkkoihin tai niitä voidaan muuten verrata vastaaviin tiedustelukeinoihin, niin kuin siviilitiedustelulaissa on säädetty.

Telekuuntelua, eli myös viestin sisällön kuuntelua tai sisällön muuta käsittelyä, voidaan suorittaa PolL 5:5 §:n mukaan valtion turvallisuuteen ja terrorismiin liittyvissä rikoksissa. Lupa voidaan antaa myös siinä tapauksessa, jos se on välttämätöntä henkeä ja terveyttä uhkaavan vakavan vaaran torjumiseksi. Telekuuntelua voidaan käyttää tiedonhankintakeinona, kun henkilön voidaan epäillä syyllistyvän:

1) Suomen itsemääräämisoikeuden vaarantamiseen
2) sotaan yllyttämiseen
3) maanpetokseen, törkeään maanpetokseen
4) vakoiluun, törkeään vakoiluun
5) turvallisuussalaisuuden paljastamiseen
6) luvattomaan tiedustelutoimintaan
7) rikoslain 34 a luvun 1 §:n 1 momentin 2–8 kohdassa tai 2 momentissa tarkoitettuun terroristisessa tarkoituksessa tehtyyn rikokseen
8) terroristisessa tarkoitukseen tehtyyn radiologista asetta koskevaan rikokseen
9) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun
10) terroristiryhmän johtamiseen
11) terroristiryhmän toiminnan edistämiseen
12) koulutuksen antamiseen terrorismirikoksen tekemistä varten
13) kouluttautumiseen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta
14) värväykseen terrorismirikoksen tekemiseen
15) terrorismin rahoittamiseen
16) terroristiryhmän rahoittamiseen, jos teon vakavuus edellyttäisi vankeusrangaistusta, tai
17) matkustamiseen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta.

Tietojen hankkimista telekuuntelun sijasta käsitellään PolL 5:6 §:ssä. Lainkohta koskee tilannetta, jossa viestiä tai siihen liittyviä tunnistamistietoja ei ole enää saatavissa. Jos PolL 5:5 § edellytykset telekuuntelulle on olemassa, niin poliisi voi hankkia tietoja teleyrityksen tai yhteisötilaajan hallusta.

Televalvonnan, eli vain viestin tunnistamistietojen hankkimisen edellytyksiä käsitellään PolL 5:8 §:ssä. Tunnistamistiedolla tarkoitetaan esimerkiksi viestinnän osapuolten ja viestinnän ajankohdan tallentamista. Televalvonnassa sisältöä ei avata. Televalvontaa saadaan käyttää, kun voidaan epäillä jonkun syyllistyvän:

1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta
2) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn rikokseen, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta
3) teleosoitetta tai telepäätelaitetta käyttäen tehtyyn, automaattiseen tietojenkäsittelyjärjestelmään kohdistuvaan luvattomaan käyttöön
4) seksikaupan kohteena olevan henkilön hyväksikäyttöön, lapsen houkuttelemiseen seksuaalisiin tarkoituksiin tai paritukseen
5) huumausainerikokseen
6) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun, kouluttautumiseen terrorismirikoksen tekemistä varten, terroristiryhmän rahoittamiseen, matkustamiseen terrorismirikoksen tekemistä varten tai terrorismirikoksen tekemistä varten tapahtuvan matkustamisen edistämiseen, taikka
7) törkeään tulliselvitysrikokseen.

Tämän lisäksi poliisilla on oikeus televalvontaan, jos se on välttämätöntä henkeä ja terveyttä uhkaavan rikoksen estämiseksi.

Teknistä kuuntelua käsitellään PolL 5:17 §:ssä. Teknisen kuuntelun avulla kohteen keskustelua kuunnellaan tai hänen viestinsä avataan tai muuten käsitellään teknisellä laitteella tai ohjelmistolla. Hallituksen esityksen mukaan teknisellä kuuntelulla tarkoitetaan myös näppäimistökuuntelua (HE 202/2017, 24). Teknisen kuuntelun edellytyksenä on, että kohteen voidaan perustellusti epäillä syyllistyvän:

> 1) rikokseen, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta
> 2) huumausainerikokseen
> 3) terroristisessa tarkoituksessa tehtävän rikoksen valmisteluun taikka kouluttautumiseen terrorismirikoksen tekemistä varten, terroristiryhmän rahoittamiseen tai matkustamiseen terrorismirikoksen tekemistä varten, jos teon vakavuus edellyttäisi vankeusrangaistusta, taikka
> 4) törkeään tulliselvitysrikokseen.

Tekniseen kuunteluun on myös oikeus, jos se on välttämätöntä henkeä tai terveyttä uhkaavan välittömän vaaran torjumiseksi.

Teknistä laitetarkkailua käsitellään PolL 5:23 §:ssä. Tekninen laitetarkkailu on tietokoneen tai teknisen laitteen muuta kuin aistinvaraista tarkkailua. Laitetarkkailu mahdollistaa tietojen tallentamisen tai muun käsittelyn. Teknisellä laitetarkkailulla voidaan saada tietoon esimerkiksi tietokoneelle tallennetun asiakirjan sisältö. Laitetarkkailulla ei kuitenkaan saa hankkia tietoa viestin sisällöstä tai tunnistetiedoista, eli laitetarkkailu eroaa tältä osin teknisestä kuuntelusta. Teknisellä laitetarkkailulla voidaan kuitenkin seurata henkilön ja laitteen välistä viestintää (HE 202/2017, 26). Laitetarkkailun edellytykset ovat samat kuin teknisessä kuuntelussa.

2.4 Rikosten selvittäminen

Esitutkinnassa käytettäviä salaisia pakkokeinoja käsitellään pakokeinolaissa. Käsittelen tässä niitä salaisia pakkokeinoja, jotka kohdistuvat viestintään tietoverkossa.

Telekuuntelun edellytyksiä käsitellään PKL 10:3 §:ssä. Luvussa on pitkä lista rikoksia, joissa voidaan käyttää telekuuntelua, mutta käytännössä pykälässä luetellaan rikoslain ylitörkeät rikokset tai rikosten törkeät tekomuodot.

Tietojen hankkimista telekuuntelun sijasta käsitellään pakkokeinolain 10:4 § ja se on samansisältöinen kuin vastaava kohta poliisilain 5:6 §:ssä.

Televalvontaa ja sen edellytyksiä käsitellään PKL 10:6 §:ssä. Televalvonta kohdistetaan rikoksesta epäillyn lähettämään tai hänelle lähetettyyn viestiin. Laissa on luettelo rikoksista, joiden perusteella televalvontaa voidaan tehdä:

1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta
2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta
3) teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä
4) seksikaupan kohteena olevan henkilön hyväksikäytöstä, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tai parituksesta
5) huumausainerikoksesta
6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta, kouluttautumisesta terrorismirikoksen tekemistä varten, terroristiryhmän rahoittamisesta tai matkustamisesta terrorismirikoksen tekemistä varten
7) törkeästä tulliselvitysrikoksesta
8) törkeästä laittoman saaliin kätkemisestä
9) panttivangin ottamisen valmistelusta
10) törkeän ryöstön valmistelusta.

Tekninen kuuntelu pakkokeinolain perusteella on samansisältöinen poliisilain kanssa, mutta edellytyksiin on lisätty kaksi rikoksen valmisteluun liittyvää rikosta: panttivangin ottamisen valmistelu ja törkeän ryöstön valmistelu. (PKL 10:16 §)

Teknistä laitetarkkailua käsittelevä kohta on samansisältöinen poliisilain kanssa. Edellytykset tekniselle laitetarkkailulle on samat kuin tekniselle kuuntelulle. (PKL 10:23 §)

2.5 Salaisesta tiedonhankintakeinosta ja pakkokeinosta päättäminen

Salaisiin tiedonhankintakeinoihin ja salaisiin pakkokeinoihin haetaan lupa tuomioistuimesta. Vaatimuksen salaisiin tiedonhankintakeinoihin poliisilain perusteella tekee pidättämiseen oikeutettu poliisimies tai suojelupoliisin päällystöön kuuluva poliisimies. Esitutkinnan käynnistyttyä vaatimuksen salaisesta pakkokeinosta voi tehdä vain pidättämiseen oikeutettu virkamies. Aikaisemmin suojelupoliisi suoritti myös esitutkintaa, mutta tiedustelulainsäädännön myötä esitutkintaoikeus poistettiin suojelupoliisilta. Suojelupoliisin päällystöä ei ole enää mainittu pidättämiseen oikeutetuissa poliisimiehissä, joten suojelupoliisi ei voi käyttää salaisia pakkokeinoja rikoksen selvittämiseksi (ETL 2:2 § 1; PKL 2:9 §).

Lupaa haettaessa hakemuksessa pitää mainita rikos ja perusteet, sille miksi rikosta on syytä epäillä. Tämän perusteella tuomioistuin tekee päätöksen, voiko viranomainen aloittaa vaatimuksen mukaisen tiedonhankinnan. Hakemuksesta tulee ilmetä myös valvonnan kohde ja luvan voimassaoloaika.

2.6 Salaisesta tiedonhankintakeinosta ja pakkokeinosta ilmoittaminen

Tiedonhankinnasta on ilmoitettava kirjallisesti viipymättä sen kohteelle, kun tiedonhankintakeinon tarkoitus on saavutettu tai viimeistään vuoden kuluttua sen käytön lopettamisesta. Ilmoitusta voidaan lykätä poliisin vaatimuksesta tuomioistuimen päätöksellä enintään kaksi vuotta kerrallaan. Tuomioistuin voi myös tehdä päätöksen, että tiedonhankinnasta ei ilmoiteta kohteelle, jos valtion turvallisuus on uhattuna tai jos ilmoittamisen seurauksena jonkun henki tai terveys vaarantuu. (PolL 5:58 §; PKL 10:60 §.)

2.7 Laillisuusvalvonta

Poliisilain ja pakkokeinolain mukaan laillisuusvalvonta toteutetaan poliisin sisäisenä valvontana. Vastuu on Poliisihallituksella ja yksikön päälliköillä. Suojelupoliisin sisäisestä laillisuusvalvonnasta vastaa sisäministeriö. Sisäministeriö raportoi vuosittain salaisten tiedonhankintakeinojen käytöstä ja niiden valvonnasta eduskunnan oikeusasiamiehelle. (PolL 5:63 §; PKL10:65 §.)

Valtionneuvoston asetuksessa 122/2014 säädetään myös salaisten tiedonhankinta- ja pakkokeinojen seurannasta. Asetuksen 3 luvun 21 §:ssä säädetään valvontaelimestä, joka seuraa tiedonhankintakeinojen käyttöä ja raportoi siitä. Suojelupoliisissa on myös vastuuhenkilöjärjestelmä, jonka tehtävänä on tarkastaa tehdyt kirjaukset ja niiden lainmukaisuuden reaaliaikaisesti (HE 199/2017, 11).

Suojelupoliisia koskevan yleisen laillisuusvalvonnan suorittaa sisäministeriön poliisiosasto kaksi kertaa vuodessa. Vuoden alussa tehtävä laillisuustarkastuksen aiheena ovat tiedonhankintakeinot ja näiden menetelmien valvonta. Poliisiosasto tekee tarkastuksen tuloksista tarkastuskertomuksen. Tarkastuskertomuksessa voi olla salassa pidettäviä osia, mutta asiakirja on lähtökohtaisesti julkinen. (Sisäministeriö 2016, 16–17.)

3 Miksi poliisilaki ja pakkokeinolaki eivät riitä tiedonhankinnan keinoina?

3.1 Rikoksen tunnusmerkistö

Kun viranomainen hakee lupaa tiedonhankintaan poliisilain tai pakkokeinolain perusteella, pitää pakkokeinovaatimuksessa olla joku laissa erikseen mainittu rikos, jonka epäillään tapahtuvan tai tapahtuneen. Siviilitiedustelulainsäädännössä tiedonhankinta on tiedustelua, jonka tavoitteena on kansallisen turvallisuuden ylläpitäminen (PolL 5a:1 §). Uhka voi olla sellainen, että teko toteutuessaan täyttää rikoksen tunnusmerkistön, mutta tiedonhankinnan alkuvaiheessa niin epämääräinen, että rikostorjunnassa ja -tutkinnassa käytettävät toimivaltuudet eivät ole käytettävissä.

3.2 Tiedonhankinnan kohde

Poliisilaissa ja pakkokeinolaissa pakkokeino kohdistuu aina tiettyyn kohteeseen. Ylensä kohde on luonnollinen henkilö, mutta se voi olla myös tuntemattoman henkilön hallussa oleva päätelaite. Aikaisemmin viranomaisella ei ole ollut mahdollisuutta hankkia tietoja ilmiöön tai uhkaan perustuvasta tietoliikenteestä, jossa uhkan aiheuttavan päätelaitteen tarkat tiedot ovat tuntemattomat.

3.3 Maantieteellinen ulottuvuus

Tiedustelulainsäädäntö on säädetty kansallista turvallisuutta uhkaavan vaaran torjumiseen. Erilaiset uhkat eivät ole enää sidottu maantieteellisesti. Rikostorjuntaan ja esitutkintaan liittyvät pakkokeinot toimivat parhaiten, kun kyseessä on tunnistettu Suomessa oleva kohde. Ulkomailla olevan kohteen tunnistaminen ja siihen kohdistettava tiedonhankinta voi olla vaativaa tai mahdotonta. Vaikka ulkomailla oleva viestinnän vastapuoli olisi tunnistettu, mutta kotimainen osapuoli on tuntematon poliisille, niin tiedonhankintaa ei voi toteuttaa Suomessa poliisilain tai pakkokeinolain perusteella. Tällöin voidaan pyytää toisen maan viranomaista toimittamaan tarvittavat tiedot oikeusapumenettelyllä (Oikeusministeriö). Jos epäily kohdistuu valtiolliseen toimijaan, niin tietojen saaminen ei ole mahdollista oikeusapupyynnön avulla.

3.4 Verkkorikollisuus

Digitalisaation myötä yhteiskunnan perustoiminnot perustuvat toimivaan tietoverkkoon. Yksittäisen henkilön tekemä vihamielinen hyökkäys tietoverkkoon voi aiheuttaa vakavaa vahinkoa, jopa valtiollisella tasolla. Tämänkaltaisen uhkan havaitsemiseksi tulee myös

verkon liikennettä pystyä havainnoimaan ja mahdolliseen vihamieliseen toimintaan pitää pystyä reagoimaan nopeasti, jotta se voitaisiin estää.

Esimerkkinä pitkään jatkuneesta Suomen valtiota kohtaan suunnatusta verkkovakoilusta oli ulkoministeriöön kohdistunut tietomurto, joka paljastui talvella 2013. Tietoa vakoilusta ei saatu selville oman viranomaistoiminnan ansiosta, vaan tieto saatiin ulkopuoliselta lähteeltä. Tiedon luovutti Ruotsin signaalitiedustelulaitos Försvarets radioanstalt. Tehtyjen selvitysten mukaan vakoilu oli jatkunut jo vuosia ennen sen ilmi tulemista. Asiaa tutkittaessa paljastui, että sama haittaohjelmaa käytettiin myös muihin maihin kohdistuvaan vakoiluun. (Helsingin sanomat 2014.)

Suomalaisilla viranomaisilla täytyy olla kyky tarkkailla erilaisia uhka-arvioon perustuvia ilmiöitä omassa tietoverkossaan. Esimerkin tapauksessa olisi ollut myös mahdollista, että vakoilusta tiedon saanut ulkomaalainen tiedustelupalvelu ei olisi ilmoittanut havainnostaan Suomelle ja olisi itsekin käyttänyt tietoturva-aukkoa hyväkseen.

4 Tiedustelulainsäädäntö

4.1 Vertailu muihin maihin

Tiedustelulainsäädännön valmisteluvaiheessa on tehty kansainvälinen vertailu siitä, miten tiedustelulainsäädäntö on toteutettu muualla. Vertailumaina on käytetty Ruotsia, Norjaa, Tanskaa, Alankomaita ja Saksaa.

4.1.1 Ruotsi

Ruotsissa verkkoon kohdistuvasta tiedustelusta vastaa puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA). FRA on siviiliviranomainen, joka toimii suoraan puolustusministeriön alaisuudessa, joten se ei puolustusvoimien joukko-osasto. (Puolustusministeriö 2015, 38)

Ruotsin signaalitiedustelusta annetussa laissa (Lag om signalspaning i försvarsunderrättelseverksamhet) tietoliikennetiedustelu on määritelty teknologianeutraaliksi ja sen tulee kohdistua Ruotsin rajan ylittävään tietoliikenteeseen. Jos viestinnän molemmat osapuolet ovat Ruotsissa, ei tietoja saa kerätä. Tiedustelun kohteet on määritelty lakiin yksityiskohtaisesti. Ruotsin signaalitiedustelusta annetun lain 1 §:n perusteella tietoliikennetiedustelun kohteina voi olla:

1) Ruotsiin kohdistuva sotilaallinen uhka
2) Ruotsin intressit kansainvälisissä operaatioissa
3) Kansainvälinen terrorismi ja järjestäytynyt rikollisuus
4) Joukkotuhoaseet, sotatarvikkeet ja kaksikäyttötuotteiden kehittäminen ja levittäminen
5) Ulkoiset yhteiskunnan infrastruktuuriin kohdistuvat uhat
6) Kansainväliseen turvallisuuteen vaikuttavat konfliktit ulkomailla
7) Ulkomainen Ruotsiin kohdistuva tiedustelutoiminta
8) Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan kannalta merkitsevä vieraan vallan toiminta

Ruotsissa tietoliikennetiedustelun voi aloittaa vain toimeksiannosta, jonka voi antaa valtioneuvosto, valtioneuvoston kanslia, puolustusvoimat, keskusrikospoliisi tai suojelupoliisi. Toimeksianto ei voi kohdistua pelkästään tiettyyn henkilöön. Luvan myöntää aina puolustustiedustelutuomioistuin. Lupahakemuksessa tulee olla kuvaus toimeksiannosta, mihin verkon osaan tiedustelua kohdistetaan, käytettävät hakuehdot ja luvan kesto. Hakuehtona ei pääsääntöisesti saa käyttää henkilöön viittaavaa hakuehtoa. Henkilöön kohdistuvaa hakuehtoa saa käyttää, jos se on erityisen tärkeä tiedonhankinnan onnistumiselle. Tiedonhankinnan kohteelle tulee ilmoittaa viimeistään kuukausi tiedustelutehtävän lopettamisesta, jos siinä ei ole muista salassapitomääräyksistä johtuvia poikkeuksia. (Puolustusministeriö 2015, 39.)

FRA:n tietosuojaneuvosto valvoo yksikön toimintaa sisäisesti ja sen vastuulla on valvoa yksityisyyden suojaa. Tarvittaessa tietosuojaneuvosto raportoi valtion tiedustelutarkastukselle, joka valvoo erityisesti käytettyjä hakuehtoja, tietojen hävittämistä ja raportointikäytäntöjä. Muita valvontaviranomaisia Ruotsissa ovat tietosuojavaltuutettu, eduskunnan oikeusasiamies ja oikeuskansleri. (Puolustusministeriö 2015, 39.)

Ruotsin lainsäädännössä ei ole säädetty parlamentaarista valvontaa. Laillisuusvalvonnasta vastaa valtion tiedustelutarkastus. Jos se havaitsee toiminnassa rikoksia se ilmoittaa siitä valtakunnansyyttäjälle tai muulle toimivaltaiselle viranomaiselle. Tiedustelutarkastus valvoo myös käytettyjä hakuehtojen käyttöä, tietojen luovuttamista, hävittämistä ja raportointia. Tiedustelutarkastus voi myös tehdä yksityishenkilön pyynnöstä tarkastuksen siitä, onko häneen kohdistettu valvontaa ja onko se ollut laillista. (HE 199/2017, 13–14.)

4.1.2 Norja

Norjassa tiedustelupalvelusta vastaa Norjan tiedustelupalvelu (Etterretningstjenesten, NIS), joka kuuluu Norjan puolustusvoimiin. Sisäisestä turvallisuudesta vastaa turvallisuuspoliisi, joka tekee yhteistyötä tiedustelupalvelun kanssa. (HE 202/2017, 39.)

Norjan lainsäädännössä ei ole säädetty erikseen käytettävistä tiedonhankintamenetelmistä. Tiedonhankintaa on rajoitettu niin, että Norjan alueella ei saa kohdistaa valvontaa tai tiedonkeruuta norjalaisista henkilöistä tai juridisista henkilöistä. Poikkeuksena tästä on mahdollisuus kohdistaa tiedonhankinta henkilöön, joka on osallisena laittomaan tiedusteluun toisen valtion puolesta. Tiedustelutoimintaa käsittelevässä laissa on luettelo niistä kansallisista intresseistä, joiden perusteella tietoa voidaan kerätä. Luettelo on kuitenkin esimerkinomainen eikä se ole tyhjentävä luettelo. Puolustusvoimien päällikkö antaa tiedustelutehtävät puolustusministeriön määräyksestä. (HE 202/2017, 39.)

Norjassa on käynnissä lainsäädäntöuudistus tietoliikennetiedustelusta. Norjassa on nähty, että yhtenä perusteena lainsäädännön saamiselle tietoliikennetiedusteluun on turvata ihmisoikeudet. Täsmällisellä lainsäädännöllä voidaan määritellä tietoliikennetiedustelun käyttöperusteet ja niiden käsittely niin, että oikeusturva toteutuu. Tietoliikennetiedustelun vastuuviranomaiseksi määrättäisiin Etterretningstjenesten ja tiedustelun kohteina olisi kyberuhat, terrorismi ja vakoilu. Hallitus esittäisi vuosittain tiedustelun kohdealueet ja ne eivät olisi julkista tietoa. Lakiesityksen mukaan hakuehdot voisi kohdistaa myös rajat ylittävän tietoliikenteen viestin sisältöön, mutta niistä pitäisi olla tuomioistuimen päätös. Tietoliikennetiedustelulla saatua tietoa ei saisi missään tilanteessa käyttää näyttönä oikeudenkäynneissä. (HE 202/2017, 41–43.)

Tiedustelupalvelun valvonnasta vastaa Norjan suurkäräjien tiedustelu-, valvonta-, ja turvallisuuspalveluiden valvontavaliokunta, joka vastaa parlamentaarisesta- ja laillisuusvalvonnasta. Valiokunta toimii itsenäisesti ja pyrkii ehkäisemään ja paljastamaan väärinkäytöksiä sekä suorittaa laillisuusvalvontaa. Valiokunta raportoi vuosittain suurkäräjille toiminnastaan. (HE 202/2017, 41.)

4.1.3 Tanska

Tanskan ulkomaan ja sotilastiedustelusta vastaa puolustusvoimien tiedustelupalvelu (Forsvarets Efterretningstjeneste, FE). Tiedustelupalvelu on siviiliviranomainen ja toimii puolustusministeriön alaisuudessa. Tämän lisäksi Tanskassa toimii poliisin turvallisuuspalvelu (Politiets Efterretningstjeneste, PET). (Puolustusministeriö 2015, 41–42.)

Toimivaltasääntely on yleisluonteista ja lainsäädännössä ei ole säädetty tiedonhankintakeinoja. Tietoa saa kerätä, jos sillä on merkitystä tiedustelutoiminnalle. Lupamenettelyyn ei ole lainsäädäntöä. Jos tiedonhankinnassa joudutaan avaamaan Tanskan kansalaisen viestin sisältö, siihen on saatava lupa tuomioistuimesta. (HE 202/2017, 43–44.)

Tiedustelutoimintaa valvoo Tanskan puolustusministeriö, valvontakomitea ja kansankäräjien tiedustelupalveluvaliokunta. Valvontakomitean tehtävänä on turvallisuuspalvelujen laillisuusvalvonta. Laillisuusvalvonta kohdistuu henkilötietojen käsittelyn ja rekisterinpidon lainmukaisuuteen. (Puolustusministeriö 2015, 42)

4.1.4 Alankomaat

Alankomaissa tiedustelua toteuttaa sisäasiainministeriön yleinen tiedustelu- ja turvallisuuspalvelu (Algemene Inlichtingen- en Veiligheidsdienst, AIVD) ja puolustusministeriön sotilastiedustelu- ja tuvallisuuspalvelu (Militaire inlichtingen en veiligheid, MIVD). Molemmat tiedustelupalvelut vastaavat kansallisesta turvallisuudesta. (Puolustusministeriö 2015, 42–43.)

Alankomaissa on säädetty laki tiedustelu- ja turvallisuuspalveluista. Tiedustelupalveluilla on yhteistyövelvollisuus ja niillä on yhteinen koordinaattori, joka vastaa toiminnan yhteensovittamisesta. Luvan signaalitiedusteluun myöntää sisäministeri tai puolustusministeri. Signaalitiedustelua saa käyttää vain, jos demokraattinen oikeusjärjestys tai valtion turvallisuus on uhattuna sekä vieraaseen valtioon kohdistuvaan vastatiedusteluun. Signaalitiedustelussa on käytössä välttämättömyyden periaate, eli sitä saa käyttää vain siinä tapauksessa, kun muita keinoja ei ole käytettävissä. (HE 203/2017, 78–80.)

Tiedustelupalvelut laativat vuosittain toimintarapotin parlamentille, jossa käydään läpi kohteet, joihin on kohdistettu tiedonhankintaa. Laillisuusvalvontaa varten on perustettu riippumaton arviointikomitea. Komitean tehtävänä on käsitellä tiedustelupalvelujen toiminnasta tehtyjä kanteluita ja raportoi tuloksista vastuuministerille. Kantelija voi tarvittaessa tehdä valituksen oikeusasiamiehelle. Tiedustelu- ja turvallisuusvaliokunta vastaa parlamentaarisesta valvonnasta ja se raportoi suoraan parlamentille. (HE 203/2017, 80.)

4.1.5 Saksa

Saksassa tiedustelupalvelut on jaettu kolmelle viranomaiselle. Ulkomaita koskevista tiedoista siviili- ja sotilastiedustelussa vastaa yleinen ulkomaan tiedustelupalvelu (Bundesnachrichtendienst, BND). BND kerää sellaisia tietoja, jotka koskevat ulko- ja turvallisuuspolitiikkaa. Tämän lisäksi Saksassa toimii sotilaallinen turvallisuuspalvelu (Militärischer Abschirmdienst, MAD) ja yleinen turvallisuuspalvelu (Bundesamt für Verfassungsschutz, BfV) ja ne vastaavat toimialojensa vastatiedustelusta kotimaassa. (Puolustusministeriö 2015, 44)

BND vastaa Saksan tietoliikennetiedustelusta ja luvasta päättää liittokanslerinvirasto ja parlamentaarinen valvontavaliokunta (HE 202/2017, 47). Tietoliikennetiedustelussa hakuehtoja voidaan kohdistaa viestin tunnistamistietoihin tai sen sisältöön. Hakuehtona ei saa käyttää yksilöityä teleosoitetta. Automaattisina hakuehtoina voidaan käyttää vain sellaisia, jotka liittyvät Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (G10-laki) 5§:ssä mainittuihin uhkiin:

1) Saksaan kohdistuva aseellinen hyökkäys
2) Saksaan kohdistuva terrori-isku
3) Sotatarvikkeiden kansainvälinen levittäminen, huomattava aseiden, tietojenkäsittelyohjelmien ja teknologian laiton ulkomaankauppa
4) Järjestäytyneen rikollisryhmän tekemä huomattava kansainvälinen huumekauppa, jolla on merkitystä Saksalle
5) Ulkomailta tapahtuva euron arvon horjuttaminen
6) Huomattava kansainvälisesti organisoitu rahanpesu
7) Järjestäytyneen rikollisryhmän organisoima laiton maahantulo EU:n alueelle
8) Huomattava kansainvälisesti organosoitu tietoturvauhka, jolla on merkitystä Saksalle

Saksassa tietoliikennetiedustelua on rajoitettu niin, että sitä saa kohdistaa enimmillään 20 prosenttiin kaikesta rajat ylittävästä tietoliikenteestä (Puolustusministeriö 2015, 45). Parlamentaarinen valvontalautakunta ja G10-komissio vastaavat tiedustelutoiminnan valvonnasta. Myös tietosuojavaltuutettu ja BND:tä valvova liittokanslerin virasto vastaavat osaltaan laillisuusvalvonnasta. G10-komission vastuulla on viestintäsalaisuuden rajoittamiseen liittyvä laillisuusvalvonta. G10 komissio käsittelee kanteluita tai tekee tarkastuksia oma-aloitteisesti. (Puolustusministeriö 2015, 45.)

4.2 Suomen perustuslain muutos

Keskustelu tiedustelulainsäädännön nopeutetusta käsittelystä ja sen vaikeudesta liittyi oleellisesti lakipakettiin kuuluvan perustuslain muutokseen. Perustuslain säätäminen kiireellisenä vaatii 5/6 enemmistön eduskunnassa (PL 73 §). Pelkästään tämän lakimuutoksen estäminen olisi kaatanut koko tiedustelulakipaketin. PL10 § käsittelee yksityiselämän suojaa. Perustuslain 10§ 3. momentissa määritellään poikkeustapaukset tähän pykälään. Aikaisempi lainsäädäntö mahdollistaa yksityisyyden suojan rajoittamisen kansallisen turvallisuuden perusteella vain, jos siihen liittyy konkreettinen rikosepäily. Jotta tiedustelulakipaketti voitiin ottaa käyttöön, niin perustuslakiakin oli muutettava tältä osin. Lakia muutettiin niin, että 10 §:än lisättiin 4. momentti.

> Lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten torjunnassa, oikeudenkäynnissä, turvallisuustarkastuksessa ja vapaudenmenetyksen aikana sekä tiedon hankkimiseksi sotilaallisesta toiminnasta taikka sellaisesta muusta toiminnasta, joka vakavasti uhkaa kansallista turvallisuutta. (PL 10 § 4.)

Kun tiedonhankinnan kohteena on valtio tai muu julkisyhteisö, niin ne jäävät perusoikeussuojan ulkopuolelle. Tällöin kuitenkin pitäisi pystyä seuraamaan sellaista liikennettä, jossa on pelkästään valtioiden tai julkisyhteisöjen välistä liikennettä, eikä siihen ole sekoittunut yksityishenkilöiden liikennettä. (HE 202/2017, 240)

4.3 Suojelupoliisin rooli

Siviilitiedustelun päämääränä on hankkia tietoa toiminnasta, joka uhkaa kansallista turvallisuutta. Tietoa hankitaan myös tukemaan ylimmän valtiojohdon päätöksentekoa ja muille viranomaisille, kun tiedonhankinnan kohde liittyy kansallisen turvallisuuteen. (PolL 5a:1 §.)

Siviilitiedustelulainsäädäntöä laadittaessa korostettiin, että suojelupoliisi on ainoa viranomainen, joka saa suorittaa siviilitiedustelua. Tämän lisäksi tärkeä elementti koko tiedustelulakipaketissa oli suojelupoliisin rooli esitutkintaviranomaisena. Lain esivalmistelussa esitettiin, että uudet tiedonhankintamenetelmät eivät voi olla samalla esitutkintoihin liittyvää tiedonhankintaa. Jos suojelupoliisin tiedustelullisia toimivaltuuksia lisätään, oikeudenmukaisen oikeudenkäynnin varmistamiseksi tulee esitutkintaan liittyviä valtuuksia rajoittaa (Sisäministeriö 2017, 126). Tiedustelulakipaketin käsittelyn yhteydessä esitutkintalakia muutettiin niin, että suojelupoliisi poistettiin esitutkintaa tekevistä viranomaisista (ETL 2:2 § 1). Samalla pakkokeinolaista poistettiin suojelupoliisin virkamiehet pidättämiseen oikeutetuista virkamiehistä (PKL 2:9 §).

4.4 Siviilitiedustelu

Poliisilakiin lisättiin 5a luku, joka käsittelee siviilitiedustelua. Lain 1 §:ssä suojelupoliisi määritellään ainoaksi viranomaiseksi, joka voi soveltaa kyseistä poliisilain lukua. Ne tiedustelumenetelmät, joita suojelupoliisi voi käyttää luetellaan 2 §:ssä. Menetelmät ovat samat kuin poliisilain 5 luvussa ja näiden lisäksi siviilitiedustelussa voidaan käyttää myös tietoliikennetiedustelua. Liitteessä 1 on kuvattu sitä, miten siviilitiedustelu sijoittuu aikaisempaan lainsäädäntöön nähden (Liite 1).

Siviilitiedustelumenetelmien käytön edellytykset eroavat poliisilain 5 luvun salaisista tiedonhankintakeinoista niin, että suojelupoliisi voi käyttää tiedustelumenetelmiä ilman että kohteena olevaan toimintaan liittyy varsinaista rikosepäilyä. Käytön edellytyksenä on yleisesti sellainen toiminta, joka uhkaa kansallista turvallisuutta (PolL 5a:4 §). Tiedonhankinnan kohteena ei tarvitse olla luonnollinen henkilö ja tiedonhankinnan kohteena voi olla myös ryhmä. (HE 202/2017, 171–172.)

Siviilitiedustelua koskevan lain 3 §:ssä luetellaan siviilitiedustelun kohteet, johon siviilitiedustelua voidaan kohdistaa:

> 1) terrorismi
> 2) ulkomaalainen tiedustelutoiminta
> 3) joukkotuhoaseiden suunnittelu, valmistaminen, levittäminen ja käyttö
> 4) kaksikäyttötuotteiden vientivalvonnasta annetun lain (562/1996) 2 §:ssä tarkoitettujen kaksikäyttötuotteiden suunnittelu, valmistaminen, levittäminen ja käyttö
> 5) kansanvaltaista yhteiskuntajärjestystä uhkaavasta toiminta
> 6) suuren ihmismäärän henkeä tai terveyttä taikka yhteiskunnan elintärkeitä toimintoja uhkaava toiminta
> 7) vieraan valtion toiminta, joka voi aiheuttaa vahinkoa Suomen kansainvälisille suhteille tai taloudellisille tai muille tärkeille eduille
> 8) kansainvälistä rauhaa ja turvallisuutta uhkaava kriisi
> 9) kansainvälisten kriisinhallintaoperaatioiden turvallisuutta uhkaava toiminta
> 10) Suomen kansainvälisen avun antamisen ja muun kansainvälisen toiminnan turvallisuutta uhkaava toiminta
> 11) yhteiskuntajärjestystä uhkaava kansainvälinen järjestäytynyt rikollisuus

4.5 Tietoliikennetiedustelu

Laissa tietoliikennetiedustelusta siviilitiedustelussa määritellään, että tietoliikennetiedustelu on:

> Suomen rajan viestintäverkossa ylittävään tietoliikenteeseen kohdistuvaa, tietoliikenteen automatisoituun erotteluun perustuvaa teknistä tiedonhankintaa sekä hankitun tiedon käsittelyä (TTST 2 §)

Lain tarkoituksena on kohdentaa tiedustelu niin, että sitä käytetään vain sellaisiin kohteisiin, jossa viestinnän toinen osapuoli on Suomen rajojen ulkopuolella. Tiedustelu perustuisi automaattiseen seulontaan verkkoliikenteestä, jolloin tiedustelu ei kohdistuisi tiettyyn teleosoitteeseen tai laitteeseen.

Laki on kirjoitettu niin, että se on teknologianeutraali. Tällä pyritään ottamaan huomioon lain soveltuminen kaikkiin viestintämuotoihin ja myös alati muuttuvaan viestintäteknologiaan (HE 202/2017, 122). Laki mahdollistaa erilaisten haavoittuvuuksien käytön ja ohjelmistojen asentamisen tietoliikennetiedustelussa (PolL 5a:16 §). Tästä on vaarana, että tieturvan heikentämiseen tarkoitettuja ohjelmistoja tai menetelmiä leviää myös yleiseen käyttöön. On epäilyjä, että jotkut haittaohjelmat ovat valtiollisen toimijan tekemiä ja levinneet muidenkin käyttöön. Esimerkiksi Wannacry-viruksesta on levinnyt muunneltu versio ja alkuperäisen viruksen epäillään olleen Pohjois-Korealaista alkuperää (Björksten, 2017).

Uudessa lainsäädännössä tietoturvatuotteita tekeviä yrityksiä ei velvoiteta tekemään takaportteja tai muuten heikentämään ohjelmistoja viranomaisten käyttöä varten. F-Securen Erka Koivunen (2018) on omassa lausunnossaan ollut tyytyväinen tähän asiaan, koska tietoturvatyökalun ei ole itsenäisesti mahdollista tunnistaa onko tietoturvaan kohdistuva hyökkäys laillinen vai ei. Tämän lisäksi, jos lainsäädännössä vaaditaan tekemään tietoturva-aukkoja yrityksen tuotteisiin, se vaikuttaa kyseisen maan yritysten luotettavuuteen ja kilpailukykyyn yleisesti. Jo pelkkä epäilys lainsäädännön vaatimista takaporteista on vaikuttanut kiinalaisen Huawein maineeseen ja luottamukseen maailmalla (Iltasanomat 2019).

Verkkoa valvotaan suodattamalla sitä tietyin hakuehdoin. Hakuehto ei saa viitata viestin sisältöön (TTST 5 §). Sisältöön kohdistuvaa hakuehtoa ei saa myöskään käyttää pilvipalveluun tallennettavan asiakirjan sisältöä. Laki ei siis mahdollista tekemään hakuehtoa, jossa haettaisiin liikennettä, joka sisältäisi hakusanat ”ISIS”, ”bomb” ja ”Helsinki”. Suodatusehdot kohdistuisivat viestin ohjaus- ja välitystietoihin. (HE 202/2017, 124.)

Suodatuksen hakuehtoina voi olla esimerkiksi sähköpostiosoitteet, domain-nimet ja erilaiset käyttäjätunnukset. Hakuehto voidaan myös muodostaa niin, että siinä voi olla IP-osoite, portti ja kuljetuskerroksen tunniste. Ehtoina voi olla viestinnässä käytettävät viestintätavat, IP-osoiteavaruudet tai viestinnän aika- ja paikkaleimat, jotka liittyvät kansallista turvallisuutta uhkaavaan toimintaan. Muita sallittuja hakuehtoja on tietyn salausohjelman tai hakuehdoissa määritellyn aakkosmerkistön käyttö. Kun hakuehtona on pilvipalveluun talletettava tieto, niin hakuehtona voi olla myös palvelun sijaintipaikkaa koskeva tieto (HE 202/2017, 124, 132).

Suomalasta teleosoitetta ei voi käyttää suodatusehtona, koska silloin voidaan käyttää poliisilakiperusteisia salaisia tiedonhankintakeinoja. Tällöin tiedonhankinta voidaan kohdistaa tiettyyn liikenteeseen eikä ulkopuolista liikennettä tule valvonnassa esiin.

Liikenne- ja viestintäministeriön hallinnossa toimii viestintävirasto, jossa toimii Kyberturvallisuuskeskus. Kyberturvallisuuskeskuksen tehtäviin kuuluu myös tietoturvauhkien ja loukkausten havainnointi. Viestintävirasto on voinut tarkkailla verkkoliikennettä jo vuodesta 2014 lähtien. Sähköisen viestinnän palveluista annetun lain 33:272 § antaa oikeuden viestinnän välittäjälle tai lisäarvopalvelun tarjoajalle oikeuden tarkkailla verkkonsa viestejä automaattisesti. Laki mahdollistaa myös viestien sisällön automaattisen analysoinnin. Lain mukaan käsittelijät voivat tarvittaessa avata viestin myös manuaalisesti, jos on ilmeistä, että se sisältää haittaohjelman. Tämä kohta on samantyyppinen kuin TTST 5 §, joka mahdollistaa automaattisen haittaohjelman tunnistamisen viestin sisällöstä ennalta tehtyjen määrittelyjen perusteella. Sisältöön kohdistuvana hakuehtona voi olla myös haitallisen tietokoneohjelman sisältöä kuvaavat merkkijonot.

Sisältöön kohdistuvia hakuehtoja voidaan käyttää vieraan valtion tai vastaavan tahon tietoliikenteeseen (TTST 5 §). Tällöin kaiken valvottavaksi tulevan liikenteen tulee olla valtiollista ja siihen ei saa sekoittua sivullisten liikennettä (HE 202/2017, 124). Valtioon rinnastettava taho on määritelty hallituksen esityksessä niin, että se on toimija, joka käyttää määrätyllä alueella omaa ja pysyvää valtaa (HE 202/2017, 240). Esimerkkinä tästä voisi olla Isiksen perustama kalifaatti Syyrian ja Irakin valtioiden alueella.

4.6 Tietoliikennetiedustelun kohteet

Poliisi- ja pakkokeinolaista poiketen tiedonhankinnan kohteena ei ole rikoksen tekijä tai oletettu tekijä, vaan uhkaava toiminta. Poliisilain 5a:3 §:ssä on lueteltu kohteet, johon siviilitiedustelua voidaan käyttää. Kohteet on lueteltu tämän tutkimuksen 4.4. luvussa. Kohteena on kansallista turvallisuutta uhkaava toiminta ja tiedonhankinnan alkuvaiheessa ei ole tietoa kuka toiminnan takana on. Tiedonhankintaa aloitettaessa ei välttämättä ole tiedossa mitä rikosta epäillään, vaan on saatu tietoa ilmiöstä, joka saattaa uhata kansallista turvallisuutta. Voi olla myös sellaisia uhkia, joiden toteutuessa ei Suomen lainsäädännössä löydy rikosnimikettä. Esimerkkinä tällaisesta voisi olla ulkomaalaisen toimijan tekemä kartoitus Suomen energianjakeluverkon toiminnasta ja mahdollisista haavoittuvuuksista (HE 202/2017, 111).

4.7 Tietoliikennetiedusteluluvan hakeminen

Kun tietoliikennetiedustelulle haetaan lupaa tuomioistuimesta, hakemuksessa täytyy olla määriteltynä perusteluiden lisäksi se, mitä verkon osaa halutaan tarkkailla (TTST 7 §). Lupaa haettaessa tuomioistuimelle pitää antaa selvitys siitä, miksi tietoliikennetiedustelu on ainoa käytettävissä oleva vaihtoehto. Ennen kuin tietoliikennetiedustelulupaa haetaan,

suojelupoliisin pitää käyttää ensisijaisesti poliisilaista saatavia tiedonhankintakeinoja. Jos niitä ei voida käyttää, voidaan hakea lupaa tietoliikennetiedusteluun.

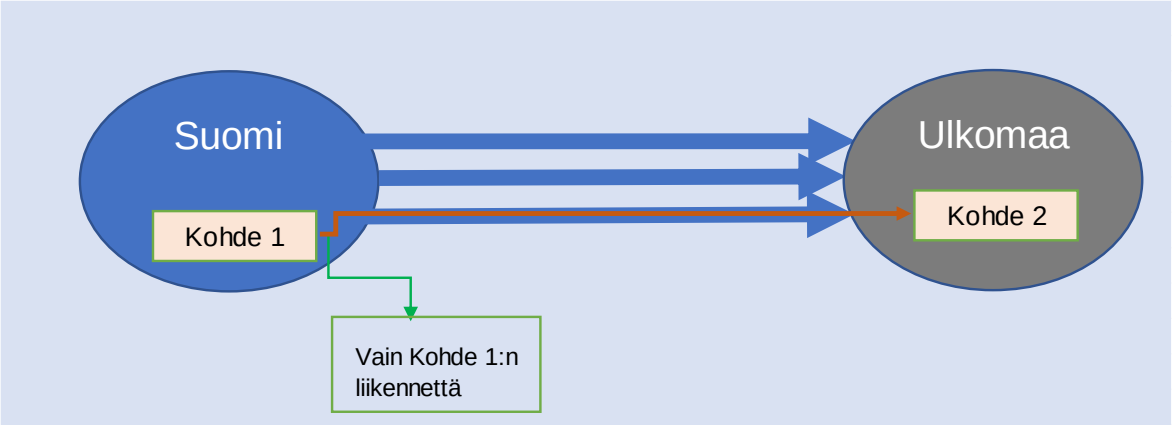
Vaikka tietoliikennetiedustelun käytön perusteissa on tyhjentävä luettelo rikoksista, milloin tietoliikennetiedustelua voidaan käyttää, ne eivät ole itsessään pakkokeinon käyttöön oikeuttavia. Kun pakkokeinoon vaaditaan lupaa tuomioistuimelta, viranomaisen tulee pystyä osoittamaan, että kyseessä on vakava uhka kansalliselle turvallisuudelle. Lupakäsittelyssä tulee myös perustella, miksi tietoliikennetiedustelulupa on välttämätön. Välttämättömyydellä tarkoitetaan sitä, että muilla keinoilla ei ole mahdollista saada tietoja. (HE 202/2017, 158.)

Kaikki tietoliikennetiedustelua koskevat päätökset tehdään Helsingin käräjäoikeudessa. Hallituksen esityksessä (HE 202/2017, 127) tätä on perusteltu sillä, että Helsingin käräjäoikeudella on paras kokemus salaisten tiedonhankinta- ja pakkokeinojen käsittelystä, joten heille on helppo keskittää uuden tehtävän vaatima erityisosaaminen. Helsingin käräjäoikeuden laamanni Tuomas Nurmi (2018) on ollut lausunnossaan sitä mieltä, että käsittelyn keskittäminen on järkevää lupapäätösten vaatiman erityisosaamisen ja takia. Tämän lisäksi Helsingin käräjäoikeus kykenee tarjoamaan helposti tilat, jossa asian turvallinen käsittely on mahdollista. Nurmi (2018) on esittänyt, että tiedusteluun liittyviä lupa-asioita käsitteleville tuomareille on tarjottava riittävästi koulutusta, jotta vaatimus tuomioistuinkontrollista toteutuu lainsäätäjän tarkoittamalla tavalla. FISC ry:n toiminnanjohtaja Juha Remes (2017) on omassa asiantuntijalausunnossaan esittänyt huolensa tuomioistuimien kyvystä arvioida viranomaisten esittämiä pyyntöjä. Kun tuomioistuin tekee päätöksen, niin se edellyttää laintuntemuksen lisäksi osaamista myös teknisistä asioista. Remeksen mukaa tuomioistuimilla pitäisi olla mahdollisuus käyttää ulkopuolisia asiantuntijoita päätöksiensä tukena.

Suojelupoliisi voi antaa TTST 10§ 2:n momentin perusteella toimeksiannon puolustusvoimien tiedustelulaitokselle tietoverkon teknisten tietojen keräämistä ja käsittelyä varten. Toimeksiannon saatuaan puolustusvoimat voi kerätä tietoja sotilastiedustelulain 66 § perusteella. Puolustusvoimat analysoi tietoliikenteestä teknisiä tietoja vain tilastollisesti ja kerätystä materiaalista ei saa olla tunnistettavissa henkilöä. Toimeksiannon tavoitteena on selvittää suojelupoliisille se verkon osa, missä tietoliikennetiedustelun lupapäätöksen perusteluissa tarvittava uhkaava tietoliikenne tapahtuu.

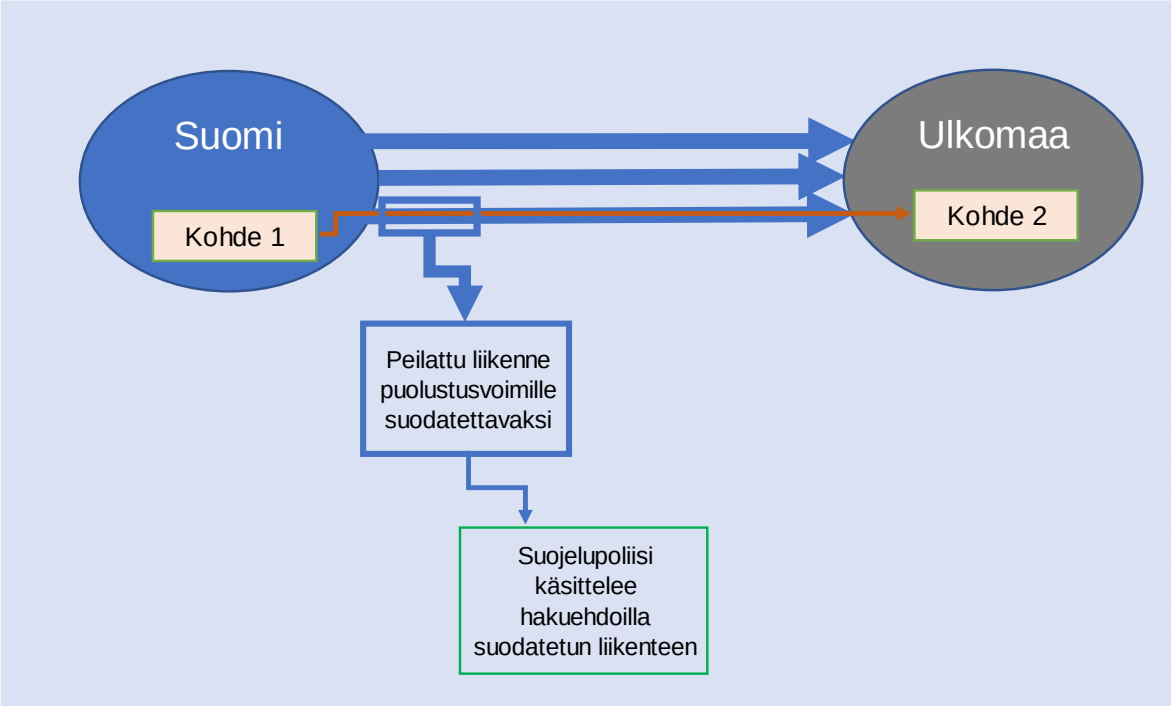
4.8 Tietoliikennetiedustelun toteuttaminen

Tietoliikennetiedustelu poikkeaa poliisilain ja pakkokeinolain perusteella tehdystä tiedonhankinnasta siinä, missä kohtaa viestintäverkkoa tieto otetaan viranomaisen käsittelyyn. Poliisilain ja pakkokeinolain perusteella tiedonhankinta kohdistuu teleosoitteeseen tai päätelaitteeseen, joten tiedonhankinta tapahtuu viestintäverkon reunalla. Tällöin käsittelyyn ei tule muuta liikennettä kuin sen kohteen viestintää, johon tiedonhankinta kohdistuu (Kuvio 2).



Kuvio 2. Poliisilaki ja pakkokeinolaki

Tietoliikennetiedustelussa päätelaitteen tai teleosoitteen yksilöivät tiedot eivät ole saatavissa. Tämän takia tietoliikennetiedustelu tapahtuu keskellä viestintäverkkoa, jossa on myös ulkopuolista liikennettä (Kuvio 3). Hallituksen esityksen mukaan toiminnalla ei pyritäkään siihen, että verkkoliikenteestä seulottaisiin vain tiedonhankinnan kohteena oleva liikenne. Esityksen mukaan riittää, että liikenteestä kyetään mahdollisimman suurella todennäköisyydellä seulomaan kansallista turvallisuutta uhkaava liikennettä, joka on määritelty lupahakemuksessa. (HE 202/2017, 78.)



Kuvio 3. Tietoliikennetiedustelu

Tietoverkkojen dynaaminen rakenne aiheuttaa käytännön ongelmia tietoliikennetiedustelussa. Verkon ohjausliikenne voi muuttua yhden istunnon aikana ja osa valvotusta liikenteestä voi mennä sellaisen verkon osan kautta, joka ei kuulu lupahakemuksen piiriin. Laissa on mainittu, että vain rajat ylittävää liikennettä voi tarkkailla ja toisen osapuolen tulee olla muualla kuin Suomessa. Tämän vuoksi IP-paketeista tulee tunnistaa molempien viestinnän osapuolien maantieteellinen paikka. Suomen sisäinen viestintä voi kulkea jonkun ulkomailla sijaitsevan palvelimen kautta, mutta se on edelleen lain tarkoittamaa Suomen sisäistä liikennettä. Tämä vaatii kaiken valvonnassa saadun verkkoliikenteen läpikäymistä, maan sisäisen liikenteen tunnistamista ja poistamista käsittelyyn jäävästä liikenteestä.

Tietoliikennetiedustelun tekninen toteuttaminen vaatii, että viestintäverkkoon rakennetaan valmiit liitynnät, jonka avulla tietoliikenteen peilaaminen voidaan toteuttaa, kun

tietoliikennetiedusteluun tarvittava lupa on myönnetty. Kytkennän toteuttaja on Suomen Erillisverkot Oy. Hallituksen esityksen mukaan kytkennän toteuttajana tulee olla tiedusteluviranomaisista riippumaton taho. Tällä varmistetaan, että viranomaisella on pääsy vain niihin tietoihin tai verkon osiin joihin tuomioistuimen lupapäätös oikeuttaa. (HE 202/2017,123.)

Kytkennän jälkeen tietoliikenne peilataan puolustusvoimien tiedustelulaitoksen käsiteltäväksi. Vaikka tietoliikennetiedusteluun oikeutettuja viranomaisia on kaksi, hallitus on tullut esityksessään siihen tulokseen, että teknisestä toteuttamisesta vastasisi aina puolustusvoimat (HE 202/2017, 128). Perusteluista tärkein on resurssi- ja kustannusperusteet. Ei ole järkevää, että molemmat toimivaltaiset viranomaiset rakentaisivat omat tekniset ratkaisunsa toteuttamaan samaa asiaa.

Lupapäätöksessä on ennakkoon määritellyt hakuehdot, joihin tietoliikennetiedustelun avulla saatua liikennettä verrataan. Se liikenne, joka vastaa hakuehtoja ohjataan jatkokäsittelyyn reaaliaikaisesti. Muu liikenne jatkaa eteenpäin ilman käsittelyä eikä se ole enää palautettavissa. Automaattisessa tietoliikenteen suodattamisessa ei ole oikeutta avata viestien sisältöä tai tarkastella sitä teknisesti. Suodatettu liikenne siirretään suojelupoliisille jatkokäsittelyyn (HE 202/2017, 123). Suodatetusta liikenteestä suojelupoliisi saa avata yksittäisen viestin sisällön manuaalisesti tai automaattisesti (TTST 6 §).

Tiedonkeruu saattaa lisätä kyberuhkia Suomen tietoverkossa. Tiedustelutiedon keräämiseen tarkoitetut laitteet voivat olla mielenkiintoisia hyökkäyskohteita. Kun tietoverkkoon asennetaan laite tai ohjelmisto pitää varautua, että myös siihen voidaan kohdistaa vihamielinen hyökkäys (Suomen Sadankomitea ry 2017). Myös virheet ohjelmistossa saattavat aiheuttaa tahattomia tietovuotoja tai valvonta saattaa kohdistua sellaiseen liikenteeseen, johon lupaa ei ole myönnetty.

4.9 Tiedon luovuttaminen rikostutkintaan

Poliisilain 5a:44 § on määritelty, milloin siviilitiedustelulla saatu tieto voidaan luovuttaa toimivaltaiselle esitutkintaviranomaiselle. Perusajatuksena on, että vain vakavimpiin rikoksiin liittyviä tietoja voidaan luovuttaa. Poikkeuksena tästä on, jos tiedustelulla saadaan tietoa, joka tukee jonkun rikoksesta epäillyn syyttömyyttä, tieto saadaan silloin luovuttaa rikosta sen tarkemmin määrittelemättä. Tieto voidaan myös luovuttaa huomattavan ympäristö-, omaisuus- tai varallisuusvahingon ehkäisemiseksi. Myös hengelle, terveydelle tai vapaudelle aiheutuvan vaaran estämiseksi tieto voidaan luovuttaa tekoa sen tarkemmin määrittelemättä. Jos luovutettua tietoa käytetään todisteena oikeudessa, niin tuomioistuin päättää sen käyttökelpoisuudesta asian käsittelyn yhteydessä.

Suojelupoliisi voi luovuttaa tietoliikennetiedustelulla saadun tiedon, jos on tapahtunut rikos, josta voidaan tuomita vähintään kolmen vuoden rangaistukseen. Rikoksen estämiseksi tieto voidaan luovuttaa, jos havaitaan rikoshanke, josta voidaan tuomita kaksi vuotta vankeutta. Suojelupoliisi voi harkita itsenäisesti, luovuttaako se tietoliikennetiedustelulla saatua tietoa vai ei. Hallitus on esityksessään (HE 202/2017, 217) korostanut, että jos uhka kohdistuu henkeen tai terveyteen, niin ilmoittamatta jättämiseen pitää olla erittäin painavat syyt.

Suojelupoliisin on ilmoitettava toimivaltaiselle viranomaiselle ilman aiheetonta viivytystä, jos he havaitsevat tiedonhankinnassa sellaisen rikoksen, josta voidaan tuomita vähintään kuuden vuoden vankeuteen. Suojelupoliisin päällikkö voi siirtää ilmoittamista vuoden kerrallaan, jos se on välttämätöntä (PolL 5a:44 § 1). Jos tällainen rikos voidaan estää, siitä pitää ilmoittaa heti (PolL 5a:44 § 2).

4.10 Tietojen luovuttaminen yritykselle ja yhteisöille

Tietoturvan parantaminen nähdään laissa laajempana kuin pelkkänä viranomaistoimintana. Viranomaisella on oikeus luovuttaa tietoliikennetiedustelun yhteydessä saamansa tieto haittaohjelmasta tai muusta tietoturvaloukkauksen tekomuodosta yrityksille ja yhteisöille (TTST 16 §). Tämä mahdollistaa tiedon jakamisen eri alan toimijoiden kesken, riippumatta siitä onko vastaanottava osapuoli viranomainen vai ei. Liikenne- ja viestintäministeriön lausunnon mukaan uusi lainsäädäntö ei saa kuitenkaan täysin korvata nykyistä vapaaehtoisuuteen perustuvaa mallia, jossa verkkojen omistajat ilmoittavat vapaaehtoisesti ilmoittavat havaitsemistaan tietoturvaloukkauksista ja -uhkista (LVM 2017).

Lain yhtenä tavoitteena on myös suojautua kaikkein vakavimpia tietoliikenneverkkoon kohdistuvia uhkia vastaan (HE 202/2017, 109). Tietoliikennetiedustelun avulla voidaan havaita kehittyneempiä tietoliikenneuhkia. F-Securen Erka Koivunen (2018) on ottanut tietojen luovuttamisen esiin lausunnossaan. Hänen mukaansa iso osa edistyneistä tietoturvaloukkauksista toteutetaan kokonaan tai osittain ilman haittaohjelmaa. Hyökkäys voi olla monivaiheinen ja siinä voidaan aluksi käyttää hyödyksi suojauksen puutetta. Kun järjestelmään on päästy sisään, varsinainen hyökkäys tehdään osana järjestelmää, ”living off the land”. Tämän tyyppisten hyökkäysten tunnistamisessa voidaan käyttää esimerkiksi yhteyksien suuntaa, määriä ja frekvenssejä, lokien poikkeavuuksia, käyttäjätunnuksia ja käyttövaltuuksien muutoksia. Hyökkäyksestä kertovia tunnistetietoja kutsutaan nimellä Indicator of Compromise ja tällaisten tunnisteiden vaihtamisesta on olemassa aikaisempia käytäntöjä.

4.11 Tietojen hävittäminen

Tietoliikennetiedustelua ei voi teknisesti suodattaa niin, ettei kerättäviin tietoihin tulisi mukaan sellaisia viestejä, jotka eivät ole lupaehtojen perusteiden mukaisia. Materiaalissa olevat sellaiset tiedot, jotka eivät uhkaa kansallista turvallisuutta on hävitettävä viipymättä. Jos tiedot ovat sellaisia, joita voidaan käyttää rikostorjunnassa ja ne täyttävät PolL 5a:44 § vaatimukset, ne voidaan luovuttaa rikostorjuntaan ja tallentaa poliisin henkilörekistereihin. Jos materiaalissa on tiedustelukiellon alaista viestintää, niin se on hävitettävä ilman poikkeuksia. (TTST 15 §.)

Tiedonhankintatyöryhmä esitti mietinnössään, että hävittämisvelvollisuus koskisi aina sellaista haltuun saatua tietoa, joka on tallennettu ulkomaiselle pilvipalvelulle. Mietinnössä ei ollut perusteita esitykselle, eikä vertailumaiden lainsäädännössä ole vastaavaa kohtaa. Kyseistä kohtaa ei tullut myöskään Suomen lainsäädäntöön. Vaikka pilvipalveluun tallentaminen ei ole varsinaista viestintää, niin pilvipalvelussa voi olla toisilleen tuntemattomien henkilöiden perustama työtila, jossa jaetaan tietoa esimerkiksi terrori-iskun suunnittelua ja toteutusta varten. Viestinnäksi voidaan ajatella tilanne, jossa tallennetaan asiakirja pilvipalveluun ja joku toinen käy lukemassa asiakirjan palvelimelta. (HE 202/2017, 131–132.)

4.12 Tietoliikennetiedustelusta ilmoittaminen

Kaikessa Suomen lainsäädännössä lähdetään yleensä siitä, että jos jonkin lain perusteella tehdään toimenpiteitä tai päätöksiä, tulee lainkäytön kohteelle aina ilmoittaa mitä lakia ja millä perusteella lakia on sovellettu. Asianosaisella pitää olla myös mahdollisuus tutustua viranomaisen hallussa olevaan aineistoon. Tämä mahdollistaa sen, että lainkäytön kohteena olevalla henkilöllä on mahdollisuus hakea muutosta viranomaisen tekemään päätökseen tai kannella viranomaisen toiminnasta.

Viranomaisten asiakirjojen julkisuutta on rajoitettu viranomaisten toiminnan julkisuudesta annetun lain 11 § 2 momentissa. Tietoa ei tarvitse antaa asiakirjasta, jos se on vastoin erittäin tärkeää yleistä tai yksityistä etua, jos siitä on haittaa asian selvittämiselle. Perusteluina voi olla tutkinnalliset syyt, hengen ja terveyden suoja, valtion turvallisuus sekä salassa pidettävät taktisten ja teknisten menetelmien suojaaminen. Jos perusteena on rikoksen selvittäminen, sille voidaan melko helposti määrittää joku aikaraja. Valtion turvallisuuteen liittyvä salaamisessa takarajan määrittäminen voi olla vaikeampaa, joten tieto voidaan salata kokonaan. (JulkL 11 § 2.)

Myös tiedustelumenetelmän käytöstä tulee ilmoittaa viipymättä. Laki tietoliikennetiedustelusta siviilitiedustelussa 20 § viittaa poliisilain 5a:47 §:n, jossa säädetään telekuuntelusta ilmoittamisesta. Pääsääntönä on, että toimenpiteestä on ilmoitettava viimeistään vuoden kuluttua tiedustelumenetelmän käytön lopettamisesta. Tuomioistuimen päätöksellä ilmoittamista voidaan lykätä ja se voidaan jättää tekemättä kokonaan, jos se on välttämätöntä kansallisen turvallisuuden suojaamiseksi taikka hengen tai terveyden suojaamiseksi.

Tiedustelun kohteelle ilmoittaminen lisää osaltaan laillisuusvalvonnan onnistumista ja lisää viranomaisen tarvetta perustella huolellisesti tietoliikenteen aloittamisen syitä jo lupaa vaadittaessa. Jos ilmoitusvelvollisuutta ei olisi, niin ei olisi pelkoa siitä, että kohde tekee asiasta kantelun, jolloin saattaisi selvitä, että kyseisessä tapauksessa ei olisikaan ollut perusteltua syytä aloittaa tietoliikennetiedustelua.

4.13 Laillisuusvalvonta

Laissa tiedustelutoiminnan valvonnasta 2 §:ssä määriteltiin kaksi uutta valvontaelintä: tiedusteluvalvontavaliokunta ja tiedusteluvalvontavaltuutettu. Näiden lisäksi suojelupoliisin toimintaa valvoo jo aikaisemmassa lainsäädännössä määritellyt valvontaviranomaiset.

Parlamentaarisella valvonnalla tarkoitetaan valvontaelintä, jonka jäseniin vaikuttaa parlamentin kokoonpano. Ennen tiedustelulainsäädännön voimaantuloa eduskunnalla on ollut oikeus saada tietoja PL 47 § perusteella suojelupoliisin toiminnasta. Perustuslain perusteella tehdyissä selvityksissä suojelupoliisi on esitellyt toimintaansa lähinnä yleisellä tasolla (HE 199/2017, 7). Tiedustelulainsäädännön myötä perustettiin tiedusteluvaliokunta, jonka tehtävänä on parlamentaarinen valvonta. Tiedusteluvalvontavaliokunnassa on 11 jäsentä ja 2 varajäsentä (Eduskunnan työjärjestys 8 §). Tiedusteluvalvontavaliokunta suorittaa valvontaa yleisellä tasolla ja sillä on oikeus saada tietoja salassapitosäännösten estämättä (Eduskunnan työjärjestys 31b §; Laki tiedustelutoiminnan valvonnasta 2:3 §). Valiokunnan tekemä valvonta ei kohdistu yksittäisten tapauksien laillisuusvalvontaan vaan se tehtävä kuuluu tiedusteluvalvontavaltuutetulle tai oikeusasiamiehelle. Lopullinen ratkaisu yksittäisessä tapauksessa käsitellään tarvittaessa tuomioistuimessa.

Orwellin kirjassaan Vuonna 1984 kuvaamassa maailmassa totuus ja historia muuttuivat aina poliittisen tilanteen mukaan. Tavallaan huoli tästä näkyy Keskustapuolueen lausunnossa (Suomen Keskusta 2017), jossa parlamentaarista valvontaa pidettiin erittäin tärkeänä, mutta korostettiin samalla, että valvonta ei saa riippua siitä, mikä poliittinen tilanne vallitsee.

Tiedusteluvalvontavaltuutetun tehtäviä käsitellään laissa tiedustelutoiminnan valvonnasta luvussa 3. Valtuutettu on täysin itsenäinen ja riippumaton tehtävässään ja hänet nimitetään enintään viideksi vuodeksi kerrallaan. Valtuutetun tehtävänä on tiedustelutoiminnan laillisuusvalvonta ja tiedustelutoiminnan seuranta ja kehittämisehdotusten laatiminen havaittuaan sen tarpeelliseksi. Tiedusteluvalvontavaltuutetun tehtävänään on suorittaa oikeudellista valvontaa tiedustelulakiin perustuvien toimenpiteiden suhteen. Hän raportoi vuosittain tiedusteluvaliokunnalle, eduskunnan oikeusasiamiehelle ja valtioneuvostolle. Suojelupoliisin on ilmoitettava mahdollisimman pian tiedusteluvalvontavaltuutetulle tuomioistuimelle tehdystä tiedustelumenetelmää koskevasta vaatimuksesta (PolL 61 §).

Tiedusteluvalvontavaltuutetulle voi tehdä kantelun, jos epäilee että on joutunut tiedustelutoiminnan kohteeksi. Tiedustelutoiminnan valvonnasta annetun lain 10 § mukaan tiedusteluvaltuutetulla on oikeus päästä kaikkiin käytettyihin tietojärjestelmiin, jotta hän voisi tutkia toiminnan lainmukaisuuden.

Valtuutetun tehtävänä olisi myös valvoa tuomioistuinkäsittelyä haettaessa lupaa esimerkiksi tietoliikennetiedusteluun. Hänellä ei ole velvollisuutta osallistua lupakäsittelyyn vaan hänellä on läsnäolo-oikeus. Valtuutettu ei kuitenkaan saa osallistua käsittelyyn vaan läsnäolollaan hänellä on mahdollisuus hankkia tietoonsa kaikki ne perusteet, joilla hakemus

on tehty ja siten tarkastaa niiden laillisuus. Puolustusvaliokunta (2018, 11) on lausunnossaan ollut sitä mieltä, että valtuutetulla on oltava mahdollisuus tulla kuulluksi. Jos valtuutettu huomaa käsittelyssä jotain sellaista, että hänellä on mahdollisuus keskeyttää toiminta, hänen täytyy ensin odottaa, että mahdollisesti lainvastainen menetelmä otetaan käyttöön ja vasta sen jälkeen viedä asia tuomioistuimen käsittelyyn.

Oikeusasiamies on pääasiallinen suojelupoliisin laillisuusvalvontaa aikaisemmin tehnyt virkamies. Keskeisimpiä toimintamuotoja on ollut kantelujen tutkiminen, omat aloitteet ja tarkastukset (HE 199/2017, 7). Sisäministeriö raportoi kerran vuodessa salaisten pakkokeinojen käytöstä. Oikeusasiamies raportoi omasta toiminnastaan kerran vuodessa eduskunnalle.

Tietosuojavaltuutetun tehtävänä on valvoa henkilötietojen käsittelyä viranomaistoiminnassa. Tietosuojavaltuutetulla on oikeus nähdä henkilötietojen käsittelyyn liittyviä tietoja salassapitosäännösten estämättä. Hän voi tarkastaa rekisteritietojen lainmukaisuuden rekisteröidyn pyynnöstä, jos rekisteri on sellainen, johon rekisteröidyllä henkilöllä ei ole muuten tarkastusoikeutta. Tarkastuksen jälkeen rekisteröity saa tiedon onko asiassa ilmennyt jotain huomautettavaa. (HE 199/2017, 9)

Tarkastusvaliokunta (2018) on lausunnossaan painottanut sitä, että tiedustelutoiminnasta pitää saada tietoja myös julkisuuteen. Tiedustelutoiminnasta tehtyjen julkisten raporttien avulla voitaisiin osaltaan valvoa laillisuutta ja samalla vähentää mahdollisia epäluuloja viranomaistoimintaa kohtaan.

5 Valvooko Isoveli?

Perustuslain tärkeimpiä tehtäviä on suojata kansalaisten oikeuksia ja yhdenvertaisuutta, niin että näiden oikeuksien loukkaamisesta pitää säätää erikseen ja oikeutta voi loukata vain tietyissä olosuhteissa. Perusoikeuksiin kuuluu myös vapausoikeudet, jolla turvataan yksilön vapautta julkisen vallan puuttumiselta. ”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton” (PL10 § 2).

Perustuslain 22 § mukaan julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Hallituksen esityksessä on katsottu, että vaikka tiedustelumenetelmillä puututaan joihinkin perusoikeuksiin, siviilitiedustelulainsäädännöllä pyritään suojaamaan muita perusoikeuksia, kuten elämää ja henkilökohtaista turvallisuutta sekä valtion itsemääräämisoikeutta (HE 202/2017, 169).

Ennen kuin haetaan tuomioistuimen lupaa tietoliikennetiedusteluun, pitää selvittää missä osassa verkkoa kiinnostuksen kohteena oleva viestintä kulkee Suomen rajan yli. Tietyn verkonosan tunnistaminen uhkaviestinnän reittinä voi olla erittäin vaikeaa tai jopa mahdotonta. Parhaimmillaan voidaan päästä vain hyvään arvaukseen. Tiedustelulainsäädännöllä ja etenkin verkkoon kohdistuvan tiedonhankinnan on arvoitu vaikuttavan sivullisten henkilöiden viestinnän suojaan. Tiedonhankinnan laajuutta on kuitenkin pyritty rajaamaan niin, että kun viestinnän suojaan puututaan, sen on oltava välttämätöntä ja viimeinen käytettävissä oleva keino.

Suurin tietoliikennetiedustelua rajaava tekijä on hakuehdon tiukka määritteleminen laissa. Jos automaattista suodatusta saataisiin kohdistaa myös viestin sisältöön, viranomaisen ei välttämättä tarvitse tietää, missä osassa tietoverkkoa kohteet viestivät. Tällöin kaikkeen tietoliikenteeseen voitaisiin kohdistaa suodatus, jossa etsittäisiin harvinaisia nimiä tai ilmaisuja, joita kohteet käyttävät. Terroristiseen toimintaan liittyvän viestinnän ei voi olettaa menevän aina tiettyyn paikkaan ja myös välityspalvelinta käyttämällä voidaan lopullinen kohde piilottaa. Lainsäädännön valmistelun aikana tehdyissä vertailussa todettiin, että useimmissa muissa maissa vastaavaa rajoitusta ei ole säädetty (HE 202/2017, 80). Vaikka hakuehtoja saadaan kohdistaa useissa vertailumaissa viestin sisältöön, niin hakuehtona voi käyttää vain sellaisia sanoja, jotka eivät ole yleisesti käytössä. Tiedonhankintatyöryhmä kuitenkin suositteli, että hakuehtoja rajataan niin, että hakuehtoina voisi olla vain verkkoliikenteen tunnistamistiedot. Ainoana poikkeuksena olisivat haittaohjelmat, joiden tunniste voitaisiin seuloa myös viestin sisällöstä. (Puolustusministeriö 2015, 64.)

Lainsäätäjän tarkoituksena on ollut tarkoitus täydentää aikaisempaa lainsäädäntöä. Aikaisemman lainsäädännön avulla voidaan hankkia tietoa tunnistetuista uhkista ja tiedustelulainsäädännöllä pyritään tunnistamaan ja havaitsemaan kansallista turvallisuutta uhkaavaa toimintaa. Lopullisena tavoitteena tietoliikennetiedustelulla on selvittää verkkoliikenteestä telepäätelaitteita ja teleosoitteita, jolloin voidaan käyttää telekuunteluun tai televalvontaan liittyvää lainsäädäntöä.

Vaikka joissain maissa viestin sisältöön voidaan kohdistaa suodatusta, nykyaikaiset salausteniikat estävät tai ainakin vaikeuttavat sitä. Tiedonhankintatyöryhmä on mietinnössään todennut, että tietoliikennetiedustelulla voidaan saada tuloksia, koska viestissä olevia liikenteen ohjaustietoja ei voida täysin salata. Tämän takia hyvin kohdennettu tunnistamistietoihin kohdistettu suodatus voi olla tehokas menetelmä, verrattuna pelkään viestin sisältöön kohdistuvassa suodatukseen. Kun suodatettua liikennettä tarkastellaan suojelupoliisissa, kyky avata salattuja viestejä on nyt ja tulevaisuudessa tärkeässä roolissa, jos tietoliikennetiedustelulla halutaan saada näkyviä tuloksia. (Puolustusministeriö 2015, 72.) Laillisuusvalvontavastuu on tiedustelua suorittavan organisaation ulkopuolella. Uskottavan valvonnan toteutumiseen vaaditaan ulkopuolista riippumatonta tahoa. Tiedustelulainsäädännön oikeudellista valvontaa tekevät henkilöt vaihtuvat säännöllisesti. Tämä mahdollistaa sen, ettei valvontaan pääse syntymään rutiineja ja hiljalleen muodostuvia käytäntöjä. Toisaalta laillisuusvalvonnassa käsitellyt asiat voivat olla hyvin sensitiivisiä ja vastuuhenkilöiden jatkuva vaihtumien voi muodostaa tietoturvaan liittyvän riskin. Jos esimerkiksi valtiolliseen turvallisuuteen liittyviä tietoja pääsee vuotamaan asiaankuulumattomille, niin yhteistyö muiden valtioiden ja viranomaisten kanssa voi vaikeutua. Jos Suomen tiedustelutoimintaan ei voi luottaa, voivatko muut valtiot luottaa Suomeen luovutettujen tietojen salassa pysymiseen? Tämä sama riski voi olla myös liiketoimintaan liittyvissä tiedoissa, jotka voivat vuotaa ulkopuolisille. Yritysten halukkuus sijoittaa toimintojaan Suomeen voi vaarantua, jos tietoa vuotaa ulkopuoliselle viranomaistoiminnan takia. Tietojen vuotaminen julkisuuteen voi aiheuttaa myös henkeen ja terveyteen liittyvän riskin asianosaisille.

Organisaation oman valvonnan pettäminen tulee parhaiten esiin oikeudenkäynneissä virkavelvollisuuden rikkomisesta, jossa syytettynä on poliisin ylintä johtoa (MTV 2018). Samalla voidaan kysyä, mahdollistiko huono valvonta Jari Aarnion epäillyt rikokset, vai olivatko ne vain sen seurausta? Tehokas ja hyvin dokumentoitu valvonta on myös lakia käyttävän viranomaisen etu. Jos Aarnio on syytön häntä vastaan nostettuihin syytteisiin, niin oikein suoritettu ja dokumentoitu laillisuusvalvonta voisi tukea hänen puolustustaan.

Suomesta kulkee tietoliikenneyhteyksiä Ruotsiin, Venäjälle ja Saksaan. Kaikissa näissä maissa tehdään ulkomaiseen liikenteeseen kohdistuvaa tiedonhankintaa. Tästä voidaan

päätellä, että Suomesta ulkomaille lähtevään liikenteeseen on kohdistunut tiedustelua jo ennen kansallisen lainsäädännön säätämistä. Ulkomainen toimija tekee tiedustelua omista lähtökodistaan ja intresseistään, joten Suomeen kohdistuvan uhkan tietoon saaminen on ollut täysin kiinni siitä, miten hyväntahtoinen tiedon saanut viranomainen on ollut. (HE 202/2017, 112)

Tietoliikennetiedustelu on vain pieni osa tiedustelulakipakettia, mutta on herättänyt paljon mielipiteitä puolesta ja vastaan. Kaikki ymmärtävät, että tietoliikennetiedustelua tarvitaan jossakin muodossa erilaisten uhkien torjumisessa. Tiedustelulakipaketti on monesta näkökulmasta mietitty kompromissi yksityiselämän suoja vastaan täydellinen verkon valvonta. Kaikkien tietoverkkoihin tehtävien tiedustelutoimenpiteiden täytyy olla hyvin rajattuja ja perusteltuja. Tämä kuitenkin vähentää merkittävästi mahdollisuuksia löytää verkosta indikaattoreita esimerkiksi mahdollisesta terrori-iskusta Suomessa. Toisaalta tietoverkoissa on niin paljon liikennettä, että vaikka kaikkea liikennettä voisi valvoa laillisesti, ei Suomen kokoisen valtion resurssit riittäisi sen tehokkaaseen analysoimiseen. Ehkä tehokkaimpana verkon yleistä valvontaa rajoittavana tekijänä ovat viranomaisten rajalliset resurssit ja sen aiheuttama tehtävien priorisointi.

6 Pohdinta

Arvioitaessa tietoliikennetiedustelua Euroopan ihmisoikeussopimuksen ja EU-oikeuden näkökulmasta voidaan lainsäädäntöä testata niin sanotun Huvig/Kruslin-testin avulla. Testi perustuu kahteen ihmisoikeustuomioistuimen tapaukseen Huvig v. Ranska 24.4.1990 ja Kruslin v. Ranska 24.4.1990, joiden ratkaisuja on myöhemmin sovellettu. Testin mukaan viestintäsalaisuuteen puuttuvassa lainsäädännössä tulee olla:

1. henkilön määrittely, jonka viestintäsalaisuuteen puututaan
2. tekojen tai uhkien määrittely, jotka oikeuttavat viestintäsalaisuuteen puuttumisen
3. kuinka puuttumisesta päätetään
4. säännöt tietojen käsittelyyn
5. säännökset viestintäsalaisuuteen puuttumisen kestosta ja tietojen säilytysajoista
6. tietojen luovutukseen liittyvät varotoimet
7. tietojen hävittämiseen liittyvät säädökset. (HE 202/2017, 81.)

Tämän työn aikana selvisi miten moneen eri lakiin siviilitiedustelulainsäädäntö vaikutti. Päähuomioni oli tietoliikennetiedustelussa, mutta jouduin ottamaan useita muita lakeja huomioon saadakseni kokonaiskuvan tietoliikennetiedustelun toteuttamisesta ja sen valvonnasta. Yhtenä esimerkkinä vaikutusten laajuudesta on se, että tehtävää aloittaessani en uskonut, että päätyisin jossain vaiheessa lukemaan eduskunnan työjärjestystä. Vaikka olen joutunut tutustumaan lainsäädäntöön aikaisemminkin, niin en ole juurikaan lukenut niihin liittyviä hallituksen esityksiä. Tehtävän aikana opin, että hallituksen esityksiä lukemalla voi päästä parempaan ymmärrykseen siitä, mitä tietyllä lailla on tarkoitettu ja miksi se on kirjoitettu niin kuin se on laissa.

Luin Orwellin kirjan Vuonna 1984 tätä työtä tehdessäni. ”Orwellin maailma” on muodostunut yleisesti tunnetuksi käsitteeksi. Kirjan maailma oli erittäin lohduton ja siinä oli selkeä sanoma siitä, millaiseksi viranomaisvalvonta ei saa missään tilanteessa kehittyä. Kirjassa oli kuitenkin pelottavan paljon enteitä siitä, mihin tämän päivän maailmanpolitiikka on kehittymässä.

Mielestäni lakipaketti on huolellisesti valmisteltu ja siitä on pyydetty asiantuntijalausuntoja hyvin monelta taholta. Jos lakipakettia arvioidaan Huvig/Kruslin-testin avulla, niin kaikkiin kohtiin on otettu kantaa siviilitiedusteluun liittyvässä lainsäädännössä. Lakiin tuli tarkennuksia lainvalmistelun ja eduskuntakäsittelyn aikana varsinkin valvontaan liittyvien kysymysten kohdalla. Laissa on myös tiukemmat rajoitteet tietoliikennetiedustelun toteuttamiselle kuin valmistelun aikana tarkastelussa olleissa vertailumaissa. Suomen lainsäädäntö on hyvin samankaltainen kuin Ruotsin vastaava, mutta siinä on rajoitteita viestin sisältöön kohdistuvan suodatuksen tekemisessä.

Koska laki on vielä uusi ja siitä ei ole oikeuskäytäntöä, niin aiheesta voisi tehdä lisätutkimuksen, miten tiedustelulainsäädäntö on otettu käyttöön suojelupoliisissa. Haasteena tutkimuksen tekemisessä saattaa olla asiakirjojen julkisuus, mutta toivottavasti ainakin joitain tilastotietoja olisi käytössä tutkimuksen tekemiseksi. Toinen lisätutkimuksen aihe voisi olla käynnissä olevat lainsäädäntöhankkeet tietoliikennetiedusteluun liittyen eri Euroopan maissa ja niiden vertaaminen Suomen voimassaolevaan lainsäädäntöön.

Myös tietoliikenteeseen kohdistuvien hakuehtojen tehokkuus olisi mielenkiintoinen tutkimusaihe, mutta teknisiä tai taktisia tietoja ei ole saatavissa ulkopuoliseen käyttöön. Uskon, että tämäntyyppistä analyysiä tullaan tekemään tietoliikennetiedustelua suorittavissa viranomaisissa, jotta voitaisiin päästä eroon mahdollisimman suuresta osasta ylimääräisestä viestiliikenteestä ja saada vain oleellinen tieto käsiteltäväksi.

Lähteet

Björksten, T. 26.5.2017. Maailmalla levinneestä tietokoneviruksesta uusi versio – lunnaita maksettu jo 100 000 euroa. Luettavissa: https://yle.fi/uutiset/3-9633383. Luettu: 15.10.2019

Eduskunnan työjärjestys. Luettavissa: https://www.finlex.fi/fi/laki/ajantasa/2000/20000040. Luettu: 8.9.2019

Esitutkintalaki 805/2011

Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses. Luettavissa: https://www.gesetze-im-internet.de/g10_2001/. Luettu: 11.9.2019

HE 14/1985. Hallituksen esitys Eduskunnalle esitutkintaa ja pakkokeinoja rikosasioissa koskevaksi lainsäädännöksi. Luettavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/he_14+1985.pdf. Luettu: 25.9.2019

HE 198/2017. Hallituksen esitys eduskunnalle laiksi Suomen perustuslain 10 §:n muuttamisesta. Luettavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_198+2017.aspx. Luettu: 8.9.2019

HE 199/2017. Hallituksen esitys eduskunnalle laiksi tiedustelutoiminnan valvonnasta ja laiksi valtion virkamieslain 7 §:n muuttamisesta. Luettavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_199+2017.aspx. Luettu: 8.9.2019

HE 202/2017. Hallituksen esitys eduskunnalle siviilitiedustelua koskevaksi lainsäädännöksi. Luettavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_202+2017.aspx. Luettu: 11.8.2019

HE 203/2017. Hallituksen esitys eduskunnalle laiksi sotilastiedustelusta sekä eräiksi siihen liittyviksi laeiksi. Luettavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_203+2017.aspx. Luettu: 11.9.2019

Helsingin sanomat. 26.9.2015. Ulkoministeriöön vuonna 2013 iskenyt vakoiluohjelma vei tietoja "rekkalasteittain". Luettavissa: https://www.hs.fi/kotimaa/art-2000002764588.html. Luettu: 19.8.2019

Iltalehti. 27.3.2014. Mika Myllylän tietojen urkinnasta tuomio yli 70:lle. Luettavissa: https://www.iltalehti.fi/uutiset/a/2014032718161680. Luettu: 8.9.2019

Ilta-Sanomat. 2.5.2019. Operaattori kiistää väitteet: Huawein ”takaportti” onkin työkalu. Luettavissa: https://www.is.fi/digitoday/art-2000006091244.html. Luettu: 8.9.2019

Koivunen, E. 13.4.2018. F-Secure Oy Asiantuntijalausunto. Luettavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-176914.pdf. Luettu: 30.8.2019

Lag om signalspaning i försvarsunderrättelseverksamhet 2008:717. Luettavissa: https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2008717-om-signalspaning-i_sfs-2008-717. Luettu: 11.9.2019

Laki sotilastiedustelusta 590/2019

Laki viranomaisten toiminnan julkisuudesta 621/1999

Laki tietoliikennetiedustelusta siviilitiedustelussa 582/2019

Liikenne- ja viestintäministeriö. 16.6.2017. Asiantuntijalausunto. Luettavissa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1d7905e4-882a-4670-8c21-f988baa9afb1. Luettu: 30.8.2019

MTV. 19.12.2008. Liedon ryöstöyrityksestä ja Turun ryöstöstä yhteensä 62 vuotta vankeutta. Luettavissa: https://www.mtvuutiset.fi/artikkeli/liedon-ryostoyrityksesta-ja-turun-ryostosta-yhteensa-62-vuotta-vankeutta/2065194. Luettu: 30.9.2019

MTV. 13.8.2018. KRP:n päällikkö Robin Lardot syytteeseen virkavelvollisuuden rikkomisesta. Luettavissa: https://www.mtv.fi/uutiset/kotimaa/artikkeli/krp-n-paallikko-robin-lardot-syytteeseen-virkavelvollisuuden-rikkomisesta/7028424. Luettu 11.8.2019

Nurmi, T. 1.3.2019. Helsingin käräjäoikeus Asiantuntijalausunto. Luettavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2018-AK-173443.pdf. Luettu: 27.9.2019

Oikeusministeriö. Kansainvälinen oikeusapu rikosasioissa. Luettavissa: https://oikeusministerio.fi/rikosasiat. Luettu: 27.9.2019

Orwell, G.1999.Vuonna 1984. WSOY. Helsinki.

Poliisilaki 872/2011

Puolustusministeriö. 2015. Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö. Luettavissa: https://www.defmin.fi/files/3016/Suomalaisen_tiedustelulainsaadannon_suuntaviivoja.pdf. Luettu: 8.9.2019

Puolustusvaliokunnan lausunto. 6.11.2018. PuVL/16/2018 vp -HE 202/2017 vp. Luettavissa: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PuVL_16+2018.aspx. Luettu: 28.8.2019

Remes, J. 16.6.2017. Finnish Information Security Cluster ry FISC asiantuntijalausunto. Luettavissa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1d7905e4-882a-4670-8c21-f988baa9afb1. Luettu: 27.9.2019

Sisäministeriö. 21.06.2016. Sisäministeriön ja sen hallinnonalan laillisuusvalvontaohje. SMDno-2016-329. Luettavissa: https://intermin.fi/documents/1410869/3724304/sisaministerion_ja_sen_hallinnonalan_laillisuusvalvontaohje_21062016.pdf/c9fc5fd9-2ae5-4d57-bce4-509c8d808355. Luettu 30.8.2019

Sisäministeriö. 19.4.2017. Sisäministeriön julkaisu 8/2017. Siviilitiedustelulainsäädäntö. Siviilitiedustelulakityöryhmän mietintö. Luettavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/79759/SM_08_2017_Siviilitiedostelulainsaadanto.pdf. Luettu: 11.8.2019

Suomen Keskusta. 15.6.2017. Asiantuntijalausunto. Luettavissa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1d7905e4-882a-4670-8c21-f988baa9afb1. Luettu: 30.8.2019

Suomen kuvalehti. 10.11.2010. Ilmestyskirjan mato: Stuxnet on yhä arvoitus, lue taustat kybersodan aseesta. Luettavissa: https://suomenkuvalehti.fi/jutut/ulkomaat/ilmestyskirjan-mato-stuxnet-on-yha-arvoitus-lue-taustat-kybersodan-aseesta/. Luettu: 19.8.2019

Suomen perustuslaki 731/1999

Suomen Sadankomitea ry. 15.6.2017. Asiantuntijalausunto. Luettavissa: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=1d7905e4-882a-4670-8c21-f988baa9afb1. Luettu: 30.9.2019

Suojelupoliisi. 2019. Luettavissa: https://www.supo.fi/. Luettu 11.8.2019

Tarkastusvaliokunnan lausunto. 10.4.2018. TrVL 3/2018 vp -HE 202/2017 vp. Luettavissa: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/TrVL_3+2018.aspx. Luettu 3.9.2019

Valtioneuvoston asetus esitutkinnasta, pakkokeinoista ja salaisesta tiedonhankinnasta 122/2014

Liitteet

Liite 1. Tiedonhankintamenetelmät