Puolustusministeriö
Försvarsministeriet
Ministry of Defence

SUOMALAISEN TIEDUSTELULAINSÄÄDÄNNÖN SUUNTAVIIVOJA

RIKTLINJER FÖR EN FINSK UNDERRÄTTELSELAGSTIFTNING

Tiedonhankintalakityöryhmän mietintö
Betänkande av arbetsgruppen för en informationsanskaffningslag

Puolustusministeriö | 2015

SUOMALAISEN TIEDUSTELULAINSÄÄDÄNNÖN SUUNTAVIIVOJA

Tiedonhankintalakityöryhmän mietintö

RIKTLINJER FÖR EN FINSK UNDERRÄTTELSELAGSTIFTNING

Betänkande av arbetsgruppen för en informationsanskaffningslag

PUOLUSTUSMINISTERIÖ

KUVAILULEHTI
14.1.2015

Tekijät	Julkaisun laji	työryhmän mietintö
Tiedonhankintalakityöryhmä Hanna Nordström (puheenjohtaja) Katriina Laitinen (varapuheenjohtaja) Mika Lundelin (työryhmän jäsen) Jenni Herrala (sihteeri) Jan Sjöblom (sihteeri) Kosti Honkanen (sihteeri) Minnamaria Nurminen (sihteeri)	Toimeksiantaja	puolustusministeriö
	Toimielimen asettamispäivä	13.12.2013
Julkaisun nimi	**Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintalakityöryhmän mietintö.**	
	Julkaisu on saatavissa internetistä osoitteesta **www.defmin.fi**	

Tiivistelmä

Mietinnössä arvioidaan tiedustelua koskevan lainsäädännön kehittämistarpeita.

Kansallisesta turvallisuudesta vastaavien viranomaisten tiedonhankinta tietoverkkoympäristöstä vakavien uhkien tunnistamiseksi on luonteeltaan tiedustelua. Suomessa ei ole tiedustelua koskevaa lainsäädäntöä. Työryhmä ehdottaa harkittavaksi, että hallitus käynnistäisi tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi.

Tiedustelun tarkoituksena olisi hankkia kansallisen turvallisuuden kannalta välttämätöntä tietoa vakavista kansainvälisistä uhista. Uhat voisivat olla sotilaallisia tai siviililuontoisia. Tiedustelulla varmistettaisiin valtion ylimmän johdon päätöksenteon perustuminen oikeaan, ajantasaiseen ja luotettavaan tietoon sekä mahdollistettaisiin toimivaltaisten viranomaisten ryhtyminen uhkien torjuntaan.

Kansallisesta turvallisuudesta vastaaville sotilas- ja siviiliviranomaisille tulisi harkita toimivaltuuksia rajat ylittävään tietoliikenteeseen kohdistettavaan tiedusteluun, jotta turvallisuusympäristön muutoksiin voitaisiin vastata. Tietoliikennetiedustelun tekninen suorittaminen olisi tarkoituksenmukaista keskittää yhdelle viranomaiselle.

Puolustusvoimille ja Suojelupoliisille tulisi harkita toimivaltuuksia ulkomaan tiedusteluun, jossa hankittaisiin tietoja henkilöiltä ja tietojärjestelmistä. Koska ulkomaan tiedusteluun liittyy ulkopoliittisesti sensitiivisiä elementtejä, sitä koskevassa päätöksenteossa olisi otettava huomioon valtion ylimmän johdon linjaukset. Ohjaus- ja vastuusuhteet tulisi arvioida mahdollisen jatkovalmistelun yhteydessä.

Tietoliikennetiedusteluun tulisi liittää riippumaton lupamenettely. Tietoliikennetiedustelua ja ulkomaan tiedustelua varten tulisi luoda riippumaton valvontajärjestelmä.

Tietoliikennetiedustelua koskevan lainsäädännön valmistelua harkittaessa on erityisesti otettava huomioon jokaiselle perus- ja ihmisoikeutena turvattu luottamuksellisen viestin salaisuuden suoja. Tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta ei näyttäisi olevan mahdollista säätää perustuslakia muuttamatta, pelkästään vieraan valtion tietoliikenteeseen kohdistuvaa tiedustelua ehkä lukuun ottamatta.

Avainsanat (asiasanat):	lainsäädäntö, tiedustelu, Suojelupoliisi, puolustusvoimat, poliisi, tietoliikenne				
Muut tiedot (HARE-numero, muu viitenumero):	HARE PLM004:00/2013				
ISBN	978-951-25-2623-9 nid. 978-951-25-2624-6 pdf	Kieli	suomi	Luottamuksellisuus	julkinen
Paino		Kustantaja	puolustusministeriö		

FÖRSVARSMINISTERIET

PRESENTATIONSBLAD
14.1.2015

Författare	Typ av publication	arbetsgruppsbetänkande
Arbetsgruppen för en informationsanskaffningslag Hanna Nordström (ordförande) Katriina Laitinen (vice ordförande) Mika Lundelin (arbetsgruppsmedlem) Jenni Herrala (sekreterare) Jan Sjöblom (sekreterare) Kosti Honkanen (sekreterare) Minnamaria Nurminen (sekreterare)	Uppdragsgivare	försvarsministeriet
	Datum då organet tillsattes	13.12.2013
Publication (även den finska titeln)	**Suomalaisen tiedustelulainsäädännön suuntaviivoja. Tiedonhankintatyöryhmän mietintö. Riktlinjer för en finsk underrättelselagstiftning. Betänkande av arbetsgruppen för en informationsanskaffningslag**	
	Publikationen är tillgänglig på internet på adressen **www.defmin.fi**	

Sammandrag

I detta betänkande bedöms behoven att utveckla en lagstiftning om underrättelse.

Informationsanskaffning i datanätsomgivningen för att identifiera allvarliga hot, vilken utförs av de myndigheter som svarar för den nationella säkerheten, är till sin art underrättelse. Finland har ingen lagstiftning om underrättelse. Arbetsgruppen föreslår att det ska övervägas om regeringen kan inleda nödvändiga åtgärder för att skapa en författningsgrund för underrättelse.

Syftet med underrättelsen är att skaffa den information om allvarliga internationella hot som är nödvändig med tanke på den nationella säkerheten. Hoten kan vara militära eller civila. Genom underrättelse säkerställs att statens högsta lednings beslutsfattande grundar sig på korrekt, aktuell och tillförlitlig information samt möjliggörs att behöriga myndigheter kan vidta åtgärder för att avvärja hoten.

För de militära och civila myndigheter som svarar för den nationella säkerheten bör övervägas gräns-överskridande befogenheter att bedriva underrättelse som riktas mot datatrafiken för att förändringar i säkerhetsomgivningen ska kunna bemötas. Det tekniska genomförandet av underrättelse i datatrafiken vore det ändamålsenligt att koncentrera till en myndighet.

Det bör övervägas om försvarsmakten och Skyddspolisen kan få befogenheter för utlandsunderrättelse för att skaffa information om personer och informationssystem. Eftersom det med utlandsunderrättelse sammanhänger utrikespolitiskt sensitiva element, bör vid beslutsfattandet om sådan beaktas de riktlinjer som statens högsta ledning har dragit upp. Styr- och ansvarsförhållandena bör bedömas i samband med den eventuella fortsatta beredningen.

Till underrättelse i datatrafiken bör ett oavhängigt tillståndsförfarande fogas. För datatrafikunderrättelse och utlandsunderrättelse bör ett oavhängigt tillsynssystem skapas.

När beredningen av en lagstiftning om datatrafikunderrättelse övervägs, bör sekretesskyddet för konfidentiella meddelanden, som har tryggats för var och en i form av en grundläggande fri- och rättighet och en mänsklig rättighet, beaktas. Det verkar som om det inte vore möjligt att stifta en lag om datatrafikunderrättelse som ska bedrivas i underrättelsesyfte utan att grundlagen ändras, eventuellt med undantag för underrättelse som enbart riktar sig mot en främmande stats datatrafik.

Nyckelord:	lainsäädäntö, tiedustelu, Suojelupoliisi, puolustusvoimat, poliisi, tietoliikenne				
Övriga uppgifter (HARE-nummer, andra referensnummer):	HARE PLM004:00/2013				
ISBN	978-951-25-2623-9 häft 978-951-25-2624-6 pdf	Språk	finska, referat även på svenska	Sekretessgrad	offentlig
Distribution		Förlag	försvarsministeriet		

MINISTRY OF DEFENCE

DESCRIPTION
14.1.2015

Authors	Type of publication	A report of the Working Group
Working group for developing legislation on intelligence Hanna Nordström (chair) Katriina Laitinen (vice-chair) Mika Lundelin (member of the working group) Jenni Herrala (secretary) Jan Sjöblom (secretary) Kosti Honkanen (secretary) Minnamaria Nurminen (secretary)	Contracted by	Ministry of Defence
	Working group nominated on	13.12.2013
Name of publication	**Guidelines for developing Finnish legislation on conducting intelligence. A report of the Working Group.**	
	The publication is available on the internet at www.defmin.fi	

Summary

The need to develop legislation on conducting intelligence activities is assessed in the report.

When the authorities responsible for national security collect information in the cyber domain to identify serious threats their work is, by its very nature, intelligence work. The existing legislation in Finland does not, however, address intelligence. The Working Group therefore proposes that the Government should initiate necessary measures to create a legal basis for intelligence activities.

The purpose would be to collect vital information to protect national security against serious international threats. These could be military or civilian in nature. Intelligence activities would thus ensure that the state leadership is able to base its decision-making on timely and trustworthy information and competent authorities are able to take measures to counter threats.

Military and civilian authorities in charge of national security should be granted powers to conduct cross-border intelligence to respond to changes in the security environment. It would be practical if just one authority was involved technically in conducting intelligence on telecommunications.

It is to be considered whether the Defence Forces and the Finnish Security Intelligence Service should be given powers to conduct foreign intelligence to gather information from individuals and on information systems. The policy-settings of the state leadership should be taken into account when making decisions on conducting foreign intelligence as this is related to sensitive foreign-policy elements. Responsibility and steering issues must be assessed if legislative drafting is begun.

An independent authorisation process should be part of intelligence on telecommunications. In addition, an independent system of supervision should be created for the purposes of foreign intelligence and conducting intelligence on telecommunications.

The protection of confidential communications, provided for as basic and human rights, should be given special attention when the drafting of legislation on telecommunications is considered. With the possible exception of conducting intelligence on the telecommunications of a foreign state, it would appear that it is not possible to draft legislation relating to telecommunications interception and access without amending the Constitution.

Key words:	legislation, intelligence, Finnish Security Intelligence Service, Defence Forces, police, telecommunications				
Other information (HARE number, other reference):	HARE PLM004:00/2013				
ISBN	978-951-25-2623-9 print 978-951-25-2624-6 pdf	Language	Finnish	Degree of confidentiality	public
Distributed by		Published by	Ministry of Defence		

Puolustusministeriölle

Puolustusministeriö asetti 13.12.2013 työryhmän kehittämään lainsäädäntöä turvallisuusviranomaisten tiedonhankintakyvyn parantamiseksi kybertoimintaympäristön uhkista. Työryhmän tuli saada työnsä valmiiksi viimeistään 30.6.2014.

Puolustusministeriö jatkoi 27.5.2014 työryhmän määräaikaa 31.12.2014 saakka.

Työryhmän tehtävänä oli arvioida Suomen lainsäädännön kehittämistarvetta siten, että Suomessa kyetään huolehtimaan kansallisesta turvallisuudesta tietoverkoissa esiintyvien uhkien torjumiseksi.

Työryhmän tehtävänä oli lisäksi koota yhteen näkemyksiä tietoverkkojen kautta Suomen turvallisuuteen kohdistuvista uhkista ja niiden vaikutuksista Suomen turvallisuudelle ja kilpailukyvylle, selvittää turvallisuusviranomaisten tiedonhankintaa koskeva nykytila ja kehittämisehdotukset, tarkastella tarvittavilta osin turvallisuusviranomaisten tiedonhankintaa koskevaa lainsäädäntöä eräissä muissa maissa, tuottaa vaikutusarviointi eri kehittämisvaihtoehdoista ja selvitetyn pohjalta tehdä lainsäädännön kehittämisehdotukset sekä esitys niiden toimeenpanon edellyttämistä toimista.

Työryhmän mietintö voitiin toimeksiannon mukaan laatia hallituksen esityksen muotoon tai siihen voitiin sisällyttää ehdotukset erillisten lainsäädäntöhankkeiden käynnistämiseksi.

Työryhmän puheenjohtajaksi määrättiin hallitusneuvos lainsäädäntöjohtajana *Hanna Nordström* puolustusministeriöstä ja varapuheenjohtajaksi hallitusneuvos, myöhemmin poliisiosaston lainsäädäntöjohtaja *Katriina Laitinen* sisäministeriöstä.

Työryhmän jäseniksi kutsuttiin oikeudellinen neuvonantaja *Minna Hulkkonen* tasavallan presidentin kansliasta, yksikön päällikkö *Mikko Kinnunen* ulkoasiainministeriöstä, lainsäädäntöjohtaja *Sami Manninen* oikeusministeriöstä, poliisitarkastaja *Jari Pajunen* sisäministeriöstä, yksikön päällikkö *Timo Junttila* ja hallitussihteeri *Pia Palojärvi* puolustusministeriöstä (4.6.2014 saakka), budjettineuvos *Petri Syrjänen* valtiovarainministeriöstä, yksikön päällikkö, lainsäädäntöneuvos *Kirsi Miettinen* liikenne- ja viestintäministeriöstä (24.10.2014 saakka), hallitusneuvos, myöhemmin henkilöstö- ja hallintojohtaja *Kari Mäkinen* työ- ja elinkeinoministeriöstä, poliisijohtaja *Tomi Vuori* Poliisihallituksesta, sektorijohtaja *Mika Lundelin* pääesikunnasta (4.6.2014 lähtien) ja viestintäneuvos, yksikön johtaja *Päivi Antikainen* liikenne- ja viestintäministeriöstä (24.10.2014 lähtien).

Työryhmän pysyviksi asiantuntijoiksi kutsuttiin oikeuspäällikkö *Päivi Kaukoranta* ulkoasiainministeriöstä, lainsäädäntöneuvos *Sami Kivivasara* valtiovarainministeriöstä (4.6.2014 saakka), lainsäädäntöneuvos *Hannele Kerola* valtiovarainministeriöstä (4.6.2014 lähtien), poliisineuvos *Antti Pelttari* ja apulaispäällikkö *Petri Knape* Suojelupoliisista, tiedustelupäällikkö *Harri Ohra-aho* pääesikunnasta, eversti *Martti J. Kari* puolustusvoimista ja neuvotteleva virkamies *Laura Tarhonen* liikenne- ja viestintäministeriöstä (10.9.2014 lähtien).

Työryhmän työhön ovat osallistuneet teknisinä asiantuntijoina järjestelmäasiantuntija *Sari Kajantie* Suojelupoliisista ja insinöörikapteeni *Jouni Flyktman* puolustusvoimista.

Työryhmän sihteerinä ovat toimineet hallitussihteeri *Jenni Herrala*, vanhempi hallitussihteeri *Minnamaria Nurminen* ja esittelijä *Kosti Honkanen* (4.6.2014 lähtien) puolustusministeriöstä, ylitarkastaja *Jan Sjöblom* Suojelupoliisista ja sektorijohtaja *Mika Lundelin* pääesikunnasta (4.6.2014 saakka). Työryhmä otti nimekseen tiedonhankintalakityöryhmä. Työryhmä on pitänyt 45 kokousta.

Työryhmä on työnsä aikana kuullut seuraavia henkilöitä.

tilannekuvakoordinaattori, yksikön päällikkö *Jarkko Korhonen*, valtioneuvoston kanslia
valtioneuvoston turvallisuusjohtaja *Timo Härkönen*, valtioneuvoston kanslia
tietohallintojohtaja *Ari Uusikartano*, ulkoasiainministeriö
erityisasiantuntija *Kimmo Janhunen*, valtiovarainministeriö

EU:n tiedusteluanalyysikeskuksen johtaja *Ilkka Salmi*
EU:n sotilastiedustelun päällikkö *Georgij Alafuzoff*

tietosuojavaltuutettu *Reijo Aarnio*
oikeustieteen professori *Veli-Pekka Viljanen*, Turun yliopisto

varautumispäällikkö ICT *Christian Fjäder*, Huoltovarmuuskeskus
johtaja *Kirsi Karlamaa*, Viestintävirasto
turvallisuussääntelyryhmän päällikkö *Jarkko Saarimäki*, Kyberturvallisuuskeskus
tietoturva-asiantuntija *Tomi Hasu*, Kyberturvallisuuskeskus
Keskusrikospoliisin päällikkö, poliisineuvos *Robin Lardot*
rikoskomisario *Timo Piiroinen*, Keskusrikospoliisi
järjestelmäasiantuntija *Pasi Paunu*, Suojelupoliisi

Nordic Policy Counsel *David Mothander*, Google
hallinto- ja turvallisuusjohtaja *Vesa Vuoti*, DNA Oyj
Head of Special Network Security *Krister Kaipio*, TeliaSonera Finland Oyj
turvallisuusjohtaja *Jaakko Wallenius*, Elisa Oyj
Platform Strategy Manager *Pasi Mäkinen*, Microsoft Oy
Vice President *Kaisa Olkkonen*, Nokia Government Relations
Head of Security Technologies *Gabriel Waller*, Nokia Solutions and Networks
tutkimusjohtaja *Mikko Hyppönen,* F-Secure Oyj
teknologiajohtaja *Kimmo Kasslin*, F-Secure Oyj
Pk- johtaja *Jyrki Hollmén*, Elinkeinoelämän keskusliitto
Associate Partner *Vesa Weissmann*, Gearshift Group Oy

Lisäksi työryhmä on kuullut luottamuksellisesti kahta ulkomaista asiantuntijaa tietoliikennetiedustelun tehokkuudesta ja tarpeellisuudesta.

Työryhmä on järjestänyt toimittajille taustoittamistilaisuuden 12.3.2014 ja yleisen kuulemistilaisuuden elinkeinoelämän edustajille 29.4.2014 sekä kansalaisjärjestöille ja muille sidosryhmille 6.5.2014.

Puolustusministeriö on työryhmän toimeksiannosta teettänyt tutkimuksen, jossa selvitettiin IT-sektorin ulkomaisia investointeja Suomessa ja Ruotsissa vuosina 2008 - 2013 sekä Ruotsin signaalitiedustelua koskevan lain mahdollisia vaikutuksia investointeihin Ruotsissa.

Arvioitaessa tiedonhankintaan tietoverkoissa liittyviä mahdollisia sääntelytarpeita kävi ilmi, että lainsäädännön kehittämistä olisi tarkasteltava laajemmin turvallisuusviranomaisten tiedustelutehtävää varten. Turvallisuusviranomaisten tiedonhankintakyvyn parantamisessa ei olisi ensisijaisesti kyse tietoturvan parantamisesta vaan viranomaisten paremmista mahdollisuuksista estää vakavia kansallista turvallisuutta uhkaavia tekoja. Työryhmä ei ole laatinut mietintöään hallituksen esityksen muotoon. Työryhmän mietinnössä arvioidaan turvallisuusviranomaisten tiedonhankinnan nykytilaa ja esitetään kehittämisehdotuksia tiedustelua koskeviksi tehtäviksi ja uusiksi toimivaltuuksiksi.

Työryhmän mietintöön on jätetty yksi eriävä mielipide sekä kaksi lausumaa, jotka ovat mietinnön liitteenä.

Saatuaan työnsä valmiiksi työryhmä luovuttaa kunnioittavasti mietintönsä puolustusministeriölle.

Helsingissä 14.1.2015

Hanna Nordström
Katriina Laitinen
Päivi Antikainen
Minna Hulkkonen
Timo Junttila
Mikko Kinnunen
Mika Lundelin
Sami Manninen
Kari Mäkinen
Jari Pajunen
Petri Syrjänen
Tomi Vuori
Martti J. Kari
Päivi Kaukoranta
Hannele Kerola
Petri Knape
Harri Ohra-aho
Antti Pelttari
Laura Tarhonen
Jenni Herrala
Kosti Honkanen
Minnamaria Nurminen
Jan Sjöblom

Sisällysluettelo

1. JOHDANTO

1.1 Taustaa

Yleinen kansainvälistymis- ja teknistymiskehitys on tärkeää ja välttämätöntä. Sen seurauksena Suomen turvallisuusympäristö on viime vuosina merkittävästi muuttunut ja monimutkaistunut. Sisäiseen ja ulkoiseen turvallisuuteen kohdistuvat uhat limittyvät toisiinsa entistä läheisemmin. Kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä maamme ulkopuolelle. Myös Suomen etuihin ulkomailla - mukaan lukien sellaiset kriisinhallintaoperaatiot, joihin Suomi osallistuu - kohdistuu enemmän ja vakavampia uhkia kuin aiemmin. Uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja niiden toiminnan ennakoiminen on vaikeutunut. Tietotekniikan kehitys on antanut pienillekin valtioille ja ei-valtiollisille toimijoille mahdollisuuden toimia tehokkaasti. Teknologian kehittyminen on mahdollistanut kansallista turvallisuutta vaarantavien tekojen toteuttamisen entistä lyhyemmällä valmisteluajalla ja vakavimmin seurauksin. Tietoverkossa toteutettavia hyökkäyksiä voidaan käyttää poliittisen ja taloudellisen painostuksen välineinä ja vakavassa kriisissä yhtenä vaikuttamiskeinona perinteisten sotilaallisten voimakeinojen ohella.

Uhkien kansainvälisestä luonteesta seuraa, että niiden taustalla olevat tahot ovat verkostoituneet eri maiden alueelle. Osalliset kommunikoivat yli valtiorajojen. Viestintäteknologian nopea kehitys on tehostanut ja helpottanut Suomelle uhan muodostavien tahojen välistä rajat ylittävää yhteydenpitoa ja verkostoitumista sekä nopeuttanut uhkien kansainvälistymistä. Siviilipuolen toimijoiden ohella myös modernien asevoimien johtaminen tukeutuu entistä enemmän yleiseen teleinfrastruktuuriin. Tietotekniikan nopean kehityksen ja alhaisempien kustannusten vuoksi asevoimat ottavat laajasti käyttöönsä sellaisia johtamis- ja viestintäjärjestelmiä, jotka on suunniteltu siviilitarpeita varten.

1.2 Työn kohteesta

Työryhmän tehtäväksi annettiin 13.12.2013 päivätyssä asettamiskirjeessä Suomen lainsäädännön kehittäminen erityisesti turvallisuusviranomaisten tiedonhankintaa koskevan sääntelyn osalta. Tavoitteena asettamiskirjeen mukaan oli se, että huolehdittaisiin paremmin kansallisesta turvallisuudesta erityisesti tietoverkoissa esiintyvien uhkien torjumiseksi.

Kyberturvallisuus oli esillä jo vuoden 2010 yhteiskunnan turvallisuusstrategiassa (valtioneuvoston periaatepäätös 16.12.2010). Kyberuhat tunnistettiin yhdeksi mahdolliseksi uhaksi ja tietojärjestelmiin tunkeutumisen todettiin tietyissä olosuhteissa voivan täyttää jopa sotilaallisen voimankäytön tunnusmerkit. Suomen kyberturvallisuusstrategiassa 2013 (valtioneuvoston periaatepäätös 24.1.2013) linjattiin visio, jonka mukaan Suomi on globaali edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallinnassa vuoteen 2016 mennessä.

Turvallisuusviranomaisten tiedonhankintakyvyn kehittämisessä ei tässä mietinnössä kysymys ole ensisijaisesti tietoturvan parantamisesta. Kysymys ei myöskään ole tavanomaisena pidettävästä verkkorikollisuuden torjunnasta vaan kansalliseen turvallisuuteen kohdistuvien vakavien uhkien havaitsemisesta ja tunnistamisesta sekä niiden torjunnan mahdollistamisesta. Tavoitteena on parantaa ylimmän valtionjohdon sekä turvallisuusviranomaisten tiedonsaan-

tia tällaisista uhista sekä Suomen turvallisuusympäristön kehittymisestä. Ylimmälle valtionjohdolle on voitava tuottaa riittävän ajoissa puolueetonta ja luotettavaa tietoa päätöksenteon tueksi siten, että sen avulla voidaan vaikuttaa ja varautua turvallisuusympäristössä esiintyviin uhkiin, riskeihin ja mahdollisuuksiin. Kansallisen turvallisuuden takaaminen tiedustelutietoa hankkimalla on tärkeää koko yhteiskunnalle ja myös elinkeinoelämän toimivuudelle. Sen vuoksi on tarkasteltava turvallisuusviranomaisten tiedonhankinnan nykytilaa ja kartoitettava siihen liittyviä kehittämisehdotuksia.

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

Poliisin tiedonhankintatoimivaltuudet ovat pakkokeino- ja poliisilain osalta vastikään uudistettu. Sen sijaan Suojelupoliisille ei ole säädetty erityisiä toimivaltuuksia tiedusteluun liittyvää tiedonhankintaa varten vaan sen tiedonhankintatoimivaltuudet perustuvat poliisia koskeviin yleislakeihin. Tiedonhankintatoimivaltuuksien käyttö on sidottu rikoksen ennalta estämiseen ja paljastamiseen. Mietinnössä painottuu tehtävänannon mukaisesti lainsäädännön kehittäminen erityisesti Suojelupoliisin tiedonhankintaa koskevan sääntelyn osalta.

Puolustusministeriön hallinnonalalle kuuluva puolustusvoimat vastaa Suomen sotilaallisesta puolustamisesta. Hallinnonalan tiedonhankintatarpeet liittyvät sotilasstrategisen tilannekuvan muodostamiseen ja ylläpitämiseen sekä kansainvälisten tehtävien turvallisuuteen. Puolustusvoimien tiedustelu- ja valvontajärjestelmä seuraa Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutoksia ja tuottaa tietoa vallitsevasta tilanteesta. Järjestelmä antaa valtionjohdolle ennakkovaroituksen sotilaallisten uhkien kehittymisestä, mikä mahdollistaa valtionjohdon oikea-aikaisen päätöksenteon ja yhteiskunnan elintärkeiden toimintojen johtamisen. Puolustusvoimien tiedustelullisesta tiedonhankinnasta eli sotilastiedustelusta ei ole nimenomaisia säännöksiä laissa. Puolustusvoimista annetun lain (551/2007) esitöiden mukaan tiedonhankinta on osa puolustusvoimien tehtäviä, mutta varsinaisista toimivaltuuksista siihen ei ole säädetty.

Suomessa ei ole säädetty siitä, mihin tiedustelutoiminnalla pyritään tai millaista tiedustelutoimintaa voidaan harjoittaa. Turvallisuusviranomaisten tiedonhankintatoimivaltuudet ovat puutteellisia toiminnan yhteiskunnalliseen merkittävyyteen nähden sekä muihin maihin verrattuna. Tilanne on epätyydyttävä, kun otetaan huomioon, että Suomen kansainvälisessä turvallisuustoimintaympäristössä on viime vuosina tapahtunut merkittäviä muutoksia.

Tässä mietinnössä kuvataan muuttuvaa turvallisuusympäristöä ja kansalliseen turvallisuuteen liittyvän tiedonhankinnan nykytilaa. Lisäksi mietinnössä kuvataan verrokkimaiden lainsäädäntöä, arvioidaan suomalaisen tiedustelulainsäädännön tarvetta, arvioidaan kehittämisehdotusten vaikutuksia sekä esitetään suuntaviivoja lainsäädännön kehittämiseksi.

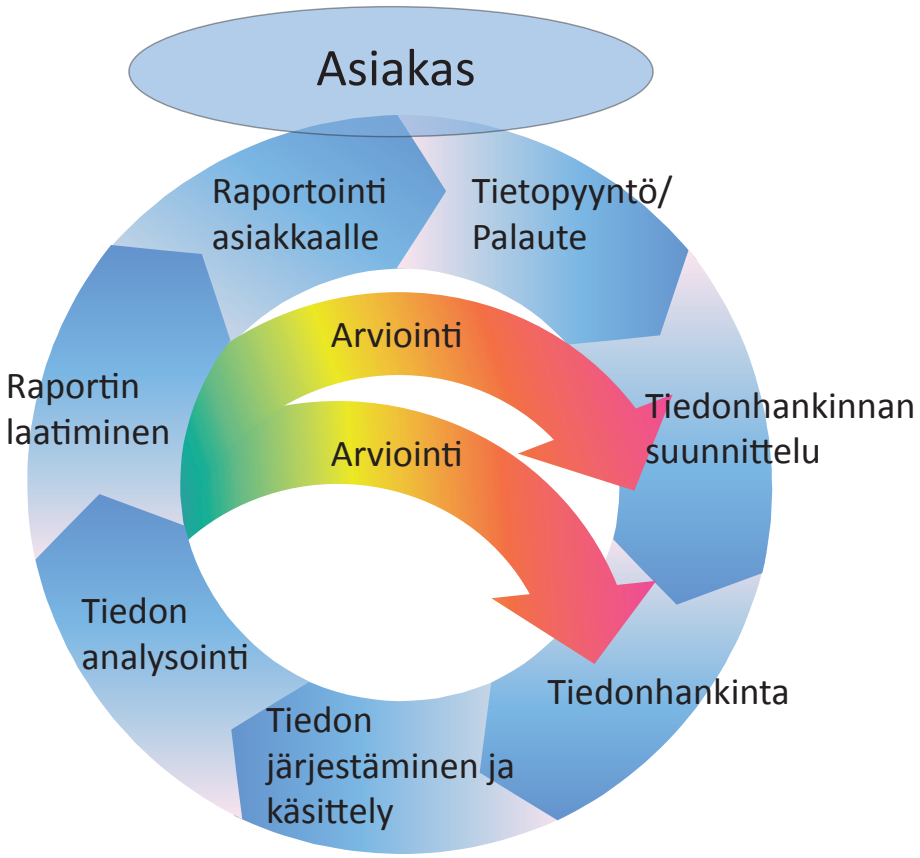
1.3 Käsitteitä

Koska tiedustelusta ei Suomessa ole säädetty laissa, on tiedustelua ja sen eri osa-alueita kuvaava käsitteistö vakiintumatonta ja tulkinnanvaraista. Tiedustelun ja sen lähi-ilmiöiden sekä niiden välisten yhteyksien ja erojen hahmottaminen edellyttää keskeisen terminologian tuntemusta.

Tiedustelun yleiskäsitteitä

Tiedustelu: 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.

Tiedustelusykli: Tiedustelusykli kuvaa asiakkaan ja tiedonhankkijan välistä suhdetta sekä tiedonhankinnan, raportoinnin ja analyysin prosesseja ja näiden välisiä vuorovaikutussuhteita. Syklin kuvaus on esitettynä alla:



Sotilastiedustelu: Sotilasviranomaisten suorittamaa tiedustelua, 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.

Siviilitiedustelu: Siviiliviranomaisen suorittamaa tiedustelua, jolla tuotetaan tietoa ylimmän valtionjohdon päätöksenteon ja oman operatiivisen toiminnan tueksi muista kuin sotilaallisen maanpuolustuksen alaan liittyvistä aiheista.

Turvallisuustiedustelu: Tiedustelua, jonka 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.

Rikostiedustelu: Lainvalvontaviranomaisen suorittamaa tiedustelua, jonka tarkoituksena on hankkia rikoksen estämisen, paljastamisen tai selvittämisen kannalta merkityksellistä tietoa rikollisista, rikoksista ja rikoksenteko-olosuhteista.

Keskeisiä tiedustelulajeja

Avointen lähteiden tiedustelu (OSINT, Open Source Intelligence): Julkisiin lähteisiin, kuten kirjallisuuteen, karttoihin, lehtiin ja julkisiin asiakirjoihin sekä Internet-sivustoihin kohdistuvaa tiedonhankintaa.

Signaalitiedustelu (SIGINT, Signals intelligence)***:*** Sotilas- tai siviiliviranomaisen suorittamaa sähköisiin signaaleihin kohdistuvaa tiedustelua. Signaalitiedustelun keskeisimmät kansainvälisesti vakiintuneet alakäsitteet ovat:

- *viestitiedustelu* (COMINT, Communications Intelligence), jolla tarkoitetaan sähköiseen viestintään kohdistuvaa elektronista tiedustelua
- *mittaustiedustelu* (ELINT, Electronic Intelligence), jolla tarkoitetaan sensori- ja navigointisignaaleihin sekä muihin teknisten laitteiden tuottamiin signaaleihin kohdistuvaa elektronista tiedustelua ja valvontaa. Mittaustiedustelu ei kohdistu henkilöiden väliseen viestintään

Henkilötiedustelu (HUMINT, Human Intelligence)***:*** Henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin perustuvaa tiedustelua. Henkilötiedustelua voidaan harjoittaa myös tietoverkon välityksellä.

Mietinnössä käytettäviä erikoiskäsitteitä

Mietintöä varten on muodostettu tietoliikennetiedustelun, ulkomaan tietojärjestelmätiedustelun ja ulkomaan henkilötiedustelun käsitteet.

Tietoliikennetiedustelulla tarkoitetaan Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua. Tietoliikennetiedustelu on signaalitiedustelua. Signaalitiedustelun alalajeista se voi pitää sisällään sekä viestitiedustelua että mittaustiedustelua.

Ulkomaan tietojärjestelmätiedustelulla tarkoitetaan ulkomailla sijaitsevassa tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin menetelmin tapahtuvaa tiedustelua.

Ulkomaan henkilötiedustelulla tarkoitetaan ulkomaita koskevaa tiedustelua, joka perustuu henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin.

Ulkomaan tietojärjestelmätiedustelussa ja ulkomaan henkilötiedustelussa on kyse ulkomailla tapahtuvasta toiminnasta, jolloin niistä voidaan käyttää yhteistä nimitystä *ulkomaan tiedustelu.* Tietoliikennetiedustelun ja ulkomaan tietojärjestelmätiedustelun yhteisenä nimittäjänä on puolestaan se, että ne molemmat tapahtuvat tietoverkoissa. Näin ollen niistä voidaan käyttää yhteistä yläkäsitettä ***tietoverkkotiedustelu***.

2. MUUTTUVA TURVALLISUUSYMPÄRISTÖ

2.1 Laaja-alainen turvallisuuskäsitys

Valtioneuvosto antoi 20.12.2012 eduskunnalle selonteon Suomen turvallisuus- ja puolustuspolitiikasta 2012 (jäljempänä selonteko 2012). Selonteko 2012 perustuu hallitusohjelman edellyttämällä tavalla laaja-alaiseen turvallisuuskäsitteeseen. Selonteon 2012 tarkastelujakso ulottuu 2020-luvulle ja se muodostaa perustan Suomen politiikan ohjaamiselle maan etujen ja tavoitteiden edistämiseksi. Selonteossa 2012 käsitellään korostuneesti kansainvälisessä toimintaympäristössä tapahtuvia kehityskulkuja sekä turvallisuuskysymysten globalisoitumisen merkitystä Suomen turvallisuudelle.

Selonteon 2012 mukaan modernit verkostoihin perustuvat yhteiskuntarakenteet ovat yhä riippuvaisempia kriittisestä infrastruktuurista, johon kuuluvat muun muassa liikenne, viestintä ja energiahuolto. Tämän lisäksi korostetaan, että keskinäisriippuvuuden lisääntyminen ja toimintaympäristön teknistyminen ovat tuoneet esiin myös yhteiskuntien uudenlaisen haavoittuvuuden. Lähes kaikki yhteiskunnan kriittiset toiminnot ja palvelut perustuvat teknisten, erityisesti sähköenergian ja tietoliikenteen varassa toimivien järjestelmien käyttöön, ja siten selonteon 2012 arvion mukaan myös yhteiskuntaan laajasti vaikuttavien häiriöiden riski kasvaa aiemmasta.

Selonteko 2012 korostaa, että Suomen on kaikissa olosuhteissa kyettävä takaamaan yhteiskunnan elintärkeiden toimintojen jatkuvuus. Rajat ylittävien uhkien torjuminen ja niihin varautuminen edellyttävät selonteon 2012 mukaan niin siviili- kuin sotilaallisten voimavarojen hyödyntämistä, laajan keinovalikoiman käyttämistä sekä sitä, että Suomi kehittää turvallisuusajatteluaan entistä kokonaisvaltaisempaan suuntaan.

Turvallisuusviranomaisten näkökulmasta haasteeseen vastaamisen ehtona on, että kansalliseen turvallisuuteen kohdistuvat rajat ylittävät uhat voidaan havaita ja tunnistaa riittävän varhaisessa vaiheessa.

2.2 Kansallinen turvallisuusympäristö

Yhteiskunnan tärkeimpänä suojattavana etuna voidaan pitää valtion itsemääräämisoikeutta, jolla tarkoitetaan valtion suvereenisuutta suhteissa ulkovaltioihin ja oikeutta muista riippumattomalla tavalla käyttää ylintä valtaa omien rajojensa sisällä. Muina keskeisinä suojattavina etuina voidaan pitää ainakin valtion johtamista, kansainvälistä toimintaa, puolustuskykyä, sisäistä turvallisuutta, talouden ja infrastruktuurin toimivuutta sekä väestön toimeentuloturvaa ja toimintakykyä.[1] Edellä mainittuihin etuihin kohdistuvien uhkien voidaan katsoa vaarantavan kansallista turvallisuutta. Uhkien torjunnasta vastaavia viranomaisia kutsutaan tässä mietinnössä kansallisen turvallisuuden viranomaisiksi.

Kansainvälistymisen myötä valtioiden ulkoisen ja sisäisen turvallisuuden välinen raja on muuttunut yhä häilyvämmäksi. Myös uhkien ja riskien rajaaminen alue- tai paikkasidonnaisiksi on entistä vaikeampaa taloudellisten, teknisten ja sosiaalisten järjestelmien valtiorajat ylittävästä luonteesta ja keskinäisriippuvuudesta johtuen. Suomen turvallisuutta uhkaavat vakavimmat tekijät liittyvät nykyisin usein Suomen ulkopuolisiin tapahtumiin. Siten

1 Yhteiskunnan turvallisuusstrategia s. 15

myös ulkomaista alkuperää olevan ja siellä syntyvän uhan seuraukset saattavat realisoitua Suomessa aiempaa herkemmin. Kansalliseen turvallisuuteen kohdistuville ulkoisille uhille on yhteistä se, että taustalla olevien valtiollisten ja ei-valtiollisten tahojen tunnistaminen ja erottaminen toisistaan on yhä vaikeampaa. Tästä johtuen uhkien ennakoiminen on aiempaa haasteellisempaa.

Uhat voidaan karkeasti jakaa siviililuonteisiin ja sotilaallisiin. Keskeisinä siviililuontoisina turvallisuusuhkina voidaan pitää ainakin kansainvälistä terrorismia, ulkovaltojen Suomeen ja sen etuihin kohdistamaa vakoilua, joukkotuhoaseiden ja kaksikäyttötuotteiden levittämispyrkimyksiä sekä sellaista kansainvälistä järjestäytynyttä rikollisuutta, joka pyrkii vaikuttamaan yhteiskunnalliseen päätöksentekoon tai soluttautumaan valtiorakenteisiin. Viime vuosina erityisesti tietoverkkoympäristössä tapahtuva rajat ylittävä vakoilu on noussut merkittäväksi uhaksi. Tällainen toiminta mahdollistaa suurten tietomäärien hankkimisen keskitetysti, mikä voi aiheuttaa korjaamatonta vahinkoa kohdevaltion turvallisuudelle ja sen eduille.

Myös sotilaallisten uhkien luonne on muuttunut. Perinteisen sotilaallisen toiminnan lisäksi modernit sotilasoperaatiot sisältävät erilaisia epäsymmetrisiä keinoja. Modernit sotilasoperaatiot alkavat ajallisesti jo rauhan aikaisilla painostus- ja disinformaatio-operaatioilla sekä tietoverkkohyökkäyksillä. Näin voidaan pyrkiä tietoisesti vaikuttamaan toisen valtion päätöksentekoon, jotta saavutettaisiin sellaisia strategisia päämääriä, joihin painostuksen kohteena oleva valtio ei muutoin suostuisi. Nykyisin painostus- ja disinformaatio-operaatiot kuuluvat valtioiden ulko- ja turvallisuuspolitiikan jatkumoon. Myös sotilasoperaatioissa ei-valtiollisten toimijoiden vaikuttamismahdollisuudet ovat kasvaneet teknologian kehittymisen ja yhteiskuntien lisääntyneen haavoittuvuuden myötä.

Poliittisen vaikuttamisen ja sodankäynnin raja hämärtyy käytettäessä poliittisia ja taloudellisia painostuskeinoja sekä disinformaatio-operaatioita. Laaja-alainenkaan voimankäyttö ei tulevaisuudessa välttämättä tarkoita kattavien maa-alueiden haltuunottoa ja hallintaa. Tavoitteet voidaan pyrkiä saavuttamaan voimankäytön yllätyksellisyydellä ja rajattujen alueiden nopealla valtaamisella.

2.3 Tietoteknistyvä viestintä

Informaatio sekä henkilöiden välinen kanssakäyminen on suureksi osin siirtynyt tietoverkkoihin. Yhteiskunta on muuttunut ympäristöksi, jossa lähes kaikki perinteiset palvelut ja toiminnot ovat tietoteknisesti ohjattuja tai kokonaan muutettu tietoverkoissa toimiviksi.

Tietoverkkojen toimintalogiikka eroaa vanhoista puhelinverkoista. Siinä missä puhelu varasi piirikytkentäisen puhelinverkon kokonaan soittajan ja vastaajan välille, internet-verkossa kulkee limittäin lukuisten yhteyksien liikennettä. Lähettävä laite jakaa viestin paketteihin, jotka vastaanottajalaite kokoaa jälleen kokonaiseksi viestiksi. Kaikki paketit eivät välttämättä kulje samaa reittiä vastaanottajalle, sillä verkko reitittää kunkin paketeista kulloisenakin hetkenä kustannustehokkainta reittiä. Kahden samassa maassa olevan osapuolen välinen tietoliikenne voi reitittyä ulkomaisen yhteyspisteen kautta.

Tietoverkkojen kehittyminen on mahdollistanut esimerkiksi pilvipalvelujen yleistymisen. Pilvipalvelussa on kyse tallennuspalvelusta, josta tieto on saatavilla miltä tahansa verkon laitteelta tiedon haltijan oikeuksin. Pilvipalveluun liittyvät palvelimet voivat sijaita yhden tai useamman valtion alueella. Käyttäjällä ei välttämättä ole mahdollisuutta selvittää, mihin tiedot fyysisesti tallentuvat.

Kansalliseen turvallisuuteen kohdistuviin turvallisuusuhkiin liittyy globalisoitumisen seurauksena yhä useammin Suomessa ja ulkomailla olevien henkilöiden välisiä kytköksiä ja siitä seuraavaa tarvetta molemminpuoliseen kommunikointiin. Sähköisiä välineitä käytetään hyväksi uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen viestinnässä, tehtäväksiannoissa, tehtävien toteuttamista koskevassa raportoinnissa, tekojen suunnittelussa, kohteita koskevassa tiedonhankinnassa, osallisten motivoinnissa ja radikalisoinnissa sekä uusien jäsenten rekrytoinnissa. Uhkien menestyksekkään torjumisen edellytyksenä on se, että kansallisesta turvallisuudesta vastaavat viranomaiset mahdollisimman varhaisessa vaiheessa saavat tiedon tällaisista yhteyksistä ja niiden puitteissa käsiteltävistä kansallista turvallisuutta vaarantavista seikoista. Varhaisvaiheen tiedonsaanti parantaa suomalaisen yhteiskunnan vastekykyä ja laajentaa sitä keinovalikoimaa, jonka avulla uhkien toteutuminen voidaan estää tai siihen varautua. Tietoverkoissa tapahtuvaan viestintään kohdistettu kansallisesta turvallisuudesta vastaavien viranomaisten tiedonhankinta on maailmanlaajuisesti ollut keskeisessä asemassa esimerkiksi terroritekojen estämisessä.

Tietoverkoissa tapahtuvan verkostoitumisen merkitys kansallista turvallisuutta uhkaavien toimijoiden keskuudessa tulee entisestään kasvamaan. Sosiaalisen median kehittyessä verkostoitumisen tavat monimuotoistuvat. Terroristi- ja muut radikaalijärjestöt panostavat omien modernien mediaorganisaatioiden kehittämiseen ja propagandan levittämiseen. Ne käyttävät yhä laajemmin sosiaalista mediaa, kuten pikaviestipalveluita, sekä ylläpitävät avoimia ja suljettuja keskustelufoorumeita. Nämä mahdollistavat sekä helppokäyttöisen kahden- ja monenvälisen viestinnän että toiminnan suunnittelun ja reaaliaikaisen koordinoinnin.

Selonteon 2012 arvion mukaan valtiotoimijoiden korostuvia sotilaallisia kykyjä ovat muun muassa tiedustelu- ja valvontajärjestelmät. Valtiot kehittävät miehittämättömiä laitteita tiedusteluun, valvontaan ja täsmäasejärjestelmien laveteiksi. Sotilaallinen toimintaympäristö on muuttunut. Ulkovaltojen sotilaalliset kohdejärjestelmät ovat muuttuneet entistä monimutkaisemmiksi, signaalien määrä on kasvanut merkittävästi, ja yhä suurempi osa tietoliikenteestä kulkee radiotien sijaan tietoliikennekaapeleissa. Toimintaympäristön muutoksen vuoksi Suomen sotilastiedustelun mahdollisuudet kerätä tiedustelutietoa ovat heikentyneet.

Tietotekniikan nopean kehityksen ja alhaisempien kustannusten vuoksi sotilastiedustelun kohteet ottavat käyttöön entistä enemmän siviilikäyttöön suunniteltuja kommunikaatiojärjestelmiä. Asevoimien johtaminen tukeutuu entistä enemmän yleiseen tietoverkkoinfrastruktuuriin. Tietoteknistymisen myötä tietojärjestelmissä käsiteltävän tiedon määrä on kasvanut merkittävästi ja suurin osa tiedosta on nykyisin digitaalisessa muodossa. Nykyisin tiedustelun tulisi kohdistua digitaaliseen tietoon ollakseen tehokasta tietoteknistyneessä toimintaympäristössä.

2.4 Kansalliseen turvallisuuteen kohdistuvat tietoverkkouhat

Kansalliselle turvallisuudelle uhan muodostavat tahot käyttävät tietoverkkoja paitsi viestinnän myös uhkien toteuttamisen välineenä.

Suomen kyberturvallisuusstrategiassa käsiteltyjä valtion elinkelpoisuutta tai valtion keskeisiä turvallisuusetuja vaarantavia uhkia ovat ennen kaikkea kybervakoilu, kyberterrorismi ja kyberoperaatiot. Viimeksi mainittu käsite pitää sisällään sekä painostuksen, kyberympäristössä toteutuvan sotaa alemman tason konfliktin että sotaan liittyvät kyberoperaatiot.

Kybervakoilulla hankitaan valtio- tai yrityssalaisuuksien tapaista luokiteltua tai sensitiivistä tietoa tietojärjestelmistä.[2] Kybertoimintaympäristössä tapahtuva vakoilu voi jatkua jopa vuosia huomaamatta. Turvallisuusviranomaisten arvion mukaan useat ulkovallat pyrkivät kohdistamaan laajaa ja teknisesti edistynyttä kybervakoilua Suomen valtionhallintoon ja kansantaloudellista merkitystä omaaviin yrityksiin. Kybervakoilussa tekovälineenä ei ole tavallinen kaupallisella virustorjuntaohjelmalla havaittava haittaohjelma, vaan teknisesti kehittynyt ja monipuolinen verkkohyökkäystyökalu. Työkalun ensimmäisenä tehtävänä on verkon tietyn osan haltuunotto ja seuraavana tehtävänä kehittyneimpien hyökkäyksellisten vakoilu- ja haittaohjelmien asentaminen. Vakoiluoperaatio on ennakkoon tarkoin suunniteltu ja sillä on täsmällinen operatiivinen tavoite kerätä tietoa esimerkiksi kohdevaltion ulko- ja turvallisuuspolitiikkaan, talouteen ja teollisuuteen liittyvistä seikoista. Tiedusteluohjelmien lisäksi voidaan tietojärjestelmiin toimittaa haittaohjelmia, jotka aktivoituvat kriisin alkaessa. Uudet teknologiat luovat uusia mahdollisuuksia kyberoperaatioilla käytävään sodankäyntiin, jonka vaikutukset kohdistetaan koko yhteiskuntaan, ei ainoastaan asevoimiin.

Kybervakoilun ja -operaatioiden merkitys kasvaa tulevina vuosina entisestään. Syitä tälle ovat mahdollisuus toteuttaa kybertoimintaympäristössä tekoja alhaisin kustannuksin, suojautumisen vaikeus ja kalleus sekä vähäinen kiinnijäämisriski. Myös kaikki Suomen turvallisuusympäristön kehityksen kannalta olennaiset ulkovallat panostavat määrätietoisesti ja mittavasti offensiivisen kyberkapasiteettinsa rakentamiseen. Esimerkkeinä valtioihin kohdistuneesta kyberoperaatioista voidaan mainita muun muassa Ukrainan (2014), Georgian (2008) ja Viron (2007) suljettuihin viranomaisverkkoihin kohdistetut verkkohyökkäykset, jotka ovat osoittautuneet hyvin organisoiduiksi ja suunnitelluiksi operaatioiksi, joiden taustalla arvioidaan olevan valtiotoimija tai siihen hyvin läheisesti kytkeytyvät tahot.

Terroristisessa tarkoituksessa toteutettujen kyberhyökkäysten uhka Suomea kohtaan on yhä rajallinen. Tilanne voi kuitenkin muuttua nopeasti kansainvälisessä toimintaympäristössä tapahtuvien kehitysten seurauksena. Eräät kansainväliset terroristiryhmät ovat pyrkineet kehittämään kyberhyökkäyskykyään ja useiden ryhmien osalta on viitteitä pyrkimyksistä sekä oman osaamisen kehittämiseen että ulkoistamiseen (ostopalveluina toteutettavat täsmäiskut). Mahdollisina tekotapoina tulevat kyseeseen kriittisten verkkopalveluiden saatavuutta haittaavat palvelunestohyökkäykset sekä SCADA-valvomojärjestelmän kautta tehdyt tuhotyöt, jotka pahimmillaan aiheuttavat mittavia henkilö- ja omaisuusvahinkoja.

2 Esimerkkeinä kyberympäristön kautta tapahtuvasta tiedonhankinnasta ja vaikuttamisesta voidaan mainita Iranin ydinohjelmaan kohdistunut Stuxnet-haittaohjelma sekä Ukrainan, usean Euroopan valtion että Yhdysvaltojen puolustushallintojen verkoista löydetyt Red October sekä Agent.btz, -lataustiedostot sekä etenkin jälkimmäisestä edelleen kehitetyt Snake, Turla, Uroboros –vakoiluohjelmat.

2.5 Tietoverkkorikollisuudesta

Tietoverkkorikollisuuden aiheuttamat uhat ovat olleet vahvassa kasvussa viimeisten vuosien aikana. Rikokset voivat kohdistua yksityisiin kansalaisiin, yrityksiin ja muihin yhteisöihin sekä koko yhteiskuntaan. Tämä näkyy poliisin tietoon tulleiden tietoverkkorikosten osalta sekä niiden määrän lisääntymisenä että tekojen muuttumisena yhä vahingollisemmaksi. YK:n alaisen UNODC:n mukaan kansalaiset uhriutuvat todennäköisemmin tietoverkkorikoksiin kuin perinteisiin rikoksiin.

Tietoverkkorikollisuus on suurelta osin piilorikollisuutta, joka ei tule poliisin tietoon ja usein asianomistajatkaan eivät havaitse tapahtumaa. Jos he havaitsevat sen, siihen saattaa kulua kauan ja usein silloinkin he käsittelevät sen ilmoittamatta asiaa viranomaisille tai edes mahdollisille asiakkailleen.

Tietoverkkorikollisuus on kansainvälistä. Rikostentekijät toimivat usein erilaisissa ryhmissä, jotka muodostuvat tarvittavan osaamisen ja resurssien omaamisen kautta. Tekijät eivät internetissä tunne toistensa todellista identiteettiä. He toimivat kukin omassa maassaan käyttäen rikosten tekemiseen resursseja ja palveluja eri maista ja kohdistaen hyökkäyksen useisiin maihin samanaikaisesti. Kohteena voivat olla yhteiskunnan kannalta kriittiset järjestelmät, kuten esimerkiksi kansainväliset pankki- ja maksuliikennejärjestelmät.

Vakavassa rikosepäilyssä ei välttämättä aina ole ollut kyse tahallisesta rikoksesta vaan ohjelmistovirheestä, laiteviasta, väärin konfiguroidusta laitteesta tai muusta inhimillisestä virheestä, tai välttämättä ei ole heti voitu todeta rikoksen taustalla olevaa tekijätahoa tai motiivia.

3. TIEDONHANKINNAN SEKÄ TIETOTURVAUHKIEN TORJUNNAN NYKYTILA

3.1 Kansallisesta turvallisuudesta vastaavien viranomaisten lakisääteiset tehtävät

3.1.1 Poliisin tehtävistä ja toimivaltuuksista

Poliisin tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisi toimii turvallisuuden ylläpitämiseksi yhteistyössä muiden viranomaisten sekä yhteisöjen ja asukkaiden kanssa ja huolehtii tehtäviinsä kuuluvasta kansainvälisestä yhteistyöstä. Poliisi suorittaa lisäksi lupahallintoon liittyvät ja muut sille laissa erikseen säädetyt tehtävät sekä antaa jokaiselle tehtäväpiiriinsä kuuluvaa apua. Jos on perusteltua syytä olettaa henkilön kadonneen tai joutuneen onnettomuuden uhriksi, poliisin on ryhdyttävä tarpeellisiin toimenpiteisiin henkilön löytämiseksi.

Poliisin toimivaltuuksista hankkia rikosten estämiseksi ja paljastamiseksi tarvittavaa tietoa säädetään poliisilaissa. Poliisin toimivaltuuksista hankkia rikosten selvittämiseksi tarvittavaa tietoa säädetään puolestaan pakkokeino- ja esitutkintalaeissa. Vuonna 2014 voimaan tulleessa poliisi- ja pakkokeinolakien kokonaisuudistuksessa lakien sääntelyä eri tiedonhankintatoimivaltuuksien lajeista yhdenmukaistettiin, mistä johtuen molemmat lait sisältävät suurin piirtein samoja tiedonhankintakeinoja koskevat säännökset. Keskeisenä erona on se tarkoitus, jota varten tiedonhankintakeinoja käytetään: yhtäältä rikoksen estämisen ja paljastamisen tarkoituksessa (poliisilaki) ja toisaalta rikoksen selvittämisen tarkoituksessa (pakkokeinolaki).

Poliisilain 4 luvussa säädetään poliisin tiedonsaantioikeuksista. Luvun 2 §:n 1 momentin mukaan poliisilla on oikeus saada viranomaiselta ja julkista tehtävää hoitamaan asetetulta yhteisöltä poliisille kuuluvan tehtävän suorittamiseksi tarpeelliset tiedot ja asiakirjat salassapitovelvollisuuden estämättä, jollei niiden antamista poliisille tai ole laissa nimenomaisesti kielletty tai rajoitettu. Saman luvun 3 §:n 1 momentin mukaan poliisilla on oikeus saada rikoksen estämiseksi tai selvittämiseksi tarvittavia tietoja yritys-, pankki- tai vakuutussalaisuuden estämättä. Säännöksen 2 momentin mukaan poliisilla on yksittäistapauksessa oikeus saada teleyritykseltä ja yhteisötilaajalta yhteystiedot teleosoitteesta, jota ei mainita julkisessa luettelossa taikka teleosoitteen tai telepäätelaitteen yksilöivät tiedot, jos tiedot ovat tarpeen poliisille kuuluvan tehtävän suorittamiseksi.

3.1.1.1 Suojelupoliisin tehtävät

Poliisin organisaatiossa kansalliseen turvallisuuteen kohdistuvien uhkien torjunnasta vastaa valtakunnallisena yksikkönä toimiva Suojelupoliisi. Poliisin hallinnosta annetun lain 10 §:n mukaan Suojelupoliisin tehtävänä on 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. Poliisihallitus määrää tarkemmin ne asiaryhmät, jotka kuuluvat Suojelupoliisin tutkittaviksi.

Poliisin hallintolakia koskevan hallituksen esityksen (HE 155/1991 vp) mukaan säännöksen kirjoittamistavassa on pyritty ottamaan huomioon ennalta estävän toiminnan korostunut

merkitys Suojelupoliisin tehtäväalueella. Esitöiden mukaan Suojelupoliisin työssä on erityisen keskeisellä sijalla valtakunnan turvallisuutta vaarantavien tekojen estäminen ennakolta, kun taas tutkinnan kohdistaminen jo tapahtuneeseen turvallisuusetujen loukkaamiseen on yleensä osoitus ennalta estävän toiminnan jonkinasteisesta epäonnistumisesta.

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

Poliisin hallintolain 10 § määrittelee Suojelupoliisin toimialan luettelemalla ne oikeushyvät - sisäinen turvallisuus, ulkoinen turvallisuus, valtiojärjestys, yhteiskuntajärjestys -, joiden suojeleminen kuuluu Suojelupoliisille. Niitä konkreettisia ilmiöitä ja turvallisuusuhkia, joiden torjuminen kuuluu Suojelupoliisille, ei mainita laissa. Määrittelemällä tehtävät oikeushyvälähtöisesti on ilmeisesti haluttu varmistaa Suojelupoliisin valtion keskeisiä turvallisuusetuja suojelevan toiminnan mukautettavuus muuttuviin olosuhteisiin sekä viraston torjuntatoimialan yleisyys.

Suojelupoliisin toimiala konkretisoidaan määräajoin uudistettavassa Poliisihallituksen määräyksessä 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

Lisäksi Suojelupoliisin tehtävänä määräyksen mukaan on muun muassa:

- joukkotuhoaseiden 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
- valtiovierailuihin ja muihin mittaviin kokouksiin liittyvä uhka-arviointi
- toimialaansa kuuluvan turvallisuustiedustelun suorittaminen
- eräiden toimialaansa kuuluvien rikosten tutkiminen

Suojelupoliisille säädettyjen tehtävien hoitaminen pitää sisällään aktiivisen Suomen turvallisuusympäristön seurannan, turvallisuusuhkia koskevan ennakoivan tiedonhankinnan ja hankittujen tietojen analysoinnin. Analysoitua tietoa tuotetaan ensisijaisesti ylimmän valtiojohdon tarpeisiin. Poliisin hallinnosta annetun lain 4 a § säätää Suojelupoliisille velvollisuuden ilmoittaa tehtäviinsä kuuluvista yhteiskunnallisesti merkittävistä asioista suoraan sisäministerille ja poliisiylijohtajalle. Säännöksen perusteluiden mukaan Suojelupoliisilla on velvollisuus informoida myös tasavallan presidenttiä, pääministeriä ja ulkoasiainministeriä ottaen huomioon heille säädetyt ulko- ja turvallisuuspoliittiset tehtävät. Lisäksi Suojelupoliisi informoi eduskunnan perustuslaki-, hallinto- ja ulkoasiainvaliokuntia Suomen turvallisuustilanteen kehittymisestä.

Turvallisuusuhkien monimutkaistuessa ja kansainvälistyessä tarvitaan yhä enemmän ja yhä laadukkaampaa tiedustelutietoa poliittisen päätöksenteon tueksi. Ylintä valtionjohtoa varten

laadittujen Suomen turvallisuustilannetta kuvaavien Suojelupoliisin raporttien määrä on kymmenkertaistunut vuoden 2008 jälkeen.

Sisäministeriössä on parhaillaan vireillä Suojelupoliisin hallinnollisen aseman muuttaminen siten, että Suojelupoliisi siirrettäisiin Poliisihallituksen alaisuudesta suoraan sisäministeriön alaiseksi poliisiyksiköksi. Asiaa koskevan hallituksen esitysluonnoksen mukaan muutoksella muun muassa vahvistettaisiin poliittisen tahon Suojelupoliisin toimintaan kohdistamaa strategista ohjausta ja selkeytettäisiin Suojelupoliisin asemaa sekä kotimaisessa viranomaiskentässä että yhä tärkeämmässä kansainvälisessä turvallisuus- ja tiedustelupalveluiden välisessä yhteistyössä. Muutoksella kavennettaisiin Suojelupoliisin hallinnollista etäisyyttä turvallisuuspoliittisiin päätöksentekijöihin ja selkeytettäisiin Suojelupoliisin suoria yhteistyö- ja raportointisuhteita. Tavoitteena on lisätä valtiojohdon mahdollisuuksia vaikuttaa Suojelupoliisin tiedonhankinnan suuntaamiseen ja siten parantaa Suojelupoliisin kykyä tuottaa Suomen sisäistä turvallisuutta ja ulko- ja turvallisuuspoliittista päätöksentekoa palvelevaa tietoa.

Palvelukyvyn parantamista koskeva tavoite liittyy kiinteästi kysymykseen pysyvän ministeriötason ohjaus- ja yhteensovittamismekanismin muodostamisesta Suojelupoliisin tiedonhankinnan suuntaamiseksi. Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittänyt työryhmä teki 24 päivänä syyskuuta 2014 sisäministerille luovuttamassaan loppuraportissa (sisäministeriön julkaisu 28/2014) ehdotuksen tällaisen mekanismin muodostamisesta. Ehdotuksen mukaan Suojelupoliisin toiminnalle asetettaisiin vuosittain tiedonhankintaprioriteetit viraston toimintaa ohjaavan ministeriön johdolla. Ennen prioriteettien vahvistamista ne tulisi käsitellä valmistelevasti ja yhteen sovittavasti esimerkiksi valtioneuvoston ulko- ja turvallisuuspoliittisessa ministerivaliokunnassa sekä niistä tulisi antaa selvitys eduskunnan asianomaisille valiokunnille. Mekanismin toteuttamisen ei ole arvioitu edellyttävän laintasoisia säädösmuutoksia.

3.1.2 Puolustusvoimien tehtävät

Puolustusvoimista annetun lain 2 §:n mukaan puolustusvoimien tehtäviin kuuluu Suomen sotilaallinen puolustaminen, muiden viranomaisten tukeminen sekä osallistuminen sotilaalliseen kriisinhallintaan. Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan a alakohdan mukaan Suomen sotilaalliseen puolustamiseen kuuluu maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen. Puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan b alakohdan mukaan Suomen sotilaalliseen puolustamiseen kuuluu lisäksi kansan elinmahdollisuuksien, perusoikeuksien ja valtionjohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen.

Valtion täysivaltaisuuteen kuuluu sen alueellinen koskemattomuus. Aluevalvontalakiin (755/2000) sisältyvät säännökset Suomen alueellisen koskemattomuuden valvonnasta ja turvaamisesta. Aluevalvonnalla ehkäistään tai paljastetaan ja selvitetään aluerikkomukset ja alueloukkaukset. Lain nojalla on annettu tarkempia säännöksiä aluevalvonnasta annetussa valtioneuvoston asetuksella (971/2000).

Aluevalvontalaissa vieraan valtion vihamielinen toiminta määritellään 34 §:n 4 ja 5 kohdassa muun muassa seuraavasti:

> ”4) vieraan valtion Suomen alueella oleviin, valtakunnan turvallisuuden kannalta tärkeisiin kohteisiin oikeudettomasti kohdistamaa tiedustelua ja elektronista häirintää;
>
> 5) vieraan valtion aluevalvontatehtävässä olevaan suomalaiseen valtionilma-alukseen tai valtionalukseen oikeudettomasti kohdistamaa elektronista häirintää.”

Puolustusjärjestelmän tehtävänä on muodostaa ja ylläpitää päätöksenteon edellyttämää sotilasstrategista tilannekuvaa. Sotilastiedustelu osana puolustusvoimien tehtäviä mainitaan puolustusvoimista annetun lain 2 §:n yksityiskohtaisissa perusteluissa (HE 264/2006 vp, s. 17 -18). Lain 2 §:n 1 momentin 1 kohdan b alakohdan perusteluissa todetaan, että ”puolustusvoimat turvaa osaltaan kansan elinmahdollisuudet ja perusoikeudet, valtionjohdon toimintavapauden ja laillisen yhteiskuntajärjestyksen. - - Jotta nämä voidaan turvata, puolustuskyvyn on oltava riittävä ja puolustusvoimien tulee ennalta ehkäistä sotilaallisia uhkia sekä torjua maahan kohdistuvat hyökkäykset.” Lisäksi lain 2 §:n perustelutekstissä on todettu, että ”sotilasstrategisen tilannekuvan muodostamiseksi ja ylläpitämiseksi tiedustelu- ja valvontajärjestelmä seuraa Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta. Järjestelmä antaa ennakkovaroituksen sotilaallisten uhkien kehittymisestä, jotta voidaan käynnistää tarvittavat vastatoimet”. Sotilastiedustelun kohteena ovat pääosin valtiotoimijat, erityisesti ulkomaalaiset sotilasorganisaatiot.

Sotilastiedustelun toimivaltuuksista ei kuitenkaan ole säädetty. Puolustusvoimien vastatiedustelutehtävästä eli maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvästä rikosten ennalta estämisestä ja paljastamisesta Suomen alueella sen sijaan on säädetty sotilaskurinpidosta ja rikostorjunnasta annetussa laissa (255/2014).

3.2 Suojelupoliisin ja puolustusvoimien tiedonhankinta kotimaassa

3.2.1 Suojelupoliisin tiedonhankinta kotimaassa

3.2.1.1 Yleistä

Suojelupoliisin tärkeimpänä tehtävänä on ennalta estää ja paljastaa terrorismiin, laittomaan tiedustelutoimintaan, joukkotuhoaseiden levittämiseen ja ääriliikkeisiin sekä valtion turvallisuutta vaarantavaan järjestäytyneeseen rikollisuuteen kytkeytyviä hankkeita ja rikoksia sekä rajatussa määrin myös suorittaa edellä mainittuihin ilmiöihin liittyvien rikosten tutkintaa. Tehtävän suorittaminen edellyttää, että Suojelupoliisi kykenee hankkimaan tällaisista hankkeista ja rikoksista tietoa.

Julkisesti saatavilla olevan tiedon hankkiminen ei yleensä edellytä perustakseen erikseen säädettyä viranomaistoimivaltuutta. Koska Suojelupoliisin torjuttavina olevat hankkeet ja rikokset pyritään valmistelemaan julkisuudelta salassa, ei torjuntatoimia voida käytännössä perustaa julkisesti saatavilla oleviin tietoihin. Keskeisessä roolissa on näin ollen toiminta, joka tähtää muiden kuin julkisesti saatavilla olevien tietojen hankkimiseen. Ollakseen tehokasta on tiedonhankinta lisäksi suoritettava salassa sen kohteelta.

Suojelupoliisille ei ole säädetty erityisiä toimivaltuuksia valtion turvallisuuteen liittyvän uhkatiedon hankkimista varten. Suojelupoliisi on poliisiviranomainen, joka toiminnassaan käyttää poliisille säädettyjä tiedonhankinta- ja muita toimivaltuuksia.

Suojelupoliisin käytännön toiminnassa keskeisiä ovat poliisilaissa säädetyt salaiset tiedonhankintakeinot rikoksen estämiseksi ja paljastamiseksi. Rikosten selvittämistehtävät rajoittuvat Suojelupoliisin osalta käytännössä lähinnä laittomaan tiedustelutoimintaan liittyvien rikosten tutkintaan. Suojelupoliisi toimittaa esitutkinnan vain harvoin.

3.2.1.2 Rikoksen ennalta estämisen ja paljastamisen käsitteet

Poliisilain 5 luvun 1 §:n 2 momentin mukaan *rikoksen estämisellä* tarkoitetaan toimenpiteitä, joiden tavoitteena on estää rikos, sen yritys tai valmistelu, kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan perustellusti olettaa hänen syyllistyvän rikokseen, taikka keskeyttää jo aloitetun rikoksen tekeminen tai rajoittaa siitä välittömästi aiheutuvaa vahinkoa tai vaaraa. Henkilön toiminnasta tehdyillä havainnoilla tai siitä muutoin saaduilla tiedoilla tarkoitetaan välittömästi henkilön omasta toiminnasta tehtyjä havaintoja ja ulkopuolisen henkilön, esimerkiksi tietolähteen antamia vihjetietoja ja muuta välillistä selvitystä. Havaintoihin ja muuten saatuihin tietoihin kuuluvat myös muun muassa rikostiedustelutiedot, tarkkailuhavainnot, muut vihjetiedot ja rikosanalyysilla tiedoista tehtävät johtopäätökset. Edellytyksenä rikoksen estämiseksi säädetyn tiedonhankintakeinon käytölle on, että tällaisten tietojen perusteella on muodostunut perusteltu oletus henkilön syyllistymisestä rikokseen (HE 224/2010 vp, s. 89).

Poliisilain mukainen rikoksen estäminen on varhaisvaiheen ennakollista viranomaistoimintaa. Poliisilain 5 luvun 1 §:n 2 momentin mukaan rikoksen estäminen kattaa toimenpiteet, joiden tarkoituksena on estää rikoksen yritys ja valmistelu. Valmistelun estämisellä tarkoitetaan rangaistavan teon valmistelun estämistä myös silloin, kun itse valmistelua ei ole kriminalisoitu.

Poliisilain 5 luvun 1 §:n 3 momentin mukaan *rikoksen paljastamisella* tarkoitetaan toimenpiteitä, joiden tavoitteena on selvittää, onko esitutkinnan aloittamiselle esitutkintalain 3 luvun 3 §:n 1 momentissa tarkoitettua perustetta[3], kun henkilön toiminnasta tehtyjen havaintojen tai siitä muuten saatujen tietojen vuoksi voidaan olettaa, että rikos on tehty. Rikoksen paljastamisen käsite viittaa rikoksen estämisen ja selvittämisen väliin jäävään harmaaseen alueeseen. Kyse ei ole rikoksen selvittämisestä, koska esitutkinnan käynnistämisen edellytykset puuttuvat, eikä myöskään rikoksen estämisestä, koska rikos oletetaan jo tehdyksi. Rikoksen paljastamisesta on kyse esimerkiksi tilanteessa jossa vihjetiedon mukaan rikos olisi jo tehty, mutta konkreettista perustetta epäilylle ei vielä ole eli esitutkintalain mukainen syytä epäillä -kynnys ei ole ylittynyt. (HE 224/2010 vp, s. 90).

3.2.1.3 Salaisten tiedonhankintakeinojen käytön edellytykset

Poliisilain 5 luku sisältää säännökset niistä tiedonhankintakeinoista, joita poliisi - Suojelupoliisi mukaan lukien - saa käyttää tietojen hankkimiseksi toimenpiteen kohdehenkilöltä salassa.

Näitä keinoja ovat:

- telekuuntelu (poliisilaki 5 luvun 5 §)
- tietojen hankkiminen telekuuntelun sijasta (poliisilaki 5:6)

3 Esitutkintalain 3 luvun 3 §:n 1 momentin mukaan esitutkintaviranomaisen on toimitettava esitutkinta, kun sille tehdyn ilmoituksen perusteella tai muuten on syytä epäillä, että rikos on tehty.

- televalvonta (poliisilaki 5:8)
- televalvonta teleosoitteen tai telepäätelaitteen haltijan suostumuksella (poliisilaki 5:9)
- tukiasematietojen hankkiminen (poliisilaki 5:11)
- suunnitelmallinen tarkkailu (poliisilaki 5:13)
- peitelty tiedonhankinta (poliisilaki 5:15)
- tekninen kuuntelu (poliisilaki 5:17)
- tekninen katselu (poliisilaki 5:19)
- tekninen seuranta (poliisilaki 5:21)
- tekninen laitetarkkailu (poliisilaki 5:23)
- teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen (poliisilaki 5:25)
- peitetoiminta (poliisilaki 5:28)
- valeosto (poliisilaki 5:35)
- tietolähdetoiminta ja tietolähteen ohjattu käyttö (poliisilaki 5:40)
- valvottu läpilasku (poliisilaki 5:43)

Salaisia tiedonhankintakeinoja voidaan käyttötapansa ja -tarkoituksensa mukaan ryhmitellä eri tavoin. Jotkut niistä ovat kohdehenkilön viestintään kohdistuvia teknisiä tiedonhankintakeinoja, kun taas joitakin voidaan luonnehtia henkilötiedonhankinnan keinoiksi. Henkilötiedonhankintakeinot voidaan edelleen ryhmitellä esimerkiksi sen mukaan, edellyttääkö tiedonhankinta keinon käyttäjän ja kohdehenkilön välistä suoraa vuorovaikutussuhdetta ja siihen sisältyvää kohdehenkilön harhauttamista vai ei. Peitelty tiedonhankinta, peitetoiminta ja valeosto perustuvat tällaiseen harhauttavaan suoraan vuorovaikutussuhteeseen, kun taas tietolähdetoiminnassa ja tietolähteen ohjatussa käytössä kohdehenkilöä koskevia tietoja hankitaan välikäden kautta. Suunnitelmallinen tarkkailu perustuu kohdehenkilön käyttäytymisen aistinvaraiseen havainnointiin.

Salaisten tiedonhankintakeinojen käytön yleisenä edellytyksenä poliisilain 5 luvun 2 §:n 1 momentin mukaan on, että sillä *voidaan olettaa saatavan* rikoksen estämiseksi tai paljastamiseksi taikka vaaran torjumiseksi *tarvittavia* tietoja. Telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, suunnitelmallisen tarkkailun, teknisen kuuntelun, henkilön teknisen seurannan, teknisen laitetarkkailun, peitetoiminnan, valeoston, tietolähteen ohjatun käytön ja valvotun läpilaskun yleisenä lisäedellytyksenä saman pykälän 2 momentin mukaan on, että niillä *voidaan olettaa olevan erittäin tärkeä merkitys* rikoksen estämiselle tai paljastamiselle. Peitetoiminnan ja valeoston käyttäminen edellyttää lisäksi, että käyttö *on välttämätöntä* rikoksen estämiseksi tai paljastamiseksi.

Eri tiedonhankintakeinojen käytölle on poliisilaissa asetettu niin sanottuja yleisiä edellytyksiä ja erityisiä edellytyksiä. Salaisten tiedonhankintakeinojen käytön erityisinä edellytyksinä ovat ennen kaikkea ne yksilöidyt rikokset, joiden estämiseksi kutakin keinoa voidaan käyttää. Eri tiedonhankintakeinoja koskevissa säännöksissä on myös voitu asettaa muita erityisiä edellytyksiä. Kokoavasti voidaan todeta, että Suojelupoliisi voi likimain kattavasti käyttää poliisilain 5 luvussa säädettyjä salaisia tiedonhankintakeinoja rikoslain 34 a luvussa rangaistaviksi säädettyjen terrorismirikosten ja rikoslain 12 luvussa rangaistaviksi säädettyjen laittomaan tiedustelutoimintaan liittyvien rikosten estämiseksi. Joukkotuhoaseiden ja kaksikäyttötuotteiden levittämiseen tähtäävien rikosten samoin kuin järjestäytyneen rikollisryhmän toimintaan liittyvien valtion turvallisuutta vaarantavien rikosten estämisen kohdalla tilanne on moniulotteisempi ja tulkinnanvaraisempi.

Rikoksen paljastamiseen yllä mainittuja salaisia tiedonhankintakeinoja voidaan käyttää vain, jos kysymyksessä on laissa tarkemmin säädetty maanpetos- tai terrorismirikos. Rikosten

paljastamisen yhteydessä ei sovelleta salaisten tiedonhankintakeinojen keinokohtaisissa säännöksissä säädettyjä erityisiä edellytyksiä (HE 224/2010 vp, s. 92).

Salaisten tiedonhankintakeinojen valintaa ja käyttöä ohjaavat poliisilain 1 luvussa säädetyt yleiset periaatteet, kuten perus- ja ihmisoikeuksien kunnioittamisen periaate, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate.

Salaisten tiedonhankintakeinojen yhteinen piirre on se, että ne on määritelty henkilö- ja rikoslähtöisesti. Niitä voidaan kohdistaa vain sellaiseen henkilöön tai käyttää hankittaessa tietoa vain sellaisen henkilön toiminnasta, jonka voidaan perustellusti olettaa tulevaisuudessa syyllistyvän tai jo syyllistyneen tietyn vakavuusasteen rikokseen tai sellaisen valmisteluun. Jos tällaista tiettyyn henkilöön liittyvää rikostorjunnallista perustetta ei ole olemassa, ei poliisilain mukaisen salaisen tiedonhankintakeinon käyttö ole mahdollista. Muun tiedustelutiedon hankinnan on näin ollen perustuttava avointen lähteiden seurantaan, poliisin niin sanottuun yleisvalvontaan sekä tietoihin, jotka Suojelupoliisi yhteistyöverkostonsa kautta saa muilta viranomaisilta ja yksityisiltä yhteisöiltä.

3.2.1.4 Hankkeiden torjunta

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

Suojelupoliisin hallinnollista asemaa ja tulosohjausta sekä valvonnan kehittämistä selvittänyt työryhmä käsitteli 24.9.2014 sisäministerille luovuttamassa loppuraportissaan kysymystä Suojelupoliisin tiedonhankintatoimivaltuuksien ulottamisesta hankkeiden torjuntaan. Työryhmän loppuraportin mukaan Suojelupoliisille olisi harkittava uusia tiedustelullisia toimivaltuuksia, jotta se kykenee vastaamaan toimintaympäristönsä muutokseen. Kyse olisi valtakunnan turvallisuutta vaarantavien hankkeiden torjumiseksi tarpeellisten tietojen hankkimisesta tietolähteinä toimivilta henkilöiltä ja tietoverkoista, vaikka hankkeet eivät olekaan edenneet estettävän, paljastettavan tai selvitettävän rikoksen asteelle. Työryhmän mukaan asiaa harkittaessa on selvitettävä tarkemmin tiedustelutoimivaltuuksien mahdollisen laajentamisen oikeudellisia edellytyksiä muun ohella perus- ja ihmisoikeuksien näkökulmasta.

3.2.2 Puolustusvoimien tiedonhankinta kotimaassa

Sotilastiedustelu kohdistuu Suomen ulkopuoliseen toimintaympäristöön. Toiminnallisesta näkökulmasta sotilastiedustelusta tulee erottaa sotilasvastatiedustelu, jota puolustusvoimat suorittaa poliisitehtävänä rikostorjunnallisista syistä. Sotilasvastatiedustelussa on kyse rikosten ennalta estämisestä ja paljastamisesta Suomen alueella. Sotilasvastatiedustelulla tarkoitetaan sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaa laittoman tiedustelutoiminnan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvää rikosten ennalta ehkäisemistä ja paljastamista.

Sotilasvastatiedustelulla estetään ulkovaltojen Suomeen kohdistama, Suomen rikoslaissa kriminalisoitu tiedonhankinta Suomessa esimerkiksi puolustusvoimien suorituskyvyistä ja kokoonpanoista. Tyypillisiä rikosnimikkeitä, jotka ovat ennalta estämisen ja paljastamisen kohteina, ovat rikoslain 12 luvussa tarkoitetut maanpetosrikokset, kuten maanpetos, vakoilu ja luvaton tiedustelutoiminta, ja 13 luvun valtiopetosrikokset. Myös tavallisemmat rikokset, kuten

omaisuusrikokset, voivat kuitenkin olla ennalta estämisen ja paljastamisen kohteina, mikäli ne liittyvät sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan. Esimerkkeinä tällaisista ovat puolustusvoimien salassa pidettävään tietoon kohdistuva tietoturvallisuusrikos tai omaisuusrikos. Tyhjentävää luetteloa toimivaltaa koskevista rikoksista ei ole säädetty.

Puolustushallinnon alalla puolustusvoimien sotilasvastatiedustelutehtävästä säädetään sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa. Puolustusvoimat toimii vastatiedustelun osalta erityisviranomaisena, jonka tehtävänä on huolehtia Suojelupoliisille laissa säädettyä toimivaltaa rajoittamatta sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estämisestä ja paljastamisesta. Puolustusvoimien toimivalta rikosten ennalta estämisen ja paljastamisen osalta on suojelupoliisille poliisin hallinnosta annetun lain 10 §:ssä säädettyä yleistoimivaltaa rajatumpi ja koskee vain niitä rikoksia, jotka liittyvät sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan. Tällä alueella toimivalta on rinnakkainen Suojelupoliisin rikosten ennalta estämistä ja paljastamista koskevan yleistoimivallan kanssa, mutta se ei rajoita Suojelupoliisin yleistoimivaltaa. Lakiin on sisällytetty poliisille otto-oikeus, eli oikeus myös oma-aloitteisesti ottaa puolustusvoimissa ennalta estettävä ja paljastettava asia hoitaakseen.

Rikosten ennalta estämisessä ja paljastamisessa noudatetaan myös puolustusvoimissa poliisilaissa säädettyjä periaatteita, ja niistä erityisesti perus- ja ihmisoikeuksien kunnioittamisen periaatetta, suhteellisuusperiaatetta, vähimmän haitan periaatetta ja tarkoitussidonnaisuuden periaatetta. Suojelupoliisi vastaa puolustusvoimien sotilasvastatiedustelussa esille tulleen rikoksen selvittämisestä.

Puolustusvoimissa rikosten ennalta estämistä ja paljastamista hoitavien virkamiesten toimivaltuuksista on sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetun lain mukaan voimassa, mitä poliisilaissa säädetään toimivaltuuksista rikosten ennalta estämiseksi ja paljastamiseksi. Salaisten tiedonhankintakeinojen osalta puolustusvoimien käytössä on kuitenkin vain seuraava rajattu osa poliisin toimivaltuuksista; 1) tukiasematietojen hankkiminen, 2) suunnitelmallinen tarkkailu, 3) peitelty tiedonhankinta, 4) tekninen kuuntelu, 5) tekninen katselu, 6) tekninen seuranta, 7) teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Lisäksi rikosten paljastamistehtävää koskevan lisärajauksen mukaisesti rikosten paljastamisessa näitä tiedonhankintatoimenpiteitä saadaan käyttää vain kun on kyse Suomen itsemääräämisoikeuden vaarantamista, sotaan yllyttämistä, maanpetosta tai törkeää maanpetosta, vakoilua tai törkeää vakoilua, turvallisuussalaisuuden paljastamista tai luvatonta tiedustelutoimintaa koskevan rikoksen paljastamisesta. Puolustusvoimien rikosten ennalta estämistä ja paljastamista hoitavan virkamiehen on ilmoitettava edellä mainittujen salaisten tiedonhankintakeinojen käyttämisestä suojelupoliisille.

Sotilaskurinpidosta ja rikostorjunnasta puolustusvoimissa annetussa laissa säädetään poliisin antamasta avusta silloin, kun puolustusvoimien rikostorjuntaa hoitavilla ei ole toimivaltaa tehtävien hoitamiseksi tarpeellisen toimenpiteen suorittamiseen. Käytännössä kyse on tietojen hankkimisesta sellaisella poliisin käytössä olevalla toimivaltuudella, jonka käyttämiseen puolustusvoimilla ei ole oikeutta. Rikosten ennalta estämistä ja paljastamista toteuttavat pääesikunnan ja sen alaisuudessa toimivaan Puolustusvoimien tiedustelulaitokseen sijoitetut virkamiehet.

3.3 Suojelupoliisin ja puolustusvoimien ulkomaita koskeva tiedonhankinta

3.3.1 Suojelupoliisin tiedonhankinta ulkomaita koskien

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

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

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

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

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

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

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

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

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

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

3.3.2 Puolustusvoimien tiedonhankinta ulkomaita koskien

Sotilastiedustelu osana maanpuolustusta

Puolustusvoimien maanpuolustustehtävässä suoritettavan sotilastiedustelutoiminnan on katsottu perinteisesti perustuvan puolustusvoimien lakisääteiseen tehtävään puolustaa valtakunnan itsenäisyyttä ja alueellista koskemattomuutta. Tällöin sotilastiedustelun on katsottu sisältyvän puolustusvoimista annetun lain 2 §:n 1 momentin 1 kohdan a ja b alakohtiin eikä sitä ole mainittu laissa erikseen.

Sotilastiedustelu kohdistuu Suomen ulkopuoliseen toimintaympäristöön. Sotilastiedustelun tehtävänä on muodostaa ja ylläpitää sotilaallisen päätöksenteon edellyttämää sotilasstrategista tilannekuvaa. Sen muodostamiseksi sotilastiedustelu seuraa Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta. Sotilastiedustelulla puolustusvoimat ylläpitää ja kehittää puolustusvalmiutta. Sotilastiedustelun kohteena ovat pääosin valtiotoimijat. Sotilastiedustelun tavoitteena on muodostaa ja ylläpitää toimintaympäristötietoisuutta. Keskeistä on ennakkovaroituskyky sotilaallisten uhkien kehittymisestä, jotta Suomen turvallisuutta koskeva ylimmän valtionjohdon päätöksenteko Suomen valtion suvereniteettia vaarantavista uhista perustuu oikea-aikaiselle tilannetiedolle, ja mahdollistaa tarvittaessa oikea-aikaisiin varautumis- ja vastatoimiin ryhtymisen.

Sotilastiedustelun tiedonhankintatoimivaltuuksista ei ole säädetty laissa. Sotilastiedustelu on järjestetty puolustusvoimien sisäisin määräyksin ja ohjein.

Puolustusvoimat tekee toiminnan edellyttämää yhteistyötä ulkomaisten tiedusteluviranomaisten kanssa. Yhteistyöllä pyritään tarpeellisten ulkomaisten tiedustelutietojen saamiseen puolustusvoimien käyttöön.

Puolustusasiamiehet ulkomaanedustustoissa

Diplomaattisia suhteita koskevan Wienin yleissopimuksen 3 artiklan mukaan diplomaattisen edustuston tehtäviin sisältyy muun muassa tutustuminen kaikin laillisin keinoin vastaanottajavaltion oloihin ja tapahtumiin sekä niistä tiedottaminen lähettäjävaltion hallitukselle. Yleissopimuksen 7 artiklassa mainitaan edustuston henkilöistä erikseen sotilas-, laivasto- ja ilmailuasiamiehet.

Suomella on akkreditoituja puolustusasiamiehiä useissa valtioissa yhteensä noin 20. Mainitut virkamiehet raportoivat asemamaastaan sotilastiedustelulle. Puolustusvoimia koskevissa laeissa ei ole säännöksiä edustustoissa toimivien puolustusvoimien virkamiesten toimivaltuuksista.

Sotilastiedustelu osana kriisinhallintaoperaatioita

Puolustusvoimista annetun lain 2 §:n 1 momentin 3 -kohdan mukaan puolustusvoimien tehtävänä on osallistuminen kansainväliseen sotilaalliseen kriisinhallintaan. Saman lain 2 luvussa säädetään puolustusvoimien toimivallasta. Lain 13 §:n mukaan puolustusvoimat osallistuu kansainväliseen sotilaalliseen kriisinhallintaan siten kuin sotilaallisesta kriisinhallinnasta annetussa laissa (211/2006) säädetään.

Sotilaallisesta kriisinhallinnasta annetun lain 5 §:n mukaan puolustusministeriö antaa sotilaallisen kriisinhallinnan edellyttämät tehtävät puolustusvoimille sekä ohjaa ja valvoo sotilaallista kriisinhallintaa. Suomalaiseen kriisinhallintaorganisaatioon voi kuulua kriisinhallintajoukkoja, erillisiä yksiköitä ja yksittäisiä henkilöitä. Kriisinhallintaorganisaatio kuuluu puolustusvoimiin ja on pääesikunnan alainen siten kuin sotilaallisesta kriisinhallinnasta annetun lain 5 §:ssä säädetään. Toiminnallisesti kriisinhallintaorganisaatio on sotilaallisesta kriisinhallinnasta annetun lain 1 §:n 3 momentissa tarkoitetun toimeenpanijan alainen. Näitä ovat YK, Euroopan turvallisuus- ja yhteistyöjärjestö (Etyj), Euroopan unioni (EU), Pohjois-Atlantin liitto (Nato) taikka muu kansainvälinen järjestö tai maaryhmä. Sotilaallisesta kriisinhallinnasta annetussa laissa tai puolustusvoimien toimintaa koskevissa laessa ei ole erityissäänteleyä kriisinhallintaoperaatioiden sotilastiedustelusta. Operaatioihin voi kuulua tiedusteluelin.

Kriisinhallintaoperaatiossa sotilasjoukko toimii toisen valtion alueella. Sotilasjoukkojen asema toisen suvereenin valtion alueella (operaation isäntävaltio) järjestetään sopimuksin, joissa määrätään joukkojen oikeudellisesta asemasta ja immuniteetista isäntävaltion alueella. Näitä sopimuksia kutsutaan joukkojen oikeudellista asemaa sääänteleviksi sopimuksiksi (Status of Forces Agreement, SOFA-sopimus). Lähtökohtaisesti SOFA-sopimusten neuvottelusta vastaa operaation valtuuttaja tai toimeenpanija suhteessa operaation isäntävaltioon. Pääsääntöisesti kyseisten sopimusjärjestelyistä johtuvat velvollisuudet, käytännössä erivapauksien ja –oikeuksien myöntäminen kriisinhallintajoukolle, kohdentuvat yksipuolisesti operaation isäntävaltioon. On syytä korostaa, että SOFA-sopimukset eivät luo toimivaltuuksia operaatioissa palveleville joukoille. Toimivaltuudet seuraavat operaation kansainvälisoikeudellisesta mandaatista, joukkoja lähettävien maiden kansallisesta lainsäädännöstä sekä operaatiossa annetuista sotilaskäskyistä.

3.4 Tietoturvauhkien torjunnasta

3.4.1 Yleistä

Suomi on tietoyhteiskuntana ja kansainvälisiin markkinoihin nojaavana taloutena riippuvainen tietoinfrastruktuurin häiriöttömästä toiminnasta. Viestintäverkkojen ja -palvelujen toimivuus ja luotettavuus ovat tärkeitä edellytyksiä Suomen talouden kasvulle, kilpailukyvylle, innovaatioille ja hyvinvoinnille kaikilla yhteiskunnan toimialoilla.

Tietoinfrastruktuurin toimintavarmuus on tärkeää myös yhteiskunnan kokonaisturvallisuuden kannalta. Yhteiskunnan tietoteknistyminen, tietoliikenneinfrastruktuurin ulkomaisen omistuksen kasvu sekä valtionhallinnon tietoteknisten toimintojen ulkoistaminen asettavat uudenlaisia vaatimuksia yhteiskunnan elintärkeiden toimintojen turvaamiseksi. Yhteiskunnan elintärkeillä toiminnoilla tarkoitetaan poikkihallinnollisia, yhteiskunnalle välttämättömiä toimintokokonaisuuksia, joiden on oltava turvattuina kaikissa tilanteissa. Tietoteknisten järjestelmien toimimattomuus, informaatioinfrastruktuurin luhistuminen ja erilaiset tietoturvauhat vaikuttavat kielteisesti julkisiin palveluihin, liike-elämään sekä hallintoon ja siten koko yhteiskunnan toimintaan. Valtaosa Suomen kriittisestä tietoliikenneinfrastruktuurista ja sen palveluista on yksityisen sektorin omistamaa ja tuottamaa, mistä johtuen sen merkitys yhteiskunnan elintärkeiden toimintojen turvaamisessa on tärkeä.

Sähköisen viestinnän sekä tietoverkkojen ja -järjestelmien toimintaa ja häiriöttömyyttä suojataan tietoturvan avulla. Tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla (luottamuksellisuus), ettei tietoja voida muuttaa muiden kuin siihen oikeutettujen toimesta (eheys) ja että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä (käytettävyys).

Sähköisten viestintäverkkojen ja -palveluiden käyttäjinä olevat tahot huolehtivat tietoturvastaan eri menetelmillä. Tietoturvaa voidaan ylläpitää esimerkiksi tietohallinnollisin keinoin ja asettamalla viestintäverkon tai palvelun käytölle teknisiä rajoituksia. Valtionhallinnon yhtenäinen luonne mahdollistaa sen, että hallinnon tietoturvaa voidaan ohjata keskitetysti ja yhdenmukaisten periaatteiden nojalla. Valtiovarainministeriö ohjaa ja johtaa julkisen hallinnon tietoturvallisuuden yleistä kehittämistä ja valtionhallinnon tietoturvallisuutta sekä ICT-varautumista. Valtiovarainministeriön ohjaava tehtävä perustuu muun muassa julkisen hallinnon tietohallinnon ohjauksesta annettuun lakiin (634/2011) ja valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä annettuun lakiin (1226/2013).

Valtion ylimmän johdon päätöksenteon ja turvallisuusviranomaisten lakisääteisten tehtävien turvaamiseksi hallitus antoi vuonna 2013 esityksen laiksi julkisen hallinnon turvallisuusverkkotoiminnasta (HE 54/2013).[4] Tavoitteena on säätää turvallisuusverkosta (TUVE), joka yhdistää samaan tietoliikenneverkkoon valtion johdon, ministeriöt, puolustusvoimat, rajavartioston, poliisin ja pelastustoimen. Turvallisuusverkolla voitaisiin varmistaa viranomaisten varautuminen tietoliikennehäiriöihin ja tietoliikenteen jatkuvuus.

Julkisen hallinnon turvallisuusverkko tarjoaisi kaikille sen käyttäjille ja heidän keskeisille palveluntuottajilleen vakaan tieto- ja viestintäteknisen palveluympäristön. Turvallisuusverkon tietoliikenne- ja tietoturvaratkaisut mahdollistaisivat eri suojaustasojen sekä käyttäjien yhteisten tai erillisten tietojenkäsittely-ympäristöjen toteuttamisen. Näin saavutettaisiin kustannustehokkaasti viranomaisille yhteinen ja yhteentoimiva koko maan kattava tietoverkko, joka

4 Eduskunta on 19.12.2014 hyväksynyt lain julkisen hanllinnon turvallisuusverkkotoiminnasta (EV 245/2014 vp).

toimii luotettavasti myös poikkeusoloissa ja muun muassa luonnonilmiöiden, sähkökatkosten tai jatkuvasti lisääntyvien tietoverkkohyökkäysten sattuessa. Valtiovarainministeriö päättäisi normaalioloissa ja niihin liittyvissä häiriötilanteissa turvallisuusverkon palvelutuotannon ja käytön ensisijaisuus-, kiireellisyys- ja muusta tärkeysmäärittelystä.

Valtiovarainministeriö käynnisti vuonna 2013 myös valtion ympärivuorokautisen tietoturvatoiminnan kehittämishankkeen (SecICT). Hankkeen tehtävänä on suunnitella ja perustaa viranomaistoiminto laajojen sekä vakavien tietoturvahäiriötilanteiden ennaltaehkäisyyn ja koordinointiin. Hankkeessa laajennetaan ja kehitetään valtionhallinnon tietoturvallisuutta parantavia palveluita. Lisäksi hankkeessa käynnistetään häiriönratkaisuryhmien toiminta (VIRT-toiminta). Kehittäminen tapahtuu yhteistyössä valtion ja yksityisen sektorin tieto- ja kyberturvallisuuden toimijoiden sekä pilottiorganisaatioiden kanssa. Hankkeen on määrä päättyä vuoden 2015 lopussa, jolloin uusi toiminto käynnistyy vuoden 2016 alusta.

Yksityisellä sektorilla keskitetty tietoturvaohjaus ei ole mahdollista, vaan tietoturvan taso ja tietoturvan ylläpitämiseksi valitut ratkaisut vaihtelevat jokaisen organisaation omien tarpeiden ja painotusten mukaan. Tietoturvauhkien havaitseminen ja niiltä suojautuminen perustuu niin hallinnossa kuin yksityiselläkin sektorilla käytännössä kaupallisiin tietoturvaohjelmiin ja -palveluihin. Osa valtionhallintoa ja huoltovarmuuskriittisistä yrityksistä hyödyntää suojautumisessaan myös Viestintäviraston vakavien tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä (HAVARO).

3.4.2 Tietoyhteiskuntakaaren 272 §

Tietoyhteiskuntakaari (917/2014) hyväksyttiin eduskunnassa 15.10.2014 (EV 106/2014 vp) ja se tuli voimaan 1.1.2015. Lailla kumotaan muun muassa sähköisen viestinnän tietosuojalaki (SVTSL). Tietoyhteiskuntakaaren 272 §:ssä on SVTSL 20 §:ää sisällöllisesti vastaava säännös. Tietoyhteiskuntakaari on säädetty perustuslakivaliokunnan myötävaikutuksella.

Tietoyhteiskuntakaaren 272 § antaa sähköisiä viestintäpalveluja hyödyntäville yrityksille, yhteisöille ja viranomaisille tietoturvastaan huolehtimisen tarkoituksessa oikeuden analysoida verkkoonsa tulevien ja siitä lähtevien viestien sisältöä muun muassa haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

SVTSL:n 20 §:n alkuperäisten esitöiden (HE 125/2003 vp, s. 71) mukaan ilmaisulla ”haittaa aiheuttavat häiriöt” viitataan muun muassa haittaohjelmien tahalliseen laajaan levittämiseen ja käyttöön. Tietoyhteiskuntakaaren 272 §:n yksityiskohtaisissa perusteluissa todetaan, ettei tämän säännöksen osalta ole tarkoitus muuttaa vallitsevaa oikeustilaa (HE 221/2013 vp, s. 106).

Viestinnän sisällön automaattinen analysointi kohdistuu kaikkien niiden viestien sisältöön, jotka tulevat sisään tai lähtevät ulos automaattista analysointia käyttävän tahon tietoverkosta tai -järjestelmästä. Analysoinnin pääasiallisena tarkoituksena on havaita haittaohjelmien yrityksiä tunkeutua tietojärjestelmään sekä järjestelmään mahdollisesti jo tunkeutuneiden haittaohjelmien viestintää isäntiensä kanssa.

Haitalliset ohjelmat ja käskyt tunnistetaan ensi vaiheessa automaattisessa sisällöllisessä analysoinnissa ennalta tehtyjen määrittelyiden perusteella, eikä viestin sisältö tällöin tule luonnollisen henkilön tietoon. Jos on ilmeistä, että automaattisessa suodatuksessa esiin noussut viesti sisältää haittaohjelman eikä tietoturvaa voida varmistaa automaattisin keinoin, sallii tietoyhteiskuntakaaren 272 § sen, että yritys, yhteisö tai viranomainen ottaa viestin sisällön manuaaliseen käsittelyyn.

3.4.3 Viestintäviraston Kyberturvallisuuskeskus

Viestintäviraston Kyberturvallisuuskeskus on kansallinen tietoturvaviranomainen, joka muun muassa ennaltaehkäisee, kerää tietoa ja selvittää yleisiin viestintäverkkoihin liittyviä ja niiden kautta suomalaisiin tahoihin suuntautuvia tietoturvaloukkauksia sekä tiedottaa merkittävistä tietoturvauhkista. Kyberturvallisuusstrategian mukaan Kyberturvallisuuskeskuksen tehtävänä on myös yhdistetyn kyberturvallisuuden tilannekuvan tuottaminen ja ylläpitäminen. Kyberturvallisuuskeskus kerää tietoja tietoverkkotapahtumista ja välittää sitä eri toimijoille sekä muodostaa ja jakaa kyberturvallisuuden yhdistettyä tilannekuvaa. Kyberturvallisuuskeskuksen asiakkaat voivat hyödyntää tilannekuvatietoa oman varautumisensa järjestämisessä ja priorisoinnissa.

Tilannekuvan muodostamisessa hyödynnetään kansallisten lähteiden lisäksi Kyberturvallisuuskeskuksen vapaaehtoisuuteen ja molemminpuoliseen luottamukseen perustuvaa kansainvälistä yhteistyöverkostoa. Yhteistyöverkostoon kuuluvien GovCERT-ryhmien emo-organisaatiot ovat sijoittuneet omissa maissaan valtionhallinnon eri toiminteisiin. Esimerkiksi Ruotsin CERT-SE on osa siviilivalmiusvirastoa kun taas Saksan CERT-BUND toimii sisäministeriön hallinnonalalla. Joissain valtioissa CERT-ryhmät on sijoitettu puolustusministeriön hallinnonalalle ja joissain CERT-ryhmät toimivat puolestaan osana tiedusteluviranomaista (Government Communications Headquarters, GCHQ).

HAVARO on Viestintäviraston Kyberturvallisuuskeskuksen huoltovarmuuskriittisille yrityksille ja valtionhallinnon toimijoille tarjoama tietoturvaloukkausten havainnointi- ja varoitusjärjestelmä, toiminta perustuu tietoyhteiskuntakaaren 272 §:ään (aiemmin SVTSL 20 §:ään). HAVAROn tarkoituksena on tunnistaa erilaisten tunnisteiden avulla haitallista verkkoliikennettä ja tietoturvaa vaarantavia kehittyneitä verkkohyökkäyksiä (Advanced Persistent Threat, yleisesti APT). Järjestelmän toisena tarkoituksena on tukea paremman tilannekuvan muodostamista suomalaisiin tietoverkkoihin kohdistuvista tietoturvauhkista. Järjestelmässä hyödynnettävät tekniset haittaohjelmatunnisteet perustuvat pääosin Kyberturvallisuuskeskuksen kotimaisilta ja ulkomaisilta yhteistyökumppaneilta saamiin tietoihin.

4. KANSAINVÄLINEN VERTAILU

Jaksossa selvitetään sitä, millaista lainsäädäntöä Ruotsissa, Norjassa, Tanskassa, Alankomaissa ja Saksassa on kansalliseen turvallisuuteen kohdistuviin uhkiin liittyvästä tiedustelusta yleensä ja tietoverkkoympäristössä tapahtuvasta tiedustelusta erityisesti.

4.1 Ruotsi

4.1.1 Tiedustelutoiminnan yleissääntely

Puolustushallinnon tiedustelutoiminnasta säädetään sotilastiedustelusta annetulla yleislailla ja sitä täydentävällä asetuksella sekä erityislaeilla.[5] Sotilastiedustelua harjoittavat puolustusvoimat (*Försvarsmakten*), puolustusvoimien radiolaitos (*Försvarets radioanstalt, FRA*), puolustusvoimien materiaalilaitos (*Försvaretsmaterielverk, FMV*) ja kokonaismaanpuolustuksen tutkimusinstituutti (*Totalförsvarets forskningsinstitut, FOI*), jotka toimivat puolustusministeriön alaisina. Tiedustelun toimiala on rajattu siten, että tiedustelutoimintaa harjoitetaan Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan tueksi ja Ruotsiin kohdistuvien ulkoisten uhkien kartoittamiseksi. Toiminnalla tuetaan myös Ruotsin osallistumista kansainväliseen turvallisuusyhteistyöhön. Tiedustelu saa koskea vain ulkomaisia olosuhteita.

Hallitus päättää tiedustelutoiminnan yleisestä kohdentamisesta. Hallituksen erikseen nimeämät viranomaiset voivat hallituksen päättämän yleisen kohdentamisen puitteissa antaa tiedustelutoiminnan tarkempaa kohdentamista koskevia määräyksiä. Tiedustelun tehtävänä on hankkia, työstää ja analysoida tietoja. Tiedot hankitaan joko teknisesti tai henkilötiedustelulla sekä avoimista että muista lähteistä. Tiedot raportoidaan toimeksiannon antaneelle taholle sekä niille mahdollisille muille tahoille, joita tiedot koskevat. Tiedustelutoimintaa harjoittavat viranomaiset voivat hallituksen tarkempien määräysten mukaan, laissa annetuin edellytyksin, tehdä yhteistyötä tiedustelutoiminnan alalla muiden maiden ja kansainvälisten organisaatioiden kanssa.

Tiedustelu ei voi ottaa hoitaakseen sellaisia tehtäviä, jotka lain tai muiden säännösten mukaan kuuluvat poliisin, turvallisuuspoliisin tai muiden lainvalvontaviranomaisten rikostorjunta- tai estämistoimivaltaan.[6] Puolustustiedustelutoiminnasta annetun lain esitöiden[7] mukaan tällä tarkoitetaan sitä, ettei tiedustelussa saada muuta lainsäädäntöä kiertämällä käyttää sellaisia esitutkinta- tai pakkokeinotoimivaltuuksia, joiden käyttöalasta ja käytön edellytyksistä säädetään oikeudenkäymiskaaressa ja esimerkiksi poliisilaissa. Toisaalta tiedustelussa saadaan antaa tukea rikostorjuntaviranomaisille. Tältä osin lain esitöissä[8] todetaan, että turvallisuuspoliisi on nykyisin monilta osin tiedustelupalvelunomaista ja suuntautuu myös ulkomailla harjoitettavaa Ruotsin turvallisuutta vaarantavaa toimintaa koskevien tietojen hankintaan. Tämän

5 Lag om försvarsunderrättelseverksamhet (2000:130), Förordning om försvarsunderrättelseverksamhet (2000:131), Lag om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst (2007:258) ja Förordning (2007:260) om behandling av personuppgifter i Försvarsmaktens försvarsunderrättelseverksamhet och militära säkerhetstjänst.

6 Säännösmuutos voimaan 1.1.2015. Aiempi sanamuoto: ”--polisens och andra myndigheters brottsbekämpande och brottsförebyggande verksamhet.”.

7 Regeringens proposition 1999/2000:25.

8 Regeringens proposition 2006/07:63: ”En anpassad försvarsunderrättelseverksamhet”.

tehtävänsä puitteissa turvallisuuspoliisin on voitava hyödyntää myös tiedustelusta vastaavien viranomaisten tiedonhankintakapasiteettia.

Tiedustelua harjoittavilla viranomaisilla on velvollisuus raportoida puolustusministeriölle toiminnan yleisestä suuntautumisesta, kansainvälisestä yhteistyöstä sekä erityisillä tiedonhankintakeinoilla tehtävästä tiedustelusta. Näitä erityisiä tiedonhankintakeinoja ei ole katsottu voitavan avata laissa, mutta lain esitöissä todetaan, että niillä viitataan pääasiallisesti henkilöja signaalitiedusteluun.[9] Tiedusteluviranomaisten tulee myös tehdä vuosittain menneen vuoden tiedustelutoiminnasta julkinen yleiskatsaus. Hallituksen määräämä viranomainen, valtion tiedustelutarkastus (statens inspektion för försvarsunderrättelseverksamheten, SIUN), valvoo puolustustiedustelutoimintaa. SIUN valvoo muun muassa lain noudattamista, tiedustelun kohdentamista ja tiedonhankinnassa käytettyjä menetelmiä.

4.1.2 Signaalitiedustelu

Signaalitiedustelusta säädetään sitä koskevassa erityislaeissa ja -asetuksessa.[10] Signaalitiedustelua harjoittaa puolustusvoimien radiolaitos (FRA), joka on puolustusministeriön alainen siviiliorganisaatio eikä siten osa puolustusvoimia. FRA:n tehtävänä on hankkia tiedustelutietoja saamiensa toimeksiantojen mukaisesti ja toimittaa hankkimansa tiedot toimeksiantajien käyttöön.

Signaalitiedustelulain mukaan signaalitiedustelulla tarkoitetaan elektronisessa muodossa olevien signaalien hakemista *(inhämta signaler i elektronisk form)*. Määritelmä on tekniikkaneutraali ja kattaa kaikki signaalitiedustelun menetelmät, kuten esimerkiksi kaapeli- ja radiosignaalitiedustelun sekä manuaalisen ja automaattisen tietojenkeruun. Signaalitiedustelu jakautuu neljään vaiheeseen, jotka ovat signaalitiedustelun kohdentaminen, tietojen kerääminen, tietojen työstäminen ja tietojen raportointi.

Signaalitiedustelun edellytyksenä on, että sekä yleisessä puolustustiedustelulaissa että signaalitiedustelua koskevassa erityislaissa määritellyt edellytyksen täyttyvät. Yleisen lain mukaan kyse tulee olla Ruotsin ulko-, turvallisuus ja puolustuspolitiikkaa tukevasta, ulkomaisia olosuhteita koskevasta tiedustelutehtävästä, jossa kartoitetaan Ruotsiin kohdistuvia ulkoisia uhkia. Signaalitiedustelua koskeva erityislaki puolestaan määrittelee tyhjentävästi ne uhat ja tilanteet, joiden kartoittamiseksi signaalitiedustelua saadaan käyttää.[11] Jos toiminnan kannalta on välttämätöntä, voidaan tietoja hankkia myös signaaliympäristössä, teknisessä kehityksessä ja signaalisuojassa tapahtuvien muutosten seuraamiseksi sekä tiedonhankinnassa käytettävän tekniikan ja menetelmien kehittämiseksi. Yleisenä rajoituksena on se, että jos sekä signaalin vastaanottaja ja lähettäjä ovat Ruotsissa, ei signaalia saa kerätä.

Signaalitiedusteluun ryhtyminen edellyttää aina toimeksiantoa, jonka FRA:lle voi antaa valtioneuvosto, valtioneuvoston kanslia, puolustusvoimat, keskusrikospoliisi tai suojelupoliisi. Toimeksianto ei saa viitata yksinomaan tiettyyn luonnolliseen henkilöön.

---

9 Regeringens proposition 2006/07:63: ”En anpassad försvarsunderrättelseverksamhet”.

10 Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet ja Förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet.

11 Tällaisia tilanteita ovat signaalitiedustelusta annetun lain 1 §:n mukaan: a) Ruotsiin kohdistuva sotilaallinen uhka, b) Ruotsin intressit kansainvälisissä operaatioissa, c) kansainvälinen terrorismi tai järjestäytynyt rikollisuus, joka voi uhata merkittäviä kansallisia intressejä, d) joukkotuhoaseet, e) ulkoiset yhteiskunnan infrastruktuuriin kohdistuvat uhat, f) kansainväliseen turvallisuuteen vaikuttavat konfliktit ulkomailla, g) ulkopuolinen Ruotsin intresseihin kohdistuva tiedustelutoiminta ja h) Ruotsin ulko-, turvallisuus ja puolustuspolitiikan kannalta merkittävä vieraan vallan toiminta tai aikomus.

Vaikka laki on tekniikkaneutraali, sisältyy siihen joitain kaapelitiedustelua koskevia erityissäännöksiä. Kaapelitietoliikennettä saadaan tiedustella vain silloin, kun se ylittää Ruotsin rajan.

Signaalitiedustelu edellyttää aina erityistuomioistuimena toimivan puolustustiedustelutuomioistuimen lupaa. Kaapelitiedustelua koskevan lupahakemuksen tulee sisältää kuvaus tiedustelutehtävästä, tieto siitä, mihin kaapelin kuituihin tiedonhankinta halutaan kohdistaa, käytettävät hakuehdot, luvan kesto ja muut seikat, joihin signaalitiedusteluviranomainen haluaa vedota. Laissa on myös annettu tarkat edellytykset sille, milloin tuomioistuin voi myöntää luvan, ja mitä luvasta tulee käydä ilmi. Myöntämisedellytykset liittyvät erityisesti toiminnan ja tehtävän lainmukaisuuteen ja suhteellisuuteen. Luvasta tulee käydä ilmi tiedonhakutehtävä, mitä kaapeleiden kuituja lupa koskee, mitä hakuehtoja tai hakuehtokategorioita saa käyttää, luvan kesto ja muut ehdot, joita tarvitaan yksittäisen henkilön yksityisyyden suojaan puuttumisen rajoittamiseksi. Hakuehdoilla tarkoitetaan lain esitöiden mukaan[12] sellaisia käsitteitä, joiden avulla tietomäärästä (*informationsmängd*) voidaan löytää sellaiset tietueet tai tietoryhmät (*uppgiftskonstellationer*), joissa kyseinen käsite esiintyy. Hakuehto voi myös sisältää sellaisia muuttujia, joilla kyetään erottelemaan suurempia tietomääriä.

Mahdollisuutta käyttää yksittäiseen luonnolliseen henkilöön viittaavaa hakuehtoa on rajattu yksityisyyden suojan varmistamiseksi. Tällaista hakuehtoa voidaan käyttää vain, jos se on erityisen tärkeää tiedustelutoiminnalle. Lisäksi FRA:lla on velvollisuus antaa selvitys signaalitiedustelua valvovalle valtion tiedustelutarkastukselle tällaisista hakuehdoista. Luonnolliselle henkilölle tulee ilmoittaa niin pian kuin mahdollista ja viimeistään kuukausi tiedustelutehtävän päättymisestä, milloin ja missä tarkoituksessa tiedustelu on toteutettu, ellei salassapitomääräyksistä muuta johdu.

Tietoliikennekaapelissa tapahtuva tietojenkeruu edellyttää tietoliikenneoperaattorin kanssa tehtävää yhteistyötä. Tämän takia kaapelin omistavilla tietoliikenneoperaattoreilla on velvollisuus viedä Ruotsin rajat ylittävä tietoliikenne määritettyyn yhteyspisteeseen tai -pisteisiin. Lisäksi operaattoreilla on velvollisuus luovuttaa viranomaiselle sellaiset tiedot, jotka helpottavat signaalien haltuunottoa. Operaattoreiden tulee suorittaa edellä mainitut toimenpiteet siten, ettei niiden salassapito vaarannu.[13]

Vain valvontaviranomaisena toimivalla valtion tiedustelutarkastuksella on pääsy operaattoreiden yhteyspisteisiin viemään tietoliikenteeseen. Sen tehtävänä on erotella ja luovuttaa FRA:lle pääsy vain tuomioistuimen luvassa yksilöityihin kaapelin kuituihin.[14] FRA:n suorittamat haut kohdistuvat näihin kuituihin. FRA raportoi signaalitiedustelulla hankitut tiedot toimeksiantajalle sekä laissa määritellyin edellytyksin muillekin viranomaisille.

FRA:ssa toimii tietosuojaneuvosto *(Integritetsskyddsråd),* jonka tehtävänä on valvoa yksityisyyden suojan toteutumista. Neuvosto raportoi FRA:n johdolle ja tarvittaessa valtion tiedustelutarkastukselle. Lisäksi signaalitiedustelua valvovat tietosuojavaltuutettu, eduskunnan oikeusasiamies ja oikeuskansleri.

Valtion tiedustelutarkastuksen valvonta koskee etenkin signaalitiedustelun hakuehtojen käyttöä, tietojen hävittämistä ja raportointia. Se voi myös määrätä tiedustelutoimenpiteen lopetettavaksi ja tiedot tuhottaviksi, mikäli toiminta ei ole ollut luvan mukaista. Valtion tiedus-

12 Regeringens proposition 2006/07:63, s. 76–77.

13 Lag (2003:389) om elektronisk kommunikation 19 a §

14 Lag om signalspaning 12 §. Kyseessä on lailla 2009:967 tehty muutos, jota koskee hallituksen esitys Prop 2008/09:21 *Förstärkt integritetsskydd vid signalspaning*. Aiemmin lupaehdon mukaisen tietojenkeruun yhteyspisteessä toteutti FRA. Muutosta perusteltiin sillä, että signaalitiedustelun uskottavuuden lisääminen edellyttää, että signaalitiedusteluviranomaisella ei ole pääsyä muihin kaapeleiden kuituihin kuin niihin, joita luvat koskevat.

telutarkastus voi luonnollisen henkilön pyynnöstä tarkastaa, onko tämän viestejä seurattu ja onko mahdollinen seuranta ollut lain mukaista. Tietosuojavaltuutettu *(Datainspektion)* valvoo yksityisyydensuojan toteutumista myös FRA:n toiminnassa.

Signaalitiedustelulla hankittujen henkilötietojen käsittelystä säädetään erillisessä laissa.[15]

4.2 Norja

Norjassa tiedustelusta ja tiedustelupalvelun toiminnasta säädetään laissa tiedustelupalvelusta ja sitä täsmentävässä asetuksessa.[16] Puolustusministeriö voi antaa asetusta täydentäviä määräyksiä. Tiedustelutoimintaa harjoittaa puolustusvoimien organisaatiossa toimiva Norjan tiedustelupalvelu (*Etterretningstjenesten, E-tjenesten, NIS*). Se vastaa tiedustelupalvelulain mukaisten ulkoisten uhkien sekä ulkomaisten toimijoiden motiivien, niiden suorituskyvyn ja käyttämien menetelmien havaitsemisesta ja analysoinnista. Tiedustelutoiminnan tarkoituksena on ehkäistä uhkia ja luoda kestävä pohja ulko-, turvallisuus- ja puolustuspolitiikkaa koskevalle päätöksenteolle. Ohjauksesta ja valvonnasta vastaa puolustusministeriö, jota kohtaan tiedustelupalvelulla on raportointivelvollisuus toiminnastaan. Valtion sisäisestä turvallisuudesta vastaa poliisin turvallisuuspalvelu (*Politiets sikkerhetstjeneste, PST*).

Norjan tiedustelupalvelun tehtävänä on hankkia, työstää ja analysoida tietoa, joka koskee Norjan etuja suhteessa vieraisiin valtioihin, organisaatioihin ja yksilöihin ja tätä taustaa vasten laatia uhka-analyyseja ja tiedusteluarvioita siinä laajuudessa, kun tämä voi myötävaikuttaa tärkeiden kansallisten intressien turvaamiseen.[17] Laissa oleva luettelo kansallisista eduista ei kuitenkaan ole tyhjentävä. Puolustusministeriö antaa tiedustelupalvelulle tehtävät puolustusvoimien päällikön kautta. Tiedustelupalvelun on laadittava selvityksiä ja kerättävä tietoa hallituksen ja asianomaisten ministeriöiden tarpeiden mukaan. Tiedustelupalvelulle on säädetty oikeus kansainväliseen tiedusteluyhteistyöhön muiden maiden ja kansainvälisten organisaatioiden kanssa sekä erityinen velvollisuus tehdä yhteistyötä niiden puolustusliittojen kanssa, joihin Norja kuuluu.

Tiedustelupalvelun käytössä olevista tiedonhankintamenetelmistä ei ole säädetty. Tiedonhankintaa on kuitenkin rajoitettu laissa siten, että tiedustelupalvelu ei saa Norjan alueella valvoa eikä muuten salassa kerätä tietoja norjalaisista luonnollisista tai juridisista henkilöistä. Poikkeuksena tästä tiedustelupalvelu voi kuitenkin kerätä tietoja sellaisista norjalaisista henkilöistä, jotka osallistuvat laittomaan tiedustelutoimintaan vieraan valtion puolesta Norjassa. Tällöin tiedonhankinnan on tapahduttava poliisin turvallisuuspalvelun välityksellä tai sen hyväksymänä.

Tiedustelupalvelun ja poliisin turvallisuuspalvelun välistä yhteistyötä säännellään asetuksella[18], jonka tarkoituksena on edistää osapuolten välistä yhteistyötä. Yhteistyön priorisoitu-

15 Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.

16 Lov om etterretningstjenesten 1998-03-20 nr 11 ja Instruks om etterretningsstjenesten FOR 2001-08-31 nr 1012.

17 Tällaisia tärkeitä kansallisia intressejä ovat muun muassa: a) Norjan ulkomaan-, puolustus- ja turvallisuuspolitiikan muotoilu, b) valmiussuunnittelu ja kriisinhallinta, c) puolustusvoimien pitkän ajan suunnittelu ja rakennekehitys, d) puolustusvoimien operatiivisten osastojen tehokkuus, e) tuki sellaisille puolustusliitoille, joissa Norja on mukana, f) norjalaiset joukot, jotka ovat mukana kansainvälisissä sotilaallisissa operaatioissa, g) Norjan osallistuminen kansainvälisiin aseriisunta- ja aserajoitussopimuksiin ja näiden sopimusten seuranta sekä h) kansainvälinen terrorismi i) ylikansalliset ympäristöongelmat ja j) joukkotuhoaseiden levittäminen ja sellaisten aseiden valmistukseen tarvittavat laitteet ja materiaalit.

18 Instruks om samarbeidet mellom Etterretningstjenesten og Politiets sikkerhetstjeneste 13. oktober 2006 nr. 1151

ja aloja ovat terrorismin, joukkotuhoaseiden levittämisen ja laittoman tiedustelutoiminnan torjunta sekä tärkeitä norjalaisia etuja koskevat muut olosuhteet. Palveluiden tulee avustaa toisiaan niin konkreettisten tiedonhankintaoperaatioiden toteuttamisessa ja operatiivisten tietojen vaihtamisessa kuin strategisten tietojen analysoinnissa ja uhka-arvioinnissa. Yhteistyön edellytyksenä on, että osapuolet noudattavat omista toimivaltuuksistaan annettuja säännöksiä.

Tiedustelupalvelun valvonnasta säädetään kaikille turvallisuusviranomaisille yhteisessä laissa tiedustelu-, valvonta- ja turvallisuuspalveluiden valvonnasta.[19] Lain mukaan tiedustelupalvelua valvoo suurkäräjien tiedustelu-, valvonta- ja turvallisuuspalveluiden valvontavaliokunta. Valiokunta on toiminnassaan itsenäinen ja suurkäräjistä riippumaton. Valvonnan tarkoituksena on ehkäistä ja selvittää mahdollisia väärinkäytöksiä, varmistaa tiedustelussa käytettävien keinojen oikeasuhtaisuus ja ihmisoikeuksien kunnioittaminen sekä valvoa, että toiminta on lainmukaista eikä aiheuta kohtuutonta vahinkoa yhteiskunnalle. Valvontaa tehdään sekä oma-aloitteisesti että käsittelemällä kanteluita. Valiokunnalle on sen tehtävien puitteissa taattu laajat pääsyoikeudet tiedustelupalvelun arkistoihin, rekistereihin ja toimitiloihin. Valvontavaliokunta antaa vuosittain toiminnastaan selvityksen suurkäräjille.

4.3 Tanska

Tanskassa tiedustelua harjoittaa puolustusministeriön alaisuudessa toimiva siviiliviranomainen, puolustusvoimien tiedustelupalvelu (*Forsvarets Efterretningstjeneste, FE*). Puolustusvoimien tiedustelupalvelusta annetussa laissa säädetään sen tehtävistä, toimivallasta ja tiedustelutoiminnan valvonnasta.

FE vastaa sekä Tanskan ulkomaantiedustelusta että sotilastiedustelusta. Se toimii myös kansallisena tietoturvaviranomaisena. FE:n tehtäviä ja toimintaa säännellään vuonna 2013 annetulla Puolustusvoimien tiedustelupalvelua koskevalla lailla[20], joka korvasi ns. puolustuslakiin[21] sisältyneen varsin suppean aiemman sääntelyn. FE:n lakisääteisinä tehtävinä on luoda tiedustelullinen perusta Tanskan ulko-, turvallisuus- ja puolustuspolitiikalle, auttaa ehkäisemään ja torjumaan Tanskaan ja Tanskan etuihin kohdistuvia uhkia, ja näissä tarkoituksissa kerätä, työstää ja analysoida ulkomaisia suhteita koskevia tietoja, joilla on merkitystä Tanskalle ja Tanskan eduille ulkomailla, sekä raportoida niistä. FE:llä on velvollisuus informoida puolustusministeriötä olosuhteista, joilla on merkitystä Tanskalle ja sen eduille, sekä FE:n tehtäväkenttään vaikuttavista olosuhteista ja seikoista. Puolustusministerin päätöksellä tiedustelupalvelu voi lisäksi suorittaa muitakin tehtäviä, jotka liittyvät johonkin edellä mainittuun tiedustelupalvelun tehtävään.

FE:tä koskeva toimivaltuussääntely on yleispiirteistä. FE saa kerätä ja hankkia tietoja, joilla voi olla merkitystä sen harjoittamalle tiedustelutoiminnalle. Ulkomaiden olosuhteisiin kohdistuvia tiedonhankintatehtäviä hoitaessaan se saa kerätä tietoja myös Tanskan kansalaisista ja tanskalaisista oikeushenkilöistä sekä maassa oleskelevista ulkomaalaisista. Laissa ei ole tämän tarkemmin säädetty tiedustelupalvelun toimivaltuuksista, eikä laki erittele eri tiedonhankintatapoja. Julkisten lähteiden mukaan tietojen hankinta tapahtuu niin henkilötiedonhankintana,

19 Lov om kontroll med etterretnings-, overvåknings- og sikkerhetstjeneste 1995-02-03 nr 07.

20 Lov om Forsvarets Efterretningstjeneste (602/2013).

21 Lov om forsvarets formål, opgaver og organisation m.v. (122/2011).

signaalitiedustelun avulla elektronisesti satelliiteista ja maassa olevista tietoliikennelinjoista kuin myös avoimista lähteistä [22]. Henkilötietojen käsittelyyn sovelletaan sekä luonnollisten että oikeushenkilöiden osalta soveltuvin osin henkilötietojen käsittelystä annetun lain säännöksiä. Lakiin ei sisälly säännöksiä tiedonhankinnan lupamenettelystä.

Tiedustelupalvelun ohella Tanskassa on poliisin turvallisuuspalvelu (*Politiets Efterretningstjeneste, PET*). PETin ulkomaantoiminnasta ei ole nimenomaisia säännöksiä, mutta sen toimintaa säätelevän lain[23] esitöiden mukaan sillä katsotaan olevan oikeus toteuttaa yhteisiä tietolähdeoperaatioita tiedustelupalvelun ja ulkomaisten tiedusteluelinten kanssa niin Tanskassa kuin ulkomailla. Tietolähteitä voidaan myös lähettää ulkomaille keräämään PET:n toimialaan kuuluvaa tietoa.

FE ja PET saavat luovuttaa toisilleen henkilö- ja muita tietoja, jos luovuttamisella voi olla merkitystä niiden tehtävien suorittamiselle. Tarkoituksena on, ettei osapuolten tarvitsisi jokaisen yksittäisen tiedonluovutustapahtuman yhteydessä arvioida erikseen sitä, onko tiedonluovutus välttämätön. FE:tä ja PET:iä koskevien lakien säätämistä esittäneen valtiollisen mietinnön mukaan palveluiden tehtävät ovat niin läheisesti sidoksissa toisiinsa, että tietojen luovuttaminen niiden välillä on pitkälti rinnastettavissa viranomaisen sisäiseen tietojen luovuttamiseen.[24]

FE:n toimintaa valvovat puolustusministeriö, valvontakomitea, kansankäräjien tiedustelupalveluvaliokunta sekä rahavarojen käytön osalta valtiontalouden tarkastusvirasto.

Valvontakomitean keskeisenä tehtävänä on valvoa henkilötietojen käsittelyn ja rekisterinpidon lainmukaisuutta tiedustelu- ja turvallisuuspalveluiden toiminnassa. Se voi ottaa henkilötietojen käsittelyä koskevan asian tutkittavakseen joko omasta aloitteestaan tai rekisteröidyn pyynnöstä. Se voi myös suorittaa tarkastuksia ja katselmuksia tiedustelu- ja turvallisuuspalveluiden tiloissa ja sillä on niiden henkilörekistereihin ja virkamiehiin kohdistuva yleinen tiedonsaantioikeus. Komitea voi antaa lausuntoja ja suosituksia tiedustelupalveluille.

Tiedustelu- ja turvallisuuspalveluiden yhteisenä parlamentaarisena erityisvalvontaelimenä toimii kansankäräjien tiedustelupalveluvaliokunta. Hallituksen tulee informoida valiokuntaa tiedustelu- ja turvallisuuspalveluiden toiminnalle osoittamistaan suuntaviivoista sekä sellaisista turvallisuuteen liittyvistä tai ulkopolitiikan alaan kuuluvista kysymyksistä, joilla on merkitystä niiden toiminnan kannalta. Olennaisten uusien tehtävien antaminen tiedustelu- ja turvallisuuspalveluille edellyttää, että tehtävät on ensin käsitelty valiokunnassa.

4.4 Alankomaat

4.4.1 Tiedustelu- ja turvallisuuspalvelut

Alankomaissa tiedustelutoimintaa harjoittavat sisäasiainministeriön alainen yleinen tiedustelu- ja turvallisuuspalvelu *(Algemene Inlichtingen- en Veiligheidsdienst, AIVD)* ja puolustusministeriön alainen sotilastiedustelu- ja turvallisuuspalvelu *(Militaire inlichtingen en veiligheid, MIVD)*. Molempien tehtävistä ja toimivaltuuksista säädetään laissa tiedustelu- ja turvallisuus-

22 http://fe-ddis.dk vierailtu 8.12.2014.

23 Lov om Politiets Efterretningstjeneste

24 Betaenkning om PET og FE (1529/2012).

palveluista.[25] Toimivaltaisella ministerillä on lisäksi oikeus antaa yksityiskohtaisempaa sääntelyä alaisensa elimen organisaatiosta, työtavoista sekä johtamisesta.

AIVD ja MIVD suorittavat sekä tiedustelua että vastatiedustelua. Palveluilla on velvollisuus tukea toisiaan tehtäviensä suorittamisessa. Niillä on yhteinen koordinaattori, jonka tehtävänä on huolehtia menettelytapojen yhteensovittamisesta. Tiedustelu- ja turvallisuuspalveluiden päälliköillä on velvollisuus tukea koordinaattoria hänen tehtävässään.

Yleisen tiedustelu- ja turvallisuuspalvelun tehtävänä on kansallisen turvallisuuden ylläpitämiseksi hankkia tietoa ja arvioida demokraattista yhteiskuntajärjestystä tai valtion elintärkeitä etuja vaarantavia ryhmiä, henkilöitä ja muita valtioita, laatia turvallisuusselvityksiä, edistää toimia valtion elintärkeiden etujen suojaamiseksi sekä laatia uhka- ja riskiarvioita tiettyjen henkilöiden, palveluiden ja omaisuuden suojaamiseksi.

Sotilastiedustelu- ja turvallisuuspalvelun tehtävänä on kansallisen turvallisuuden ylläpitämiseksi hankkia tietoa ja arvioida muiden valtioiden asevoimien operatiivista suorituskykyä, tehdä turvallisuusselvityksiä, tutkia ja arvioida omien asevoimien tilaa ja organisointia, edistää asevoimien operatiivisten intressien suojaamista sekä laatia uhka- ja riskiarvioita sotilaallisten kohteiden ja tiettyjen niihin liittyvien henkilöiden, tilojen ja palveluiden suojaamiseksi.

Alankomaissa toimivaltuussääntely on varsin yksityiskohtaista. Turvallisuus- ja tiedustelupalveluiden tulee ensisijaisesti käyttää julkisista lähteistä tai yhteistyökumppaneilta saatavia tietoja. Tämän lisäksi niillä on oikeus käyttää laissa määriteltyjä erityisiä toimivaltuuksia, joiden nojalla ne voivat harjoittaa esimerkiksi henkilö- ja signaalitiedustelua.[26] Erityisten toimivaltuuksien käyttö edellyttää lupaa, jonka pääsääntöisesti myöntää sisäministeri tai puolustusministeri. Toimivaltuuksien käyttöä koskevat muun muassa vähimmän haitan periaate ja suhteellisuusperiaate.

Tiedustelu- ja turvallisuuspalvelut raportoivat toiminnastaan vuosittain parlamentille. Ohjaavien ministereiden antama raportti sisältää katsauksen siitä, millaisiin kohteisiin palvelut ovat kohdistaneet tai tulevat kohdistamaan toimintaansa.

Tiedustelu- ja turvallisuuspalveluiden toiminnan lainmukaisuutta arvioi riippumaton arviointikomitea. Komitea perustettiin Euroopan ihmisoikeussopimuksen artiklan 8 mukaisen yksityisyyden suojan ja artiklan 13 mukaisen tehokasta oikeussuojakeinoa koskevan oikeuden varmistamiseksi. Valvontakomitea käsittelee ja tutkii tiedustelu- ja turvallisuuspalveluiden toiminnasta tehtyjä kanteluita. Valvontakomitea antaa kantelun ratkaisemista koskevan ehdotuksensa vastuuministerille. Ehdotus ei ole ministeriä sitova. Jos kantelija on tyytymätön ministerin asiassa tekemään ratkaisuun, hän voi valittaa siitä oikeusasiamiehelle. Laillisuusvalvonnan ohella valvontakomitean tehtävänä on antaa tiedustelu- ja turvallisuuspalveluita koskevia neuvoja ja suosituksia niiden toiminnasta vastuullisille ministereille.

Komitea voi suorittaa tarkastuksia ja katselmuksia tiedustelu- ja turvallisuuspalveluiden tiloissa. Tehtäviinsä liittyen sillä on yleinen tiedonsaantioikeus.

Tiedustelu- ja turvallisuuspalveluita valvovana parlamentaarisena erityisvalvontaelimenä toimii parlamentin alahuoneen tiedustelu- ja turvallisuuspalveluvaliokunta. Valiokunta raportoi työstään parlamentille.

25 Wet op de inlichtingen- en veiligheidsdiensten 2002, Intelligence and Security Services Act, ISSA 2002 (eng.).

26 Tiedustelu- ja turvallisuuspalveluista annetussa laissa säädetyt toimivaltuudet koskevat muun muassa tarkkailua, teknistä tarkkailua, peitetoimintaa, peiteyhteisöjen perustamista, tietolähteiden ohjattua käyttöä, salaisia etsintöjä, postilähetysten salaista avaamista sekä tietoteknisiin ympäristöihin tunkeutumista esimerkiksi salauksen purkamalla ja telekuuntelua.

4.4.2 Lainsäädännön kehittäminen

Tiedustelu- ja turvallisuuspalveluita koskevan lain uudistustarpeita on käsitelty niin sanotun Dessensin komitean[27] 2.12.2013 luovuttamassa mietinnössä. Mietinnön mukaan laki on liian tekniikkasidonnainen, jolloin viestintätekniikan kehitys on tehnyt siitä vanhentuneen. Voimassaoleva laki estää tiedustelupalveluita kohdistamasta tehokasta valvontaa kaapeliyhteyksien kautta välittyvään tietoliikenteeseen.

Komitea esittää tiedustelu- ja turvallisuuspalveluille nykyistä huomattavasti laajempia toimivaltuuksia kaapeleissa liikkuvan tietoliikenteen tiedusteluun. Dessensin mietinnössä ei käsitellä tiedustelun toteuttamistapaa, mutta kyse olisi ilmeisesti samankaltaisesta tietoliikenteen seulontaan perustuvasta tiedustelutoiminnasta, josta Ruotsissa on säädetty. Tiedustelutoimivaltuuksiin ehdottamansa laajennuksen vastapainoksi komitea katsoo, että näiden toimivaltuuksien valvontaa tulisi kehittää.

Sisäministeriö ja puolustusministeriö ovat ryhtyneet toimiin Dessensin mietinnön tietoliikennetiedustelua koskevien suositusten toteuttamiseksi.

4.5 Saksa

Saksassa on liittovaltion tasolla kolme tiedustelua suorittavaa elintä: yleinen ulkomaan tiedustelupalvelu (Bundesnachrichtendienst, BND), sotilaallinen turvallisuuspalvelu (Militärischer Abschirmdienst, MAD) ja yleinen turvallisuuspalvelu (Bundesamt für Verfassungsschutz, BfV). BND vastaa sekä siviili- että sotilastiedustelusta kun taas MAD ja BfV vastaavat omien toimialojensa vastatiedustelusta. BND:n ja MAD:n tehtävistä ja toimivaltuuksista säädetään niitä koskevissa laeissa.[28] BfV:n ja osavaltioiden yleisten turvallisuuspalveluiden toiminnasta säädetään liittovaltion perustuslainsuojasta annetussa laissa[29], johon sisältyvä yleinen tiedustelutoiminnan sääntely koskee myös BND:n ja MAD:n toimintaa.

BND toimii liittokanslerinviraston alaisuudessa ja raportoi sille toiminnastaan. BND:n tehtävänä on kerätä ja analysoida sellaisia ulkomaita koskevia tietoja, joilla voi olla merkitystä Saksan ulko- ja turvallisuuspolitiikalle. BND saa kerätä, käsitellä ja käyttää ulkomaan tiedustelussa tarpeellisia tietoja, mukaan lukien henkilötiedot, ellei tietojen käsitteleminen ole vastoin tietosuojalain tai muun erityissääntelyn määräyksiä. BND voi hyödyntää käytössään olevia tiedustelukeinoja, jos tarvittavaa tietoa ei voida saada muilla tavoin ja mikään muu viranomainen ei ole vastuussa sen keräämisestä.

BND voi käyttää toiminnassaan salaisen tiedonhankinnan menetelmiä, välineitä ja laitteita, mikäli se on välttämätöntä tehtävien suorittamiseksi. Henkilötietojen käsittelemisestä ja asianomaisen tiedonsaantioikeudesta säädetään tarkemmin perustuslainsuojalaissa.

Laissa kirje-, posti- ja puhelinsalaisuuden rajoittamisesta (G 10-laki)30 säädetään BND:n, MAD:n ja BfV:n oikeudesta valvoa ja tallentaa televiestintää sekä avata ja tarkistaa kirje- ja

27 Evalutiecommissie Wet op de inlichtingen– en veiligheidsdiesten 2002.

28 Gesetz über den Bundesnachrichtendienst, BND-laki, BNDG ja Gesetz über den militärischen Abschirmdienst, MAD-laki, MADG.

29 Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz, Bundesverfassungsschutzgesetz, BVerfSchG.

30 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses.

postilähetyksiä. Laki sisältää säännökset Saksan perustuslain 10 artiklan31 mukaisten perusoikeuksien rajoituksista, rajoitusedellytyksistä sekä rajoittamismenettelystä, yksityiselämän ydinalueen suojasta sekä henkilötietojen luovuttamisesta. Tämän lisäksi laissa säädetään tiedustelutoiminnan valvonnasta.

G 10 -laissa säädetään myös erikseen BND:n oikeudesta hankkia tietoja kansainvälisestä tietoliikenteestä. Tiedonhankinnan on oltava välttämätöntä ja siihen on haettava lupa, jonka myöntämisestä päättää liittovaltion ministeri yhteistyössä jäljempänä käsiteltävän G 10 -komission kanssa. Kansainvälisiin tietoliikenneyhteyksiin kohdistuvassa tiedustelussa käytettävien automaattisten hakuehtojen on oltava määritelty sekä lupahakemuksessa että luvassa. Hakuehdot voivat liittyä ainoastaan laissa erikseen lueteltujen uhkien[32] selvittämiseen. Tiedustelu- ja turvallisuuspalvelut saavat lain nojalla kohdistaa hakuehtoperusteista seulontaa enimmillään 20 %:iin kansainvälisestä tietoliikenteestä.

Henkilötiedustelussa tiedustelu- ja turvallisuuspalvelut saavat hankkia tietoja henkilölähteiltä ja ohjata niitä sekä käyttää vääriä henkilötietoja ja harhauttavia rekisterimerkintöjä.

Keskeisimmät valvontatoimielimet ovat parlamentaarinen valvontalautakunta[33] ja G 10 -komissio. Muita valvovia tahoja ovat tietosuojavaltuutettu ja BND:tä valvova liittokanslerinvirasto.

Parlamentaarinen valvontalautakunta valvoo kaikkien kolmen tiedustelua suorittavan viranomaisen toimintaa, siltä osin kuin kyse ei ole suoraan G 10 -lain tarkoittamista tilanteista. Lautakunnalla on tehtäviensä puitteissa yleinen tiedonsaantioikeus sekä oikeus suorittaa tarkastuksia ja katselmuksia tiedustelu- ja turvallisuuspalveluiden toimitiloissa. Valvontalautakunta antaa määräajoin selvityksen toiminnastaan liittovaltiopäiville.

G 10 -komissio valvoo viestintäsalaisuuden rajoittamista. Komissio päättää viran puolesta tai kanteluiden perusteella perustuslain 10 artiklan rajoitusten luvallisuudesta ja välttämättömyydestä. Komission valvonta kohdistuu tiedusteluviranomaisten henkilötietojen käsittelyyn sekä siitä ilmoittamiseen asianosaisille. Komissiolla on tehtäviensä puitteissa yleinen tiedonsaantioikeus sekä oikeus suorittaa tarkastuksia ja katselmuksia tiedustelu- ja turvallisuuspalveluiden toimitiloissa.

Tietosuojavaltuutettu valvoo tietosuojalainsäädännön soveltamista.

31 Kirje-, posti- ja puhelinsalaisuus.

32 Perusoikeuksia rajoittava tiedonhaku on G 10-lain 5 §:n mukaan sallittua vain, jos tieto on välttämätöntä seuraavien uhkien tunnistamiseksi: a) Saksaan kohdistuva aseellinen hyökkäys, b) Saksaan välittömästi liittyvä kansainvälinen terrori-isku, c) sotilasaseiden kansainvälinen levittäminen sekä huomattavaa merkitystä omaava aseiden, tietojenkäsittelyohjelmien ja teknologian laiton ulkomaankauppa, d) sellainen ammattimaisen tai järjestäytyneen rikollisuuden organisoima huumeiden tuonti EU:n alueelle, jolla on huomattavaa merkitystä Saksalle, e) ulkomailta tapahtuva euron arvon horjuttaminen, f) huomattavaa merkitystä omaava kansainvälisesti organisoitu rahanpesu tai g) ammattimaisen tai järjestäytyneen rikollisuuden organisoima ulkomaalaisten henkilöiden salakuljetus EU:n alueelle.

33 Gesetz über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes.

5. NYKYTILAN ARVIOINTI

Kansallisesta turvallisuudesta vastaavien viranomaisten tehtävänä on ennakoida ja ennalta estää toimialallaan sellaisia vahingollisia tekoja ja toimenpiteitä, jotka voivat vaarantaa erityisen tärkeiksi miellettyjä kansallisia etuja. Suomeen voidaan kohdistaa vakavia turvallisuusuhkia Suomen rajojen ulkopuolelta. Tietoverkkojen kehitys on vähentänyt fyysisen etäisyyden merkitystä uhkien toteuttamisessa.

Kansallisesta turvallisuudesta vastaavat viranomaiset harjoittavat lakisääteisten tehtäviensä hoitamisen edellyttämää tiedustelua. Tiedustelua varten ei kuitenkaan ole laissa säädettyjä toimivaltuuksia. Tiedustelu perustuu yksinomaan julkisiin lähteisiin sekä kansainvälisen ja muun vapaaehtoisen yhteistyön puitteissa saataviin tietoihin.

5.1 Sähköinen viestintäteknologia ja kansalliseen turvallisuuteen kohdistuvat uhat

Mietinnön jaksossa 2 ilmenevällä tavalla tieto- ja viestintäteknologian kehityksellä on kahtalainen merkitys kansalliseen turvallisuuteen kohdistuvien uhkien muotoutumisen kannalta.

Tietoverkkoja hyödynnetään välineenä viestiä sellaisista suunnitelmista ja aikeista, jotka koskevat reaalimaailmassa toteutettavia tekoja. Tietoverkkoja ei tässä tapauksessa hyödynnetä tekovälineenä vaan suunnittelun ja valmistelun välineenä. Teot voivat olla luonteeltaan sotilaallisia (aseellinen hyökkäys) tai ne voivat kohdistua muihin kansallisiin etuihin kuin valtion alueelliseen koskemattomuuteen (vakoilu, terrori-isku, kaksikäyttötuotteiden maastavienti).

Toisaalta tietoverkkoja hyödynnetään varsinaisena tekovälineenä kohdistaa kohteeseen - esimerkiksi Suomen valtioon - tätä vakavasti vahingoittavia tekoja. Kyse voi olla esimerkiksi Suomen kyberturvallisuusstrategian tarkoittamista sotilaallisista kyberoperaatioista taikka kybervakoiluksi tai kyberterrorismiksi luonnehdittavista teoista.

Tietoverkkouhkien ja uhkia koskevan viestinnän havaitseminen, niiden taustalla olevien tahojen tunnistaminen ja uhan luonteen selvittäminen muodostaa edellytyksen sille, että kansallista turvallisuutta vaarantavien tekojen toteutuminen voidaan estää. Torjunnasta vastaavan tahon on mahdollisimman varhaisessa vaiheessa saatava tieto uhista tai niitä koskevasta viestinnästä.

5.2 Organisaatioiden mahdollisuudet havainnoida niihin kohdistuvia tietoverkkouhkia

Tietoverkkojen käyttäjinä olevat yritykset, yhteisöt ja viranomaiset suojautuvat tietoverkkouhilta tietoturvan avulla. Toimintaoikeuksista tietoturvasta huolehtimiseksi säädetään tietoyhteiskuntakaaren 272 §:ssä. Säännös antaa yrityksille, yhteisöille ja viranomaisille työkaluja niihin kohdistuvien kybertekojen havaitsemiseksi ja torjumiseksi. Havainnointitoimenpiteet suoritetaan hajautetusti, jolloin niiden laatu ja taso vaihtelevat organisaatiokohtaisesti. Tietoyhteiskuntakaaren 272 § sekä sen edeltäjä SVTSL 20 § ovat mahdollistaneet myös tietoturvauhkien keskitetyn havainnointijärjestelmän (HAVARO) kehittämisen yhteiskunnan kokonaisturvallisuuden kannalta merkittävimpien tahojen suojaksi.

Haittaohjelmista vaikeimmin havaittavia ja samanaikaisesti suurinta vahinkoa kansalliselle turvallisuudelle aiheuttavia ovat valtiolliset vakoilu- ja muut haittaohjelmat. Tällaisia

haittaohjelmia koskevat tunnisteet ovat sellaista korkean suojaustason tietoa, jota vaihdetaan tyypillisesti osana turvallisuus- ja tiedustelupalveluiden kansainvälistä yhteistyötä. Koska Viestintävirasto ei ole eikä voi olla osapuolena tässä luottamuksellisessa yhteistyössä, HAVARO-järjestelmään ei voida luovuttaa niitä tunnisteita, joiden merkitys kansallisen turvallisuuden suojaamiseksi on suurin.

Tietoyhteiskuntakaaren 272 §:n mahdollistamien tietoturvatoimenpiteiden, HAVARO mukaan lukien, tarkoituksena on toteuttaa tietoturvaa suojaamalla yksittäisiä kohdeorganisaatioita niihin kohdistuvilta loukkauksilta. Tietoturvatoimenpiteiden tarkoituksena ei ole kattaa niitä tiedontarpeita, jotka liittyvät kansallista turvallisuutta vaarantavan toiminnan torjuntaan. Tietoturvatoimenpiteiden suorittajan näkökulmasta sellaiset kansallisen turvallisuuden ylläpitämisen kannalta olennaiset tiedot, kuten vakavimpien tietoturvaloukkausten syyt, olosuhteet, tekijät ja taustamotiivit, eivät ole keskeisiä.

5.3 Tiedonhankintatoimivaltuudet

Poliisin ja puolustusvoimien toimivalta käyttää salaisia tiedonhankintakeinoja on lainsäädännössä sidottu rikoksen käsitteeseen. Rikoksen estämisellä tarkoitetaan poliisilaissa 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. Salaisia tiedonhankintakeinoja voidaan käyttää valmistelun estämiseksi siinäkin tapauksessa, että asianomaisen rikoksen valmistelua ei ole kriminalisoitu.

Vaikka salaisia tiedonhankintakeinoja voidaan käyttää myös rikoksen valmistelun estämiseksi ja keinojen käyttöala on siten laaja, on selvää, ettei salaisia tiedonhankintakeinoja voida nykyisin käyttää pelkän tiedustelutiedon hankkimiseen sellaisesta esimerkiksi kansallista turvallisuutta uhkaavasta toiminnasta, joka ei ole edennyt rikoksen valmistelun asteelle tai ei ole säädetty rangaistavaksi.

5.4 Havaintoja kansainvälisestä vertailusta

Kaikissa mietinnössä tarkastelluissa verrokkimaissa säädetään tiedustelusta. Tiedustelua koskevaan lainsäädäntöön voi sisältyä säännöksiä tietoverkkoympäristön kautta tapahtuvasta tiedonhankinnasta. Sääntelytarkkuus vaihtelee maittain. Tästä syystä kaikkien verrokkimaiden lainsäädännöistä ei voida suoraan tehdä johtopäätöksiä käytössä olevista yksittäisistä tiedonhankintamenetelmistä. Myös siinä on eroja, miten tarkasti ne uhat, joiden torjumista varten tiedonhankintaa saa toteuttaa, on yksilöity lain tasolla.

Verrokkimaissa tiedustelutoiminnasta vastaa joko yksi tiedusteluviranomainen tai vaihtoehtoisesti toimivalta on jaettu siviili- ja sotilastiedustelupalveluiden kesken. Tiedustelutoimivaltuuksien jakaminen siviili- ja sotilasviranomaisten välillä perustuu pääsääntöisesti siihen, onko kyse siviili- vai sotilaallisluontoisesta uhasta. Tiedustelupalvelut toimivat yleensä puolustusministeriön ja/tai sisäasiainministeriön johdossa ja ohjauksessa. Tiedonhankintatoimeksiannot voivat tulla valtiojohdolta, ohjaavilta ministeriöiltä tai esimerkiksi puolustusvoimien johdolta.

Verrokkimaissa on katsottu tärkeäksi säätää tiedustelutoiminnan valvonnasta. Valvonnan muotoina ovat hallinnonalan sisäisen valvonnan lisäksi sekä parlamentaarinen että ulkopuolinen oikeudellinen valvonta. Oikeudellista valvontaa toteuttaa tiedustelupalvelusta riippumaton taho. Kyse voi olla esimerkiksi pysyvästä itsenäisestä valvontakomiteasta tai tarkastuslautakunnasta. Valvontaelimen tehtävänä on tyypillisesti joko oma-aloitteisesti tai kanteluiden johdosta valvoa toiminnan lainmukaisuutta sekä tiedonhankinnassa käytettäviä menetelmiä. Valvontaa suorittavilla elimillä on tyypillisesti rajoittamaton pääsy tiedustelupalvelun tiloihin ja asiakirjoihin. Valvontaelinten jäseniä sitoo vaitiolovelvollisuus. Valvontaelimet raportoivat yleensä havainnoistaan sekä yksittäistapauksissa että vuosiraporteissaan tiedustelutoimintaa ohjaavalle ministerille ja valvonnan kohteelle. Oikeudellisen valvonnan tavoitteena on myös turvata Euroopan ihmisoikeussopimuksen mukainen yksilön oikeussuoja.

Lisäksi vertailumaiden lainsäädäntöön sisältyy säännöksiä esimerkiksi yksityisyyden suojaa rajoittavien tiedustelumenetelmien viimesijaisuudesta, niiden käyttöön liittyvistä lupamenettelyistä sekä hankittujen henkilötietojen käsittelystä.

5.5 Turvallisuusviranomaisten tehtävien ja toimivaltuuksien suhde

Mietinnön jaksossa 3.1. on käsitelty Suojelupoliisin ja puolustusvoimien tehtäviä. Yhteisenä piirteenä tehtäville on, että ne koskevat kansalliseen turvallisuuteen kohdistuvien uhkien torjuntaa. Uhkien torjuminen edellyttää, että ne kyetään havaitsemaan ja niistä saadaan tietoa riittävän varhain.

Suojelupoliisin tehtävänä on rikosten estämisen, paljastamisen ja vähäisemmässä määrin selvittämisen ohella torjua sellaisia hankkeita, jotka voivat vaarantaa valtio- ja yhteiskuntajärjestystä tai valtakunnan sisäistä tai ulkoista turvallisuutta. Hankkeen käsitettä ei täsmennetä poliisin hallinnosta annetussa laissa tai sen esitöissä. Hankkeissa ei voida katsoa olevan kyse rikoksista, mistä johtuen viraston tehtävässä tältä osin on kyse tiedustelullisesta eikä rikostorjunnallisesta toimeksiannosta. Tiedustelua koskevista toimivaltuuksista ei ole säännöksiä.

Puolustusvoimissa rikostorjunnasta - rikosten estämisestä ja paljastamisesta - vastaa sotilasvastatiedustelu. Sotilasvastatiedustelusta erillinen asia on sotilastiedustelu, jonka yleisenä tehtävänä on sotilasstrategisen tilannekuvan muodostamiseksi seurata Suomen turvallisuusympäristön kehitystä, määrittää ympäristön muutokset ja tuottaa tietoa vallitsevasta tilanteesta. Sotilastiedustelun tiedonhankinnan kohteena on erityisesti lähialueen sotilaspoliittinen ja sotilaallinen kehitys. Sotilastiedustelun tehtävät eivät ole rikostorjuntaa. Sotilastiedustelusta ei ole lainsäädäntöä.

Kansalliseen turvallisuuteen kohdistuvia uhkia torjuvien viranomaisten tiedustelutoimivallasta ja tämän toimivallan jakautumisesta siviili- ja sotilasviranomaisten välillä ei ole säännöksiä. Nykysääntelyssä viranomaisten tiedonhankintatoimivaltuudet perustuvat tiedustelun sijaan yksinomaan rikostorjuntaan.

Muuttuneeseen turvallisuusympäristöön liittyvät epävarmuustekijät korostavat tarvetta tuottaa objektiivista, varmennettua ja analysoitua tietoa Suomeen kohdistuvista turvallisuusuhkista sekä poliittisen päätöksenteon että turvallisuusviranomaisten päätöksenteon tueksi. Vain todenmukainen ja mahdollisimman varhaisessa vaiheessa saatava tieto uhkien taustatahojen aikeista ja suunnitelmista takaa riittävän kyvyn varoittaa näistä ennakolta. Varhaisvaiheen tiedonsaanti parantaa suomalaisen yhteiskunnan mahdollisuuksia varautua uhkiin ja laajentaa sitä keinovalikoimaa, jonka avulla uhkien toteutuminen voidaan estää. Myös poikkeusoloihin

varautumisen näkökulmasta on välttämätöntä, että tieto Suomeen kohdistuvista sotilaallisista uhista pystytään hankkimaan jo normaalioloissa.

Nykytilaa voidaan pitää epätyydyttävänä ottaen huomioon ne muutokset, joita turvallisuusympäristössä on tapahtunut. Suomalaisen yhteiskunnan toimivuus tulisi turvata erityisen vakavia ulkoisia uhkia sekä kriittiseen infrastruktuuriin kohdistuvia tekoja vastaan. Kansallisen turvallisuuden näkökulmasta keskeistä on saada riittävän varhaisessa vaiheessa tietoa Suomen turvallisuusympäristössä tapahtuvista muutoksista, ei ainoastaan esitutkinnan toteuttamiseen pyrkivä tiedonhankinta. Keskeistä olisi hankkia tietoa vallitsevasta tilanteesta ja analysoida sen merkitystä Suomen kansallisen turvallisuuden kannalta.

6. KEHITTÄMISEHDOTUKSET

Suomen ulkoinen turvallisuusympäristö ja sodankäynnin luonne muuttuvat kiihtyvällä vauhdilla. Tämän vuoksi viranomaisten tiedonhankintamenetelmiä tulee kehittää. Nykyisillä toimivaltuuksilla ei voida riittävän tehokkaasti ja varhaisessa vaiheessa havaita uhkia eikä ryhtyä niiden edellyttämiin toimenpiteisiin, mukaan lukien sotilaallisen ennakkovaroituksen antaminen. Väärän tiedon levittäminen ja käyttäminen korostavat turvallisuusviranomaisten tarvetta tuottaa objektiivista, varmennettua ja analysoitua tietoa ylimmän valtionjohdon ja sotilaallisen päätöksenteon tueksi.

Tiedustelu on laaja kokonaisuus, johon kuuluu useita eri tiedustelumenetelmiä. Kuten kansainvälisestä vertailusta käy ilmi, valtiot eivät tyypillisesti säädä ainoastaan yhdestä tiedustelumenetelmästä. Millään yksittäisellä tiedustelumenetelmällä ei saada välttämättä kansallista turvallisuutta koskevaa kaikkea tarpeellista tietoa vaan tieto joudutaan hankkimaan ja varmistamaan useilla toisiaan tukevilla tiedustelumenetelmillä.

Jäljempänä kuvataan kolmea sellaista tiedustelumenetelmää, jotka työryhmän arvion mukaan tuottaisivat erityisen merkityksellistä tietoa Suomen kansallisen turvallisuuden näkökulmasta. Nämä ovat tietoliikennetiedustelu, ulkomaan henkilötiedustelu sekä ulkomaan tietojärjestelmätiedustelu. Tiedustelumenetelmät eivät korvaa toisiaan, koska ne ovat luonteeltaan osittain erilaisia. Tietoliikennetiedustelulla on ennen kaikkea tarkoitus havaita kansainvälisiä uhkia. Ulkomaan henkilötiedustelulla ja ulkomaan tietojärjestelmätiedustelulla hankittaisiin pääasiassa tietoa jo tunnistetuista uhista.

6.1 Tietoliikennetiedustelu

6.1.1 Yleistä

Viestintään kohdistuvalla tiedustelulla on mietinnön jaksossa 2 käsitellyistä muutoksista johtuen keskeinen rooli kansalliseen turvallisuuteen kohdistuvien uhkien havaitsemisessa. Valtaosa maailmanlaajuisesta viestinnästä yksityisten henkilöiden, yritysten ja julkisten toimijoiden välillä välittyy nykyisin kiinteässä tietoliikenneverkossa. Suomen alueella olevat tietoliikennelaitteet ja -kaapelit välittävät maan sisäisen viestiliikenteen ohella kansainvälistä viestiliikennettä. Kansainvälinen viestiliikenne pitää sisällään Suomesta lähtevän ja Suomeen päättyvän rajat ylittävän liikenteen sekä kansainvälisen kauttakulkuliikenteen, jonka alku- ja päätepiste sijaitsevat Suomen ulkopuolella. Viestintätekniikan kehittymisen johdosta juuri tietoliikennekaapeleissa välittyvä tieto on keskeistä uhkien havaitsemisessa.

Kaapelivälitteisen tietoliikenteen merkitys kansalliseen turvallisuuteen kohdistuvien uhkien torjunnan kannalta on tunnistettu useissa Suomeen verrattavissa olevissa länsimaissa. Kansainvälisestä vertailusta käy ilmi, että useimpien verrokkimaiden lainsäädäntö mahdollistaa viranomaisten oikeuden kohdistaa tiedustelua kaapeliverkkoihin tai tällaista lainsäädäntöä suunnitellaan.

Tietoliikennetiedustelussa on kyse siitä, että viranomainen hankkii kansallisen turvallisuuden kannalta olennaista tietoa tietoliikenteestä ja sen sisällöstä. Tietoliikennetiedustelu voi yleisesti kohdistua valtion sisäiseen tai rajat ylittävään tietoliikenteeseen. Toiminnan toteuttaminen edellyttää, että tiedusteluviranomaisella on pääsy tietoliikennekaapeleiden liityntäpisteisiin. Tyypillisesti tiedustelutiedon hankintaa suunnataan tietoliikennettä seulovien automatisoitujen hakuehtojen avulla. Tällöin tietoliikennetiedustelulla rajoitetaan luottamuksellisen viestin suojaa. Kehittämisehdotuksia harkittaessa on otettava huomioon Suomea velvoittavat kansainväliset sopimukset ja perustuslain vaatimukset.

6.1.2 Kansainvälisten ihmisoikeussopimusten ja perustuslain vaatimukset

6.1.2.1 Kansalaisoikeuksia ja poliittisia oikeuksia koskeva Yhdistyneiden Kansakuntien yleissopimus

YK:n yleiskokouksen vuonna 1966 hyväksymä kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (ns. KP-sopimus; SopS 8/1976) tuli Suomea sitovaksi vuonna 1976.

Luottamuksellisen viestinnän suojan kannalta keskeinen on sopimuksen 17 artikla, jonka mukaan kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä. Lisäksi jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan. Artiklan mukaisesta velvoitteesta voidaan poiketa ainoastaan yleisen hätätilan aikana, joka uhkaa kansallista olemassaoloa ja joka on virallisesti sellaiseksi julistettu.

KP-sopimuksen 17 artiklan määräämä kielto puuttua yksityiselämään ja kirjeenvaihtoon ei ole ehdoton, vaan kielto koskee ”mielivaltaista” ja ”laitonta” oikeuksiin puuttumista. Sopimusvaltiot voivat kansallisessa lainsäädännössään säätää puuttumisen oikeuttavista tilanteista ja puuttumisessa käytettävistä keinoista. Kaikki sopimusvaltiot ovatkin säätäneet rikostorjuntatarkoituksessa tapahtuvasta oikeuksiin puuttumisesta ja monet myös kansallisen turvallisuuden ylläpitämisen tarkoituksessa tapahtuvasta oikeuksiin puuttumisesta.

KP-sopimuksen täytäntöönpanoa valvoo YK:n ihmisoikeuskomitea, joka jatkuvasti kehittää sopimusmääräysten tulkintaa. Ihmisoikeuskomitean yleiskommentissa nro 16 vuodelta 1988 (A/43/20) tulkitaan 17 artiklan sisältöä muun muassa sähköisen viestinnän näkökulmasta. Kommentin mukaan riittävää ei ole, että yksityiselämän suojaan puuttumisesta on säädetty lailla. Puuttumisen oikeuttava lainsäädäntö ei saa olla sisällöltään mielivaltainen eikä sen soveltaminen mielivaltaista. Lainsäädännön on oltava KP-sopimuksen määräysten ja tavoitteiden mukainen, ja siinä on tarkoin yksilöitävä olosuhteet, joissa puuttuminen on sallittu. Yksityisyyden suojaan puuttuvaa toimenpidettä koskeva päätös tulee voida tehdä ainoastaan tapauskohtaisesti ja laissa määrätyn viranomaisen toimesta, ja niiden tietojen, joita puuttumisen avulla kerätään, on oltava yhteiskunnan etujen kannalta välttämättömiä (”essential in the interests of society”). Henkilön yksityiselämään liittyviä tietoja ei saa käyttää KP-sopimuksen kanssa ristiriidassa oleviin tarkoituksiin.

Yksityisyyden suojaa koskevan 17 artiklan loukkauksista on tehty useita valituksia KP-sopimuksen valinnaisen pöytäkirjan nojalla, mutta komitea ei toistaiseksi ole käsitellyt tietoverkkoturvallisuuteen ja sähköiseen viestintään liittyviä asioita. Todennäköisenä voidaan pitää, että sähköisen viestinnän luottamuksellisuuteen liittyvät kysymykset nousevat näkyvämmin esille ihmisoikeuskomitean työssä[34].

6.1.2.2 Euroopan ihmisoikeussopimuksen 8 artikla

Tietoliikennetiedustelusta säätämisen sallittavuutta arvioitaessa on KP-sopimusta suurempi käytännön merkitys Euroopan neuvoston piirissä vuonna 1950 tehdyllä Euroopan ihmisoikeussopimuksella (EIS; SopS 63/1999), johon Suomi liittyi vuonna 1989. Ihmisoikeussopimuksen noudattamista valvoo Euroopan ihmisoikeustuomioistuin (EIT), joka tässä tarkoituksessa käsittelee ja ratkaisee sopimusrikkomuksia koskevia valituksia. EIT on lukuisissa ratkaisuis-

34 Esimerkiksi Yhdysvaltojen neljäs määräaikaisraportti KP-sopimuksen täytäntöönpanosta (CCPR/C/USA/4) käsittelee yksityiskohtaisesti sähköisen tietoliikenteen valvontaa. Yhdysvalloille osoittamissaan lisäkysymyksissä komitea pyytää lisätietoja National Security Agencyn suorittaman sähköisen tiedonvälityksen oikeudellista valvonnasta niin valtion alueella kuin sen ulkopuolellakin (CCPR/C/USA/Q/4).

saan ottanut kantaa siihen, miten ihmisoikeussopimuksen mukaista oikeutta luottamuksellisen viestin suojaan tulisi tulkita. Monet näistä ratkaisuista koskevat sähköistä viestintää ja muutamat tietoliikennetiedustelua tai siihen läheisesti rinnastuvia viranomaistoiminnan muotoja.

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

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

Viranomaisen ei tarvitse tosiasiassa käsitellä tietoja, jotta kyse olisi yksityiselämään puuttumisesta, vaan puuttumiseksi on katsottava jo se, että viranomainen kerää ja tallentaa niitä myöhempää käyttöä varten (*Marper v. Yhdistynyt Kuningaskunta*). Pelkkä sellaisen lainsäädännön olemassaolokin, joka mahdollistaa viestintäyhteyksien salaisen tarkkailun, puuttuu viestinnän osapuolten ja potentiaalistenkin osapuolten EIS 8 artiklan takaamiin oikeuksiin (*Klass v. Saksa, Liberty ja muut v. Yhdistynyt Kuningaskunta*). Valvonnan potentiaalisilla kohteilla on tällöin oltava oikeus EIS 13 artiklan takaamaan tehokkaaseen oikeussuojakeinoon kansallisen viranomaisen edessä. EIS 13 artiklan mukaan jokaisella, jonka yleissopimuksessa tunnustettuja oikeuksia ja vapauksia on loukattu, on oltava käytettävissään tehokas oikeussuojakeino kansallisen viranomaisen edessä siinäkin tapauksessa, että oikeuksien ja vapauksien loukkauksen ovat tehneet virantoimituksessa olevat henkilöt.

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

Sallittu puuttuminen EIS 8(1) artiklan mukaisiin oikeuksiin

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

Vaatimus puuttumisen perustumisesta lakiin

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

EIT on ratkaisuissaan toistuvasti korostanut sitä, että yksityiselämän suojaan puuttuvat salaiset viranomaistoimenpiteet mahdollistavan lain on oltava oikeusvaltioperiaatteiden mukainen, kansalaisten saatavilla sekä laadultaan sellainen, että kansalaiset kykenevät ennakoimaan sen soveltamisen seuraukset omalta osaltaan (mm. *Kruslin v. Ranska, Huvig v. Ranska, Lambert v. Ranska*). Sen on oltava tarpeeksi selkeä [”sufficiently clear in its terms”] antaakseen riittävän osoituksen [”an adequate indication”] siitä, missä olosuhteissa ja millä edellytyksillä kansalaiset voivat joutua salaisten viranomaistoimenpiteiden kohteeksi (*Kopp v. Saksa, Kruslin v. Ranska, Huvig v. Ranska*). Laki ei voi olla sellainen, että se mahdollistaa salaisen tarkkailun kohdistamisen sattumanvaraisesti keneen tahansa (*Amann v. Sveitsi*).

Arvioitaessa sitä, täyttyykö ennakoitavuusvaatimus, on huomioon otettava kansanedustuslaitoksen säätämän varsinaisen lain ohella myös asetukset ja viranomaismääräykset. Varsinaisen lain hyvinkin yleistasoisia säännöksiä voidaan täsmentää alemmantasoisin instrumentein. Näiden tulee kuitenkin olla julkistettuja - sellaiset sisäiset viranomaismääräykset, jotka eivät ole kansalaisten saatavilla, eivät täytä ennakoitavuusvaatimusta (*esim. Silver ja muut v. Yhdistynyt Kuningaskunta, Malone v. Yhdistynyt Kuningaskunta*). Yleisesti saatavilla olevan lain tulee määritellä ainakin salaisesti käytettävien tarkkailuvaltuuksien laatu ja laajuus; niiden henkilöiden kategoriat, joita vastaan valtuuksia voidaan käyttää; sen toiminnan luonne, joka antaa aiheen valtuuksien käyttöön; valtuuksien avulla hankittuja tietoja tutkittaessa, hyödynnettäessä, tallennettaessa, edelleen jaettaessa ja poistettaessa noudatettavat menettelyt; säännökset valtuuksien valvonnasta ja niitä koskevista oikeussuojakeinoista (*Amann v. Sveitsi, Valenzuela Contreras v. Espanja, Prado Bugallo v. Espanja, Shimovolos v. Venäjä*). Lainsäädännön ennakoitavuudelle asetettavat vaatimukset ovat siitä riippumattomia, onko kyse yksittäisten henkilöiden viestiyhteyksiä koskevasta rikosperusteisesta tarkkailusta vai laajamittaisesta viestiyhteyksien uhkaperusteisesta yleisvalvonnasta (*Weber ja Saravia v. Saksa*, *Liberty ja muut v. Yhdistynyt Kuningaskunta*).

EIT on arvioinut kansainvälisten viestiyhteyksien laajamittaisen yleisvalvonnan ihmisoikeussopimuksen mukaisuutta kahdessa tärkeässä ratkaisussaan. Tapauksessa *Liberty ja muut v. Yhdistynyt Kuningaskunta* se katsoi yleisvalvonnan mahdollistavan kansallisen lainsäädännön olevan laadultaan sellainen, ettei se täyttänyt EIS 8(2) artiklassa asetettua vaatimusta salaisen tarkkailun perustumisesta lakiin. Tapauksessa *Weber ja Saravia v. Saksa* se päätyi päinvastaiseen tulokseen - kansallinen lainsäädäntö täytti lain laadulle asetettavat vaatimukset ja oli siten ihmisoikeussopimuksen mukainen.

Tapauksessa *Liberty ja muut v. Yhdistynyt Kuningaskunta* kyse oli Iso-Britannian puolustusministeriön alaisen signaalitiedustelulaitoksen suorittamasta laajamittaisesta ulkomaan puhelinliikenteen valvonnasta, jonka puitteissa pystyttiin kuuntelemaan samanaikaisesti jopa 10 000 puhelinlinjaa. Asiassa oli sinänsä riidatonta, että toiminta perustui kansalliseen lakiin.[35] Kyseisen lain mukaan sisäministeri saattoi antaa eri turvallisuusviranomaisille luvan [”warrant”] kohdistaa tiedonhankintaa Iso-Britannian ja ulkomaiden välisiin viestiyhteyksiin. Lu-

35 Interception of Communications Act 1985

vissa ne viestiyhteydet, joihin tiedonhankintaa voitiin kohdistaa, määriteltiin hyvin yleisellä tasolla (esimerkiksi ”kaikki Iso-Britannian ja muun Euroopan välisten merikaapelien kautta välittyvät viestit”). Luvan myöntämisen yhteydessä sisäministerin oli määriteltävä se aineisto, jota tiedonhankinta koski. Lain mukaan määrittelyksi kuitenkin riitti se, että hankittavat tiedot sisäministerin käsityksen mukaan olivat tarpeen joko kansallisen turvallisuuden ylläpitämisen, vakavan rikollisuuden ennalta estämisen tai paljastamisen taikka maan taloudellisten etujen turvaamisen kannalta. Luvan myöntäessään sisäministerin tuli myös antaa tarpeellisina pitämänsä salassa pidettävät määräykset sen varmistamiseksi, että luvan alaan kuulumattomia viestejä ei tarkastettu ja että tarkastettavia viestejä paljastettiin tai jäljennettiin vain tarpeellisessa laajuudessa. Laissa ei ollut tarkempia säännöksiä näiden määräysten sisällöstä tai alasta. Luvan sisäministeriltä saatuaan turvallisuusviranomaiset muotoilivat itsenäisesti ne automaattiset hakuehdot, joiden avulla kansallista turvallisuutta tai muita laissa mainittuja intressejä koskevat tiedot suodatettiin viestinnän kokonaismassasta. Turvallisuusviranomaisilla oli omat sisäiset määräyksensä siitä, millä perusteilla suodatuksen tuloksena saatuja tietoja käsiteltiin, tallennettiin, jaettiin ja poistettiin, mutta nämä määräykset eivät olleet julkisia tai yleisesti saatavilla.

Asiassa antamassaan ratkaisussa EIT totesi, että sisäministerin lupapäätöksen alaan voitiin lain mukaan sisällyttää millainen viesti tahansa, minkä johdosta kenen tahansa henkilön maan ulkopuolelle lähettämä tai sieltä saama mikä tahansa viesti oli voitu siepata. Niin ollen toimeenpanovallalle oli ulkomaisten viestien sieppaamisen osalta myönnetty tosiasiassa rajoittamatonta harkintavaltaa. Laki myös jätti väljän harkintamarginaalin sen suhteen, mitkä viestit tosiasiassa tarkastettiin. Riittävää tässä suhteessa oli, että sisäministeri piti tarkastamista tarpeellisena kansallisen turvallisuuden tai muiden laissa mainittujen yleisesti muotoiltujen etujen kannalta. Laissa ei ollut tarkempia säännöksiä luvan alaan kuulumattomien viestien käsittelystä eivätkä sisäministerin asiasta antamat määräykset olleet julkisia. Yhteenvetona EIT totesi, että kansallisella lailla ei ollut osoitettu riittävän selkeästi toimeenpanovallalle viestien sieppaamista ja tarkastamista varten myönnetyn hyvin väljän harkintavallan rajoja. Varsinkaan ei ollut osoitettu julkisesti, miten siepatun aineiston seulonta, käyttö, säilytys ja hävittäminen oli toimitettava. Näin ollen Iso-Britannian signaalitiedustelulainsäädäntö ei vastannut EIS 8(2) artiklan asettamia laatuvaatimuksia ja ihmisoikeussopimusta oli rikottu.

Tapauksessa *Weber ja Saravia v. Saksa* kyse oli Saksan tiedustelupalvelu BND:n harjoittamasta Saksan ja ulkomaiden välisen matkapuhelinliikenteen laajamittaisesta niin sanotusta strategisesta valvonnasta, josta oli säädetty kansallisessa laissa.[36] Kyseisen lain mukaan matkapuhelinliikenteen strategista valvontaa saatiin harjoittaa eräiden kansalliseen turvallisuuteen kohdistuvien erikseen mainittujen uhkien torjumiseksi. Tällaisia laissa määriteltyjä uhkia olivat Saksaan kohdistuva sotilaallinen hyökkäys, Saksassa toteutettavat luonteeltaan kansainväliset terroriteot, kansainvälinen aseiden salakuljetus, huumeiden laajamittainen maahantuonti, ulkomailla tapahtuva rahan väärentäminen ja edellä mainittuihin ilmiöihin liittyvä rahanpesu. Luvan kunkin strategisen valvontatehtävän suorittamiseen myönsi liittovaltion ministeri kuultuaan lupahakemuksen johdosta ensin parlamentaarista valvontaelintä. Niiden automaattisten hakuehtojen, joiden avulla matkapuhelinliikennettä oli tarkoitus suodattaa, oli käytävä ilmi sekä BND:n lupahakemuksesta että ministerin myöntämästä luvasta. Laki sisälsi säännökset siitä, kuinka suodatettua aineistoa oli käsiteltävä ja missä tapauksissa suodatuksen myötä esiinnousseita henkilöitä koskevia tietoja saatiin käyttää rikosten ennalta estämistä, paljastamista ja selvittämistä varten. Laki sisälsi samoin säännökset siitä, milloin suodatettua tietoa oli pidet-

36 Gesetz für Beschrenkung des Brief-, Post- und Fernmeldegeheiminisse 1968 ja Verbrechenbekämpfungsgesetz 1994.

tävä asiaankuulumattomana ja miten asiaankuulumattoman tiedon suhteen oli meneteltävä. Edelleen laissa säädettiin valvontalupien voimassaoloajoista, suodatettujen tietojen säilyttämisajoista, tietojen hävittämisestä sekä niistä perusteista ja edellytyksistä, joilla tietoja voitiin luovuttaa muille viranomaisille.

EIT katsoi, että Saksan lainsäädäntö täytti EIS 8(2) artiklan nojalla laille asetettavat laatu- ja ennakoitavuusvaatimukset. Keskeistä tässä suhteessa oli muun muassa se, että laki määritteli ne uhat, joiden torjumiseksi valvontaa voitiin harjoittaa. Lain katsottiin myös tarjoavan riittävän osoituksen siitä, mihin henkilöluokkiin valvonta voitiin lainmukaisesti kohdistaa.[37] Valvonnan kohdentamiseksi käytettävien automaattisten hakuehtojen tuli suoraan lain nojalla ilmetä valvontaa varten myönnettävistä luvista, jolloin valvontaa harjoittavalla viranomaisella ei ollut rajoittamatonta harkintavaltaa niiden määrittelemisessä. Ennakoitavuusvaatimuksen täyttymisen kannalta merkityksellistä oli myös se, että laki määritteli lupien maksimaaliset voimassaoloajat ja sisälsi säännökset niistä menettelyistä, joita oli noudatettava tietoja tarkastettaessa ja hyödynnettäessä. Samoin merkitystä EIT:n mukaan oli sillä, että laki sääti niistä rajoituksista ja ehdoista, joita tietojen edelleen luovuttamisessa oli noudatettava, sekä niistä olosuhteista, joissa tiedot oli hävitettävä. *Weber ja Saravia* -tapauksen johdosta antamassaan ratkaisussa EIT totesi erikseen myös sen, ettei Saksan maaperällä harjoitettava viestiyhteyksien yleisvalvonta lähtökohtaisesti voi loukata muiden maiden valtiosuvereniteettia vaikka viestiyhteyksien toinen osapuoli jossain tällaisessa muussa maassa oleskelisikin.

Kansallinen turvallisuus puuttumisen oikeuttavana intressinä

Kansallinen turvallisuus on yksi niistä eduista, joka EIS 8(2) artiklan mukaan voi oikeuttaa puuttumisen yksityiselämän suojaan. EIT on oikeuskäytännössään vain harvoin kyseenalaistanut vastaajavaltioiden väitteet siitä, että puuttuminen on tapahtunut kansallisen turvallisuuden vuoksi.[38] Valtioilla vaikuttaisi olevan varsin laaja harkintamarginaali sen suhteen, millaisen toiminnan ne katsovat vaarantavan kansallista turvallisuuttaan ja siten voivan oikeuttaa EIS 8 artiklan takaamiin oikeuksiin puuttumisen. Taustalla on se, että kansallinen turvallisuus kuuluu perinteisesti valtiosuvereenisuuden piiriin (*Bucur ja Toma v. Romania*). Tuomioistuimen ratkaisukäytännön perusteella on selvää, että ainakin sotilaallinen maanpuolustus, terrorismin torjunta ja laittoman tiedustelutoiminnan torjunta kuuluvat kansallisen turvallisuuden piiriin (mm. *Klass v. Saksa, Weber ja Saravia v. Saksa*). Kansalliseen turvallisuuteen saattaa kuitenkin kohdistua monenlaisia uhkia, joita on vaikea ennakoida tai määritellä etukäteen. Tästä seuraa, että käsitteen selventäminen on ensisijaisesti jätettävä kansallisen käytännön varaan (*Kennedy v. Yhdistynyt Kuningaskunta*). Valtioiden harkintavaltaa saattaa omalta osaltaan lisätä se, että kansallisen turvallisuuden raja muihin sallittuihin perusteisiin (mm. yleinen turvallisuus ja epäjärjestyksen tai rikollisuuden estäminen) puuttua EIS 8(1) artiklan takaamiin oikeuksiin, voidaan tapauskohtaisesti mieltää häilyväksi.[39]

37 ”Satelliitin avulla välittyviin kansainvälisiin matkapuhelinkeskusteluihin osallistuvat henkilöt, joiden keskusteluiden sisältö on sellainen, että se Saksaan kohdistuvaan sotilaalliseen hyökkäykseen, kansainväliseen terrorismiin yms. liittyvän automaattisen hakuehdon perusteella suodattuu jatkotarkasteluun”.

38 EIT on tosin suhtautunut epäilevästi esimerkiksi siihen, voiko vuotta 1937 koskevilla tiedoilla henkilön poliittisesta suuntautumisesta olla merkitystä kansalliselle turvallisuudelle kuusikymmentä vuotta myöhemmin (Rotaru v. Romania). Se on myös esimerkiksi katsonut, ettei ainakaan savukkeiden salakuljetus voi kuulua kansallisen turvallisuuden alaan vaikka salakuljetuksessa olisi käytetty hyväksi sotilaslentokenttää (Dumitru Popescu v. Romania).

39 Tällaiseen etujen osittaiseen limittymiseen viitataan esim. ratkaisussa Silver ja muut v. Yhdistynyt Kuningaskunta.

Puuttumisen välttämättömyys demokraattisessa yhteiskunnassa

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

Välttämätön demokraattisessa yhteiskunnassa -edellytys pitää sisällään sen, että oikeuksiin puuttumisen tulee vastata pakottavaan yhteiskunnalliseen tarpeeseen (*correspond to a pressing social need*). Edellytyksestä seuraa myös, että puuttumisen on oltava suhteellisuusperiaatteen mukaista: puuttumisen on oltava järkevässä suhteessa siihen EIS 8(2) artiklan sallimaan tavoitteeseen, johon vedotaan oikeuttamisperusteena (mm. *Gillow v. Yhdistynyt Kuningaskunta*, *Silver ja muut v. Yhdistynyt Kuningaskunta, Handyside v. Yhdistynyt Kuningaskunta*).

Puuttumisen välttämättömyyden arviointi niin yhteiskunnallisen tarpeen pakottavuuden kuin suhteellisuudenkin näkökulmasta kuuluu ensisijaisesti tai ainakin ensi vaiheessa kansalliselle lainsäätäjälle ja kansallisille viranomaisille (*Silver ja muut v. Yhdistynyt Kuningaskunta, Handyside v. Yhdistynyt Kuningaskunta*). Tätä arviointia suorittaessaan kansallisilla tahoilla on tiettyä harkintamarginaalia, jonka laajuutta määrittää muun muassa se, mitä EIS:n takaamaa oikeutta puuttuminen koskee, se, kuinka syvällekäyvästä puuttumisesta on kyse, sekä se, mikä EIS 8(2) artiklan sallima tavoite on puuttumisen oikeuttamisperusteena. Harkintamarginaali on tavanomaista väljempi silloin, kun oikeuttamisperusteena on kansallinen turvallisuus (*Klass ja muut v. Saksa, Leander v. Ruotsi*). Kansallisen turvallisuuden kysymyksissä valtion melko laaja harkintavalta koskee myös niitä konkreettisia keinoja ja menetelmiä, joiden avulla se kyseistä etua suojaa. Ratkaisussaan *Weber ja Saravia v. Saksa* EIT katsoi, että valtio sille kuuluvan harkintavallan puitteissa oli voinut säätää laajamittaisesta viestintäyhteyksien valvonnasta menetelmänä suojata kansallista turvallisuuttaan. Kyse oli demokraattisessa yhteiskunnassa välttämättömästä puuttumisesta EIS 8 artiklan yksityisille oikeussubjekteille takaamiin oikeuksiin.

Toiselta puolen EIT on korostanut, että kansallisen turvallisuuden nimissä käytettävät viranomaisten salaiset tarkkailu- ja valvontavaltuudet saattavat muodostaa vaaran demokraattiselle yhteiskuntajärjestykselle (mm. *Antunes Rocha v. Portugali*). Tästä syystä valtion tulee järjestää niiden käytön riippumaton valvonta ja tehokkaat oikeussuojakeinot. Laillisuusvalvontaa suorittavien tahojen ratkaisuilla tulisi olla oikeudellisesti sitova vaikutus suhteessa valvottuihin tahoihin - demokratian suojelemisen kannalta riittävää ei ole, että laillisuusvalvojat voivat ohjata valvomiaan tahoja suositusten avulla (*Segerstedt-Wiberg ja muut v. Ruotsi*). Salaisia valtuuksia koskevan oikeudellisen sääntelyn tulee olla julkista ja siinä määrin täsmällistä, että laillisuusvalvontaa voidaan uskottavasti suorittaa (*Liberty ja muut v. Yhdistynyt Kuningaskunta*), kuitenkaan salaisen tiedonhankinnan tarkoitusta vaarantamatta (*Segerstedt-Wiberg ja muut v. Ruotsi*). Demokratian suojelemisen kannalta merkitystä on myös sillä, että kansanedustuslaitos osaltaan osallistuu salaisten tarkkailuvaltuuksien valvontaan (*Campbell v. Yhdistynyt Kuningaskunta, Leander v. Ruotsi*).

6.1.2.3 Euroopan unionin perusoikeuskirja

Vuonna 2009 voimaantullut Euroopan unionin perusoikeuskirja määrittelee unionin tasolla pätevät perusoikeudet. Jäsenvaltiot ovat velvollisia noudattamaan perusoikeuskirjaa aina, kun ne soveltavat unionin oikeutta. Perusoikeuskirjan 7 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa sekä viesteihinsä kohdistuvaa kunnioitusta. Perusoikeuskirjan 8 artiklan mukaan puolestaan jokaisella on oikeus henkilötietojensa suojaan. Henkilötietojen suojaan kuuluvien tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava laissa määritettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty ja saada ne oikaistuiksi. Riippumattoman viranomaisen on valvottava näiden sääntöjen noudattamista.

Perusoikeuskirjan 52 artikla määrää perusoikeuskirjalla turvattujen oikeuksien kattavuudesta. Artiklan 1 kappaleen mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttämistä voidaan rajoittaa ainoastaan lailla, ja kyseisten oikeuksien ja vapauksien olennaista sisältöä noudattaen. Suhteellisuusperiaatteen mukaisesti rajoituksia voidaan tehdä ainoastaan, jos ne ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia. Saman artiklan 3 kappaleen mukaan, siltä osin kuin perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamista koskevassa eurooppalaisessa yleissopimuksessa taattuja oikeuksia, niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa. Tämä ei kuitenkaan estä unionia määräämästä tätä laajemmasta suojasta.

Perusoikeuskirjan 52 artiklan 3 kohdasta seuraa, että perusoikeuskirjan 7 artiklan sisältö vastaa EIS 8 artiklan sisältöä. Perusoikeuskirjan johdannossa todetaan erikseen, että vahvistettavat oikeudet perustuvat paitsi Euroopan ihmisoikeussopimukseen, myös Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön. EIT:n laajalla ihmisoikeussopimuksen 8 artiklaa koskevalla ratkaisukäytännöllä on näin ollen katsottava olevan relevanssia myös perusoikeuskirjan 7 artiklan tulkinnalle.

Perusoikeuskirjan mukaisten perusoikeuksien kunnioittamisen valvonta ei edellä sanotusta huolimatta kuulu EIT:lle vaan Euroopan unionin tuomioistuimelle (EUT) ja kansallisille tuomioistuimille. Tietoliikennetiedustelun kannalta merkitystä on EUT:n huhtikuussa 2014 antamalla tuomiolla[40], jolla tuomioistuin julisti pätemättömäksi vuonna 2006 säädetyn Data Retention -direktiivin. Direktiivi oli asettanut unionin jäsenvaltioille velvoitteen säätää teletunnistamistietojen kattavasta säilyttämisestä vakavien rikosten torjunnan ja tutkinnan tarpeita varten.

EUT katsoi edellä mainitussa tuomiossaan, että Data Retention -direktiivi oli perusoikeuskirjan 52 artiklan 1 kappaleessa tarkoitetun suhteellisuusperiaatteen vastainen. Suhteellisuusperiaate pitää sisällään sen, että perusoikeuden rajoitus on välttämätön. Arvioidessaan Data Retention -direktiivillä tapahtuneen oikeuksien rajoittamisen välttämättömyyttä EUT kiinnitti huomiota siihen, että direktiivin säätämä teletunnistamistietojen säilyttämisvelvoite kattoi kaikki henkilöt, kaikki sähköisen viestinnän tavat ja lähes kaikki tunnistamistiedot ilman minkäänlaista vakavan rikollisuuden ehkäisemisen tavoitteeseen perustuvaa erottelua, rajaamista tai poikkeusta. Säilyttämisvelvollisuuden piirissä olivat myös kaikkien sellaisten henkilöiden teletunnistamistiedot, joiden osalta ei ole mitään näyttöä edes etäisestä tai epäsuorasta kytkennästä rikollisuuteen. Näin ollen direktiivin oli katsottava puuttuvan käytännössä jokaisen EU:n alueella oleskelevan henkilön oikeuksiin.

40 Tuomio yhdistetyissä asioissa C-293/12 ja C-594/12.

EUT:n mukaan direktiivin olisi tullut sisältää ainakin osa[41] seuraavista elementeistä ollakseen suhteellisuusperiaatteen mukainen:

- Jonkinlaiset direktiivin tavoitteeseen liittyvät objektiiviset rajat sille, keiden henkilöiden teletunnistamistiedot saadaan säilyttää.
- Tarkemman määrittelyn niistä rikoksista, joiden torjumiseksi tai tutkimiseksi kansalliset viranomaiset saavat säilytettyihin tunnistamistietoihin tutustua ja niitä käyttää. Direktiivi viittaa tältä osin ainoastaan ”vakaviin rikoksiin”, joiden sisältö määräytyy kunkin jäsenvaltion kansallisen lainsäädännön mukaan.
- Aineelliset ja menettelylliset edellytykset tietoihin tutustumiselle ja niiden käytölle. Tietoihin tutustumisen edellytykseksi ei ole direktiivissä asetettu esimerkiksi tuomioistuimen tai muun riippumattoman elimen lupaa, vaan menettelystä päättäminen on siinä jätetty kansallisten säädösten varaan.
- Tarkemmat säännökset tunnistamistietojen säilyttämisajoista. Direktiivissä säädetään vähimmäissäilytysajaksi kuusi kuukautta tekemättä mitään eroa sen suhteen, voivatko tiedot olla rikostorjunnassa hyödyllisiä.
- Tehokkaan tietosuojan varmistamiseksi riittävät takeet siitä, että säilytettäviä tietoja ei väärinkäytetä. Direktiivi sallii sen, että teleyritykset huomioivat taloudelliset näkökohdat määrittäessään soveltamansa turvan tason.
- Määräykset siitä, että tiedot on säilytettävä unionin alueella.

Eduskunnan perustuslakivaliokunta on lausunnossaan PeVL 18/2014 vp esittänyt EUT:n tuomiota koskevia huomioita. Valiokunnan mukaan tuomiosta ei voida suoraan johtaa vastausta siihen, millainen kansallinen lainsäädäntö täyttäisi yksityiselämän ja henkilötietojen suojaan liittyvät oikeasuhtaisuusvaatimukset. Lähtökohtana on valiokunnan mukaan kuitenkin pidettävä sitä, että oikeasuhtaisuusvaatimuksen vastaisena voidaan pitää ainakin sellaista sääntelyä, joka merkitsee laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tietojen säilyttämistä yhdistettynä viranomaisten erittelemättömään ja rajoittamattomaan pääsyyn näihin tietoihin. Perustuslakivaliokunta totesi myös, että tuomion perusteella jää avoimeksi, merkitseekö viranomaistarpeita varten säädetyn säilyttämisvelvollisuuden ulottuminen käytännössä kaikkien sähköisiä viestimiä käyttävien ihmisten tietoihin jo yksinään oikeasuhtaisuusvaatimuksen loukkausta.[42]

Tuomiossaan EUT totesi, että direktiivin olisi tullut asettaa tavoitteeseensa liittyvät objektiiviset rajat sille, keiden henkilöiden tunnistamistiedot saadaan säilyttää. Lisäksi direktiivin olisi tullut tarkemmin määritellä ne rikokset, joiden torjumiseksi säilyttämisvelvollisuus asetettiin. Tärkeää on tältä osin tiedostaa, ettei EUT:n tuomio varsinaisesti luo uutta oikeutta. Se vastaa Euroopan ihmisoikeustuomioistuimen vakiintunutta ratkaisukäytäntöä. Ihmisoikeustuomioistuin on antanut suurehkon määrän ratkaisuja, joissa se EUT:n tuomiota vastaavalla tavalla mutta yksityiskohtaisemmin on käsitellyt niitä elementtejä, jotka yksityiselämän suojaan puuttuvan lain on sisällettävä ollakseen suhteellisuusperiaatteen mukainen ja ennakoitava. Merkittävimpiä tässä suhteessa ovat ihmisoikeustuomioistuimen tietoliikennetiedustelua tai sen lähi-ilmiöitä suoraan koskeneet ratkaisut *Klass vastaan Saksa* (1978), *Weber ja Saravia vastaan Saksa* (2006) ja *Liberty ja muut vastaan Yhdistynyt Kuningaskunta* (2008).)

41 Perustuslakivaliokunnan kannanoton mukaan unionin tuomioistuimen tuomio perustuu kokonaisarvioon käsiteltävänä olleesta direktiivistä (PeVL 18/2014 vp, s.6).

42 PeVL 18/2014 vp, s. 6.

6.1.2.4 Suomen perustuslaista johtuvia vaatimuksia luottamuksellisen viestinnän suojaa rajoittavalle lainsäädännölle

Oikeusvaltioperiaate

Perustuslain 2 §:n 3 momentin mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia. Jos tiedustelulainsäädännöllä luodaan viranomaisille uusia tehtäviä ja niihin liittyviä toimivaltuuksia, on sekä tehtävistä että toimivaltuuksista säädettävä lailla. Samalla on riittävällä sääntelyllä taattava viranomaistoimivaltuuksien kohteena olevien henkilöiden oikeusturva.

Perusoikeudet

Perusoikeudet eivät yleensä ole ehdottomia, vaikka perusoikeussäännös olisi kirjoitettu oikeuden turvaavaan muotoon ja vaikka säännös ei sisältäisikään sääntelyvarausta tai muuta lakiviittausta. Tällöin kysymys perusoikeuden rajoittamisesta ratkaistaan perusoikeuksien rajoittamista koskevien yleisten oppien mukaisesti.

Perustuslakivaliokunta on johtanut perusoikeusjärjestelmän kokonaisuudesta ja oikeuksien luonteesta perustuslaissa turvattuina oikeuksina joitakin yleisiä perusoikeuksien rajoittamista koskevia vaatimuksia (PeVM 25/1994 vp s. 4 – 5). Näitä ovat vaatimukset:

1. lailla säätämisestä
2. lain täsmällisyydestä ja tarkkarajaisuudesta
3. rajoituksen hyväksyttävyydestä
4. rajoituksen suhteellisuudesta
5. perusoikeuden ydinalueen koskemattomuudesta
6. oikeusturvajärjestelyjen riittävyydestä ja
7. ihmisoikeusvelvoitteiden noudattamisesta.

Luottamuksellisen viestin salaisuuden suoja

Perustuslain 10 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu ja kirjeen, puhelun sekä muun luottamuksellisen viestin salaisuus on loukkaamaton. Säännöksen lähtökohtana on, että yksilöllä on oikeus elää elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä. Pykälä turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä[43].

Perustuslain 10 §:n 3 momentin mukaan 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. Nämä mahdollisuudet rajoittaa luottamuksellisen viestin suojaa on perusoikeusuudistuksen yhteydessä tarkoitettu tyhjentäväksi luetteloksi (HE 309/1993 vp, s. 54). Esimerkiksi Euroopan ihmisoikeussopimuk-

43 HE 309/1993 vp.

sen 8 artiklasta poiketen perustuslain 10 §:n 3 momentti ei mainitse kansallista turvallisuutta sellaisena etuna, joka oikeuttaisi säätämään lailla luottamuksellisen viestin salaisuuden rajoittamisesta.

Perustuslakivaliokunta on katsonut, että rikosten tutkinnasta perustuslain 10 §:n 3 momentin tarkoittamassa merkityksessä voi olla kysymys myös sellaisissa tapauksissa, joissa on esillä konkreettinen ja yksilöity rikosepäily, vaikka rikos ei vielä olisi ehtinyt toteutuneen teon asteelle.[44]

Perustuslain säännös luottamuksellisen viestin salaisuudesta on muotoiltu väline- ja tekniikkaneutraaliksi. Kirje- ja puhelinsalaisuus on mainittu erikseen, mutta säännös turvaa yleisesti kaikenlaisen luottamuksellisen viestinnän salaisuutta.[45]

Luottamuksellisen viestin salaisuutta koskevan perustuslakisääntelyn ensisijaisena tarkoituksena on suojata luottamukselliseksi tarkoitetun viestin sisältö ulkopuolisilta. Perustuslaki turvaa jokaiselle oikeuden luottamukselliseen viestintään ilman, että ulkopuoliset saavat oikeudettomasti tiedon hänen lähettämiensä tai hänelle osoitettujen luottamuksellisten viestien sisällöstä. Tämä merkitsee esimerkiksi suojaa kirjeiden tai muiden suljettujen viestien avaamista tai hävittämistä sekä puhelujen kuuntelemista tai nauhoittamista vastaan. Sääntely ei suojaa ainoastaan viestin lähettäjää, vaan kysymyksessä on viestinnän molempien osapuolten perusoikeus.[46]

Säännös ei suojaa tavallisen kuuloetäisyydellä käytävän, aistihavainnoin kuultavissa olevan keskustelun sisältöä, mutta luottamukselliseksi tarkoitetun keskustelun kuunteleminen teknisin apuvälinein merkitsee rajoitusta luottamuksellisen viestin salaisuuden suojaan.[47]

Perustuslakisääntelyllä ei ole pyritty järjestämään viestinnän osapuolten keskinäisiä suhteita tai heidän käyttäytymistään. Kysymys luottamuksellisen viestinnän osapuolen oikeudesta julkistaa luottamukselliseksi tarkoitettu viesti on jäänyt ratkaistavaksi muilla perusteilla.[48]

Luottamuksellisen viestin tunnistamistiedot

Viestin sisällön lisäksi perustuslain säännökset suojaavat myös viestin lähettäjän ja vastaanottajan tunnistamistietoja sekä muita tietoja, joilla voi olla merkitystä viestin luottamuksellisuuden säilymiselle. Viestin tunnistamistietojen on perustuslakivaliokunnan vakiintuneessa käytännössä katsottu jäävän luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle[49]. Tuoreessa lausunnossaan valiokunta on kuitenkin katsonut, että käytännössä viestien tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, ettei katego-

44 PeVL 19/2008 vp, s. 3-4, PeVL 11/2005 vp, s. 3, PeVL 9/2004 vp, s. 3, PeVL 37/2002 vp, s. 3, PeVL 26/2001 vp, s. 3, PeVL 2/1996 vp

45 HE 309/1993 vp, s.53.

46 HE 309/1993 vp, s. 53-54, PeVL 28/2000 vp, s. 3, PeVL 30/2001 vp, s. 2, PeVL 54/2001 vp, s. 4, PeVL 13/2003 vp, s. 4-5, PeVL 9/2004 vp, s. 3-4, PeVL 10/2004 vp, s. 4-5, PeVL 16/2004 vp, s. 6, PeVL 59/2006 vp, s. 2, PeVL 19/2008 vp, s. 3.

47 HE 309/1993 vp, s. 53, PeVL 11/2005 vp, s. 4, PeVL 36/2002 vp, s. 6, PeVL 2/1996 vp, PeVL 5/1999 vp, s. 4.

48 HE 309/1993 vp, s. 54.

49 PeVL 6/2012 vp, s. 3–4, PeVL 67/2010 vp, s. 4, PeVL 66/2010 vp, s. 7, PeVL 62/2010 vp, s. 4, PeVL 29/2008 vp, s. 2, PeVL 3/2008 vp, s. 2, PeVL 59/2006 vp, s. 2, PeVL 23/2006 vp, s. 2-3, PeVL 11/2005 vp, s. 4, PeVL 10/2004 vp, s. 4, PeVL 9/2004 vp, s. 4, PeVL 37/2002 vp, s. 3, PeVL 26/2001 vp, s. 3, PeVL 5/1999 vp, s. 7, PeVL 26/1998 vp, s. 2-3, PeVL 7/1997 vp, PeVL 47/1996 vp.

rinen erottelu suojan reuna- ja ydinalueeseen ole aina perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen[50].

Tunnistamistietojen salaisuuden suojaan puuttuvan sääntelyn on täytettävä perusoikeuksien rajoittamisen yleiset edellytykset[51]. Perustuslakivaliokunnan käytännössä on tältä pohjalta pidetty mahdollisena, että tunnistamistietojen saaminen rikosten tutkinnassa jätetään sitomatta tiettyihin rikostyyppeihin, jos sääntely muutoin täyttää perusoikeuksien yleiset rajoitusedellytykset.[52] Sääntely tulee tällöin kuitenkin rajata yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tyyppisiin tai niihin törkeysasteeltaan verrattaviin rikoksiin.[53]

6.1.2.5 Toimenpiteet tietoturvan toteuttamiseksi

Tietoliikennetiedustelua teknisesti lähellä oleva tilanne voidaan katsoa olevan tietoyhteiskuntakaaren 272 §:ssä. Säännöksessä on kyse toimenpiteistä tietoturvan toteuttamiseksi ja se antaa teleyritykselle, lisäarvopalvelun tarjoajalle ja yhteisötilaajalle oikeuden muun muassa automaattisesti analysoida kaikkien niiden viestien sisältöä, jotka kulkevat kyseisen yhteisön verkosta ulos tai tulevat siihen sisään. Säännöksen 3 momentin mukaan:

> ”Jos viestin tyypin, muodon tai muun vastaavan seikan perusteella on ilmeistä, että viesti sisältää haitallisen tietokoneohjelman tai käskyn eikä 2 momentin 1 kohdassa *(sisällön automaattinen selvittäminen)* tarkoitetulla toimella pystytä turvaamaan 1 momentissa tarkoitettujen tavoitteiden toteutumista, yksittäisen viestin sisältöä saa käsitellä manuaalisesti. - -”

Niistä tarkoituksista, joiden turvaamiseksi edellä mainittuihin toimenpiteisiin voidaan ryhtyä, säädetään 1 momentissa. Turvattavat edut näyttäisivät liittyvän vain osaksi rikostorjuntaan.

Tarkoituksia ovat:

> ”1) viestintäverkkojen tai niihin liitettyjen palvelujen sekä tietojärjestelmien tietoturvalle haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi;
> 2) viestin lähettäjän tai viestin vastaanottajan viestintämahdollisuuksien turvaamiseksi; tai
> 3) viestintäpalvelujen kautta laajamittaisesti toteutettavien rikoslain 37 luvun 11 §:ssä tarkoitettujen maksuvälinepetosten valmistelun ehkäisemiseksi.”

Alun perin sääntely otettiin tietoyhteiskuntakaarta edeltäneeseen SVTSL:iin (20 §) vuonna 2004. Luottamuksellisen viestin sisältöön sai tuolloin puuttua vain säännöksessä mainittujen rikosepäilyjen (vaaran aiheuttaminen tietojenkäsittelylle ja tietoliikenteen häirintä) perusteella.

---

50 PeVL 18/2014 vp, s. 6.

51 PeVL 62/2010 vp, s. 4-5, PeVL 23/2006 vp, s. 3, PeVL 7/1997 vp

52 PeVL 29/2008 vp, s. 2, PeVL 11/2005 vp, s. 4, PeVL 9/2004 vp, s. 4, PeVL 26/2001 vp, s. 3, PeVL 37/2002 vp, vp, s. 3, PeVL 7/1997 vp.

53 PeVL 66/2010 vp, s. 7, PeVL 67/2010 vp, s. 4.

Tuolloista sääntelyä koskevan perustuslakivaliokunnan lausunnon mukaan sääntelyn keskeisenä tarkoituksena oli viestinnän eri osapuolten etujen mukaisesti turvata tietoverkkojen toimivuutta ja turvallisuutta sekä näin luoda edellytyksiä sananvapauden käyttämiselle ja viestinnän luottamuksellisuudelle tietoverkoissa. Perusoikeuksien käyttämiseen ja niiden toteutumisen edistämiseen tällä tavoin liittyvät seikat olivat perustuslakivaliokunnan mukaan hyväksyttäviä ja painavia perusteita tietoverkoissa harjoitettavaan viestintään kohdistuville rajoituksille. Luottamuksellisen viestin sisältöön sai puuttua vain säännöksessä mainittujen rikosepäilyjen perusteella. Tietoliikenteen ja tietoturvallisuuden vaarantumista voitiin pitää riskinä yksilön ja yhteiskunnan laajasti ymmärretyn turvallisuuden kannalta. Sääntely ei perustuslakivaliokunnan mielestä ollut käsillä olevassa yhteydessä lähtökohdiltaan ongelmallinen perustuslain 10 §:ssä turvatun luottamuksellisen viestin salaisuuden kannalta.[54]

Säännöstä muutettiin vuonna 2008. Tuolloin luovuttiin siitä, että viestin sisältöön puuttuminen sidotaan yksinomaan rikostunnusmerkistöihin. Säännöksen yksityiskohtaisten perusteluiden (HE 48/2008 vp) mukaan viestin sisältöön puuttumisen sitomisesta rikostunnusmerkistöihin seuraa, että analyysi voidaan tehdä vain silloin, kun teko on tahallinen. Käytännössä haitallisia viestejä ei aina lähetetä tahallisesti. Tietoturvan ylläpitämiseksi myös tahattomasti lähetetyt viestit, jotka aiheuttavat tietoturvalle vaaran, tulisi pystyä analysoimaan. Edelleen esitöissä todetaan tarve käsitellä yksittäisen viestin sisältöä manuaalisesti, jos on ilmeistä, ettei automaattisen tietojenkäsittelyn avulla pystytä turvaamaan ehdotetussa 1 momentissa tarkoitettujen tavoitteiden toteutumista. Tietoyhteiskuntakaaren kumoama SVTSL 20 § on säädetty perustuslakivaliokunnan myötävaikutuksella (PeVL 29/2008 vp), samoin tietoyhteiskuntakaari (PeVL 18/2014).

6.1.3 Kansallisen tietoliikennetiedustelun mahdollisia suuntaviivoja

Suomea velvoittavat kansainväliset ihmisoikeussopimukset sallivat tietyin reunaehdoin sekä sisäiseen että rajat ylittävään tietoliikenteeseen kohdistuvan tiedustelun. Mietinnön nykytilan kuvauksessa on todettu, että Suomen kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat ensisijaisesti ulkoisia. Tämän vuoksi Suomen tarpeet liittyvät rajat ylittävän tietoliikenteen tiedusteluun.

Tietoliikennetiedustelussa olisi kyse tiedustelutoimivaltuudesta, jonka tarkoituksena olisi tuottaa kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa ulkomaisista toimijoista ja olosuhteista ylimmän valtionjohdon päätöksenteon tueksi. Lisäksi tarkoituksena olisi havaita ja tunnistaa kansalliseen turvallisuuteen kohdistuvia vakavia ulkoisia uhkia sekä kerätä niistä sellaista tietoa, joka mahdollistaa tilannekuvan muodostamisen, torjuntatoimiin ryhtymisen sekä sotilasviranomaisten osalta ennakkovaroituksen antamisen. Tiedustelu ei ole samalla tavalla henkilö- ja rikossidonnaista toimintaa kuin rikosten ennalta estäminen. Tietoliikennetiedustelun kohteet olisivat yleisluonteisempia toimintatapoja kuin rikoslaissa tarkoitettuja rikollisia tekoja.

Tietoliikennetiedustelun yhteiskunnallisen hyväksyttävyyden keskeisenä edellytyksenä voidaan pitää sitä, että ne uhat, joita tiedonhankinta saa koskea, määritellään mahdollisimman selkeästi ja suppeasti. Kansainvälisten ihmisoikeussopimustenkaan mukaan tietoliikennetiedustelu ei voi olla keino hankkia tietoa mistä tahansa uhasta tai riskistä. Verrokkimaissa ne uhat ja tilanteet, joita tiedustelu saa koskea, on yleensä lueteltu laissa.

54 PeVL 9/2004 vp, s. 4

Tietoliikennetiedustelun avulla tunnistettavien uhkien tulisi olla riittävän vakavia ja kohdistua kansallisen turvallisuuden kannalta keskeisiin turvallisuusintresseihin. Uhat voisivat olla luonteeltaan joko sotilaallisia tai siviililuontoisia. Riittävän vakavina kansalliseen turvallisuuteen kohdistuvina uhkina voitaisiin pitää esimerkiksi Suomeen kohdistuvaa sotilaallista uhkaa, terrorismia ja siihen vaikutuksiltaan vertautuvaa toimintaa sekä vakoilua. Vakoilun havaitsemiseen ja tunnistamiseen tietoliikennetiedustelua tulisi voida käyttää riippumatta siitä, kohdistuuko se valtioon tai yksityiseen sektoriin. Tietoliikennetiedustelun avulla tulisi olla mahdollista kartoittaa uhan lähteitä ja ulkovaltojen vakoilussaan käyttämiä toimintatapoja.

Kansainvälinen järjestäytynyt rikollisuus voisi olla tietoliikennetiedustelun piirissä siltä osin, kun se vaarantaa kansallista turvallisuutta. Samoin tietoliikennetiedustelua tulisi voida käyttää joukkotuhoaseiden levittämisen estämiseksi tarvittavan tiedon hankkimiseksi.

Kansainväliset kriisinhallintaoperaatiot ovat kehittyneet vaativammiksi ja tämän kehityksen voidaan olettaa jatkuvan tulevaisuudessakin. Kriisinhallintaoperaatioiden turvallisuutta voitaisiin parantaa tietoliikennetiedustelulla saatavan tiedon avulla.

Tietoliikennetiedustelua tulisi voida käyttää kriittiseen infrastruktuuriin kohdistuvien vakavien uhkien havaitsemiseksi. Tällaiset uhat voivat tulla myös tietoverkkojen kautta.

Vieraiden valtioiden suunnitelmat, aikeet ja toimet saattavat eräissä tilanteissa vahingoittaa tai vaarantaa Suomen ulko- ja turvallisuuspoliittisia etuja. Tietoliikennetiedustelun avulla voitaisiin näissä tilanteissa varmistaa ylimmän valtionjohdon riittävä, luotettava ja oikea-aikainen tiedon saanti.

Tietyissä tilanteissa valtion sisäiset uhat voivat vakavuudeltaan ja vaikutuksiltaan rinnastua edellä käsiteltyihin uhkiin, ja niistä voitaisiin saada tietoa rajat ylittäviin tietoliikenneyhteyksiin kohdistuvan tiedustelun avulla. Vaikutuksiltaan riittävän vakavan teon osalta voidaan viitata Norjan vuoden 2011 joukkosurmiin.

Edellä jaksossa 6.1.2 on käsitelty kansallisen turvallisuuden käsitettä Euroopan ihmisoikeussopimuksen valossa. Työryhmän käsityksen mukaan edellä mainitun tapaiset uhat kuuluvat kansallisen turvallisuuden käsitteen alaan siten kuin esimerkiksi Euroopan ihmisoikeustuomioistuin on käsitettä tulkinnut.

Tiedustelun tarkoituksena olisi havaita, tunnistaa ja hankkia tietoa uhista. Sen sijaan tiedustelulla ei estettäisi uhkien toteutumista. Rajapinta tiedustelun ja torjuntatoimien välillä olisi järjestettävä erikseen. Tiedustelun tuottaman tiedon johdosta toimivaltaisen viranomaisen olisi voitava ryhtyä tarvittaviin toimiin uhan torjumiseksi. Jatkotyöskentelyssä olisi pohdittava, missä laajuudessa ja millä tavalla tiedustelutietoa voitaisiin siirtää käytettäväksi esimerkiksi rikoksen ennalta estämisessä.

Kansainväliset ihmisoikeussopimukset eivät näyttäisi asettavan kategorista estettä käyttää tietoliikennetiedustelua rikosten selvittämiseen. Selvänä lienee pidettävä sitä, ettei tietoliikennetiedustelu voisi olla tavanomaisena pidettävän verkko- tai muunkaan massarikollisuuden tutkintaa varten käytettävä menetelmä. Lähtökohdaksi voitaisiin ottaa se, ettei tietoliikennetiedustelua voida lainkaan käyttää rikostutkinnallisena menetelmänä. Tämän puolesta näyttäisivät puhuvan sekä yksilön oikeusturvaan että tietoliikennetiedustelun menetelmien salassa pidettävyyteen liittyvät syyt.

Tietoliikennetiedustelun varsinaisesta rikostutkinnallisesta käytöstä erillinen asia on, että toiminnan yhteydessä tiedusteluviranomaisen tietoon saattaa tulla tietoja, jotka viittaavat siihen, että rikos on tapahtunut. Jos kyse on erityisen vakavasta rikoksesta, olisi pohdittava, millä tavoin tieto siitä voitaisiin antaa esitutkintaviranomaiselle. Tällöinkään kyseessä ei saisi olla tietojen käyttö oikeusprosessissa vaan rikostutkinnan suuntaamisesta.

Jos tietoliikennetiedustelun yhteydessä havaitaan yksityiseen sektoriin kohdistuvia vakavia kybertekoja, tulisi harkita, millä tavoin näistä voitaisiin ilmoittaa teon kohteena olevalle yritykselle. Tavoitteena olisi minimoida elinkeinoelämälle ja kansantaloudelle aiheutuvat vahingot.

Lisäksi työryhmässä on tuotu esille, että olisi tarpeen analysoida tietoliikennevirtoja myös tietoliikennetiedustelun selektiivisyyden varmistamiseksi ja teknologisen kehityksen seuraamiseksi. Kyse olisi tietoliikennetiedustelujärjestelmän toimintakyvyn turvaamisesta. Jatkotyössä tulisi tarkastella, onko ja missä laajuudessa tällainen toiminta mahdollista järjestää ottaen huomioon kansainväliset ihmisoikeussopimukset sekä perustuslain vaatimukset.

6.1.4 Tietoliikennetiedustelun toteuttaminen

Tietoliikennetiedustelu tulisi toteuttaa siten, että tietoliikenteen joukosta voitaisiin seuloa mahdollisimman tehokkaasti tiedustelutehtävän kannalta olennainen liikenne ja estää tehtäviin kuulumattoman liikenteen päätyminen analysoinnin kohteeksi.

EIT:n mukaan laista on riittävän selkeästi käytävä ilmi, missä olosuhteissa ja millä edellytyksellä kansalaiset voivat joutua viranomaisten salaisesti toteutettavan tarkkailun kohteeksi. Lisäksi EUT:n Data Retention -tuomio edellyttää henkilötietojen käsittelyn rajaamista ennakkoon. Nämä reunaehdot on otettava huomioon tietoliikennetiedustelun toteuttamista harkittaessa.

Tietoliikenteestä on kyettävä erottamaan ne tiedot, joilla on merkitystä kansallisen turvallisuuden kannalta. Eräs tapa täyttää vaatimukset olisi käyttää toiminnan suuntaamiseen riittävän tarkkoja ennakkoon määrättyjä hakuehtoja tai kansallista turvallisuutta vaarantavan toiminnan sanallisia kuvailuja, jotka mahdollisimman konkreettisesti luonnehtisivat tiedonhankinnan kohdetta.

Kuvailun kohteena olisivat sellaiset viestinnälliset ja muut toimintamallit, joiden tiedetään tai voidaan olettaa liittyvän kansallista turvallisuutta vaarantavaan toimintaan. Toiminta voitaisiin järjestää esimerkiksi niin, että 6.1.6 jaksossa käsiteltävä lupaviranomainen hyväksyisi kuvailun tietoliikennetiedustelutehtävän perustaksi, minkä voidaan katsoa täyttävä ennakollisen rajaamisen vaatimuksen. Kuvailun perusteella tietoliikennetiedustelusta vastaava viranomainen muodostaisi tiedonhankinnan suuntaamisen kannalta välttämättömät hakuehdot. Viranomaisen muodostamien hakuehtojen käyttö olisi dokumentoitava kattavasti, mikä mahdollistaisi kattavan jälkikäteisen valvonnan.

Tietoliikennetiedustelun ensivaiheen toiminnassa käytettävät hakuehdot voisivat olla tunnistamistietoja. Tällaisia olisivat esimerkiksi verkkolaitteita ja verkko-osoitteita kuvaavat yksilöintitiedot sekä esimerkiksi viestinnän aikaa ja paikkaa kuvaavat tiedot. Jotta tietoliikennetiedustelun kohteena olevista uhista saataisiin riittävät tiedot, olisi hakuehtojen perusteella valikoidusta viestinnästä voitava selvittää myös sisältö.

Silloin, kun tietoliikennetiedustelun tarkoituksena on havaita haittaohjelmien avulla toteutettavaa tietoverkkovakoilua, tulisi myös sisältöön kohdistuvia hakuehtoja voida poikkeuksellisesti käyttää heti ensivaiheessa. Hakuehtona olisi tällöin tekninen haittaohjelmatunniste, ja toimintamalli olisi sama kuin tietoyhteiskuntakaaren 272 §:ssä säädetyssä toiminnassa.

Yksityisyyden suojaan kohdistuvaa rajoitusta voitaisiin lieventää sillä, että hakuehtojen mukainen seulonta tapahtuu ensivaiheessa koneellisesti. Hakuehtojen avulla viestinnän kokonaismassasta voitaisiin tarkoituksenmukaisella tavalla erottaa tiedustelutehtävän kannalta olennaiset tiedot. Tiedot olisivat otettavissa manuaalisen käsittelyn kohteeksi vasta koneellisesti suoritetun seulonnan jälkeen. Yksityisyyden suojan näkökulmasta olennaista olisi, että mikään

sellainen viesti tai viestin tunnistamistieto, joka ei vastaa hakuehtoa, ei päädy manuaaliseen käsittelyyn.

Tietoliikennetiedustelu, siten kuin se on yllä kuvattu, olisi useasta toinen toistaan seuraavasta työvaiheesta koostuva tiedustelun prosessi, jossa käsittelyn kohteena olevan viestinnän määrä prosessin edetessä jatkuvasti supistuu. Tallennettaviksi voisivat tällöin tulla ainoastaan ne viestinnän tiedot, jotka ovat läpäisseet prosessin jokaisen vaiheen. Muut tiedot hävitettäisiin eivätkä ne hävittämisen jälkeen enää olisi viranomaisten esiin haettavissa. Suomea sitovat kansainväliset ihmisoikeusvelvoitteet edellyttävät selkeiden menettelytapojen luomista tietojen käsittelylle.

Tietoliikennetiedustelu rajoittaisi eri vaiheissaan eri laajuudessa luottamuksellisen viestin suojaa. Tietoliikennetiedustelun alkuvaiheessa hakuehtoja verrattaisiin kaikkiin niihin viesteihin, jotka liikkuvat kohteeksi valikoiduissa tietoliikennevirroissa. Myös se tietoliikenteen valtaosa, jolla ei ole merkitystä kansallisen turvallisuuden kannalta, olisi automaattisesti suoritetun vertailun kohteena. Tässä vaiheessa vertailu voisi perustua muun tietoliikenteen kuin haittaohjelmaliikenteen osalta tunnistamistietoihin. Vertailu tapahtuisi automatisoidusti eivätkä hakuehtoja vastaamattomat viestit tulisi manuaaliseen käsittelyyn. Toiminnassa käytettävien automaattisten hakuehtojen täsmällisyyden aste vaikuttaa riskiin siitä, seuloontuuko myös sivulliseksi katsottavaa viestintää manuaalisen jatkokäsittelyn kohteeksi. Mitä täsmällisempiä hakuehdot ovat, sitä vähäisempi on vaara, että tiedustelutehtävät kannalta epäolennaista tietoa suodattuu jatkokäsittelyyn.

Tietoliikennetiedusteluprosessin seuraava vaihe sisältäisi syvällekäyvemmän, mutta olennaisesti suppeampaan henkilöpiiriin kohdistuvan viestinnän luottamuksellisuuden rajoituksen. Käytettyjen hakuehtojen perusteella suodatettu viestintä otettaisiin tällöin manuaalisen analysoinnin kohteeksi. Manuaalisen käsittelyn kohteeksi nouseva tietoliikenne on tiedustelutehtävän kannalta lähtökohtaisesti merkittävää, ja viestin sisältö tulisi voida tarvittaessa selvittää.

Tietoliikennetiedustelun järjestäminen siten kuin edellä on esitetty, ei edellyttäisi laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tunnistamistietojen tallentamista, vaan kyse olisi ennakkoon määritettyihin hakuehtoihin perustuvasta tietoliikenteen suodattamisesta ja siihen perustuvasta kansallisen turvallisuuden kannalta olennaisten tietojen tallentamisesta.[55] Tallennettavat tiedot voisivat enimmilläänkin muodostaa vain vähäisen murto-osan rajat ylittävän viestinnän kokonaisvolyymista.

Tietoliikennetiedustelun järjestäminen edellyttäisi, että teleyrityksille tai rajat ylittävien tietoliikennekaapeleiden omistajille asetetaan velvoite osoittaa liityntäpisteet sekä antaa tämän edellyttämät tiedot tietoliikennetiedustelun toteuttamisesta vastaavalle viranomaiselle. Toteuttamisella ei saataisi aiheuttaa yleisen tietoliikenteen hidastumista. Liityntä tulisi suunnitella yhteistyössä teleyritysten kanssa siten, että niille koituvat haitat minimoitaisiin. Lähtökohtaisesti teknisestä toiminnasta yrityksille mahdollisesti aiheutuvat suorat kustannukset katettaisiin tietoliikennetiedustelua käyttävien tahojen puolelta.

55 PeV on lausunnossaan PeVL 18/2014 vp katsonut ainakin tällaisen tunnistamistietojen tallentamisen suhteellisuusperiaatteen vastaiseksi.

6.1.5 Tietoliikennetiedustelun hallinnollisen järjestämisen suuntaviivoja

Edellä mietinnön 6.1.3 jaksossa on käsitelty niitä uhkia, joista tietoliikennetiedustelulla olisi kansallisen turvallisuuden vuoksi tarpeen hankkia tietoa. Näiden uhkien seuranta kuuluu voimassa olevan lainsäädännön perusteella eri viranomaisille. Tiedonhankinta sotilaallisista uhista kuuluu puolustusvoimille, kun taas mietinnössä tarkoitettujen siviililuonteisten uhkien seuranta kuuluu pääasiassa Suojelupoliisille. Keskusrikospoliisi torjuu kansainvälistä järjestäytynyttä rikollisuutta. Viranomaisten välistä tehtäväjakoa ei työryhmän näkemyksen mukaan ole tarpeen muuttaa.

Ei ole tarkoituksenmukaista, että tiedustelutietoa tarvitsevat viranomaiset harjoittaisivat tietoliikennetiedustelua kukin erikseen, vaan toiminnan olisi syytä perustua keskitettyyn ratkaisuun. Keskitetyssä ratkaisussa tietoliikennetiedustelun tekninen toteuttaminen osoitettaisiin yhdelle viranomaiselle (*tietoliikennetiedusteluviranomainen*), joka muiden tietoliikennetiedustelutietoon oikeutettujen viranomaisten (*toimeksiantajaviranomaiset*) toimeksiannosta hankkii niiden tarvitsemat tietoliikennetiedustelutiedot. Keskitettyä ratkaisua puoltaisivat toiminnan yhdenmukaisuudelle ja salassa pidettävyydelle asetettavat vaatimukset, toiminnan edellyttämä erikoistuminen ja tekninen osaaminen, sekä toiminnan lainmukaisuuden valvontaan liittyvät näkökohdat. EIT on edellyttänyt selkeiden menettelyiden luomista toiminnalle sekä sen lainmukaisuuden kattavaa laillisuusvalvontaa. Näistä voidaan parhaiten huolehtia keskitetyssä mallissa.

Tietoliikennetiedustelun teknisen suorittamisen olisi oltava viranomaistoimintaa. Toiminnassa on tarpeen käsitellä sellaista salassa pidettävää tietoa, jonka julkitulo vaarantaisi vakavalla tavalla kansallisen turvallisuuden.

Tietoliikennetiedusteluviranomaiseksi olisi tarkoituksenmukaisinta nimetä sellainen viranomainen, jolla on jo valmiiksi toiminnan edellyttämä tekninen osaaminen ja kansainväliset tiedusteluyhteistyösuhteet. Tietoverkkouhkien torjuntaan osallistuvalla Kyberturvallisuuskeskuksella olisi toiminnan edellyttämää teknistä osaamista. Sillä ei kuitenkaan ole tiedustelutiedon hankintaan liittyviä tehtäviä eikä siten myöskään tiedustelutoiminnan edellyttämiä yhteistyösuhteita. Keskusrikospoliisilla on kansainvälisiä yhteistyösuhteita. Se on kuitenkin toimialaansa kuuluvien rikosten selvittämisestä vastaava viranomainen ja se huolehtii poliisi- ja pakkokeinolakiin liittyvien telepakkokeinojen teknisestä toteuttamisesta rikosprosessia varten. Suojelupoliisilla on tiedustelutiedon hankintaan liittyvää kansainvälistä yhteistyötä. Puolustusvoimien tiedustelulaitoksella on sekä toiminnan edellyttämää teknistä osaamista että tiedustelutoiminnan edellyttämiä kansainvälisiä yhteistyösuhteita.

Tehtäviä tietoliikennetiedusteluviranomaiselle antaisivat toimeksiantajaviranomaiset. Toimeksiantajaviranomaisina tulisivat kyseeseen tiedustelun kohteena olevien uhkien torjunnasta vastaavat viranomaiset. Tällaisia ovat puolustusvoimat, Suojelupoliisi ja Keskusrikospoliisi.

Jos jatkotyössä päädytään ratkaisuun, jossa tietoliikennetiedustelun tekninen suorittaminen osoitetaan puolustusvoimiin kuuluvalle toiminnolle, tulisi myös sen siviiliviranomaisia avustavista tehtävistä ja siviiliviranomaisten siihen kohdistuvasta toimeksiantovallasta säätää laissa.

Työryhmän käsityksen mukaan myös Suomen ylimmällä valtiojohdolla olisi tarve saada tietoliikennetiedustelulla hankittavaa tietoa. Tämän vuoksi myös ylimmällä valtiojohdolla tulisi olla mahdollisuus antaa toimeksiantoja tietoliikennetiedusteluviranomaiselle. Toimeksiannot tulisi kuitenkin kanavoida tietoliikennetiedustelun tekniselle suorittajalle niiden viranomaisten kautta, jotka vastaavat uhkien torjunnasta.

6.1.6 Oikeusturvan kannalta huomioon otettavia seikkoja

Tietoliikennetiedustelua mahdollisesti järjestettäessä tulisi ottaa huomioon ohjaavina periaatteina perus- ja ihmisoikeuksien kunnioittaminen, suhteellisuusperiaate, vähimmän haitan periaate ja tarkoitussidonnaisuuden periaate.

Lupamenettely

EIT on pitänyt tärkeänä, että tiedonhankintaviranomaisella ei ole rajoittamatonta harkintavaltaa tiedonhankinnan kohdentamisessa. Yksi tapa rajoittaa viranomaisen harkintavaltaa on säätää siitä, että jokaisen tiedustelutehtävän suorittamista varten on haettava lupa ulkopuoliselta taholta.

EIT:n mukaan lupaharkinnan alan tulisi käydä ilmi laista. Olennaista tässä suhteessa on se, että lupahakemuksessa ja luvassa riittävällä tarkkuudella kyetään osoittamaan, mihin henkilöryhmiin tiedustelu kohdistuu. Lupaharkinnan, joka perustuu joko seulonnassa käytettävien hakuehtojen taikka kansallista turvallisuutta vaarantavan toiminnan tai henkilöiden mahdollisen täsmällisen kuvauksen hyväksymiseen, voidaan katsoa täyttävän edellä mainitut vaatimukset.

EIT on edellyttänyt, että luvan voimassaoloajasta säädetään laissa. EIT on ratkaisussaan *Weber & Saravia v. Saksa* katsonut kolmen kuukauden määräajan olevan suhteellisuusperiaatteen mukainen.

Kuten kansainvälisestä vertailusta käy ilmi, verrokkivaltioittain vaihtelee, mikä taho luvan myöntää. Luvan voi myöntää erityinen sitä varten perustettu tuomioistuin tai poliittisesti vastuussa oleva taho. Suomen oikeusjärjestelmän mukaista olisi, että lupaharkinta olisi luonteeltaan oikeudellista. Lupamenettelyn järjestämisessä tulisi ottaa huomioon salassapitoseikat, asioiden vaatima erityisosaamisen tarve sekä yksilön oikeusturvan varmistaminen. Esimerkiksi Ruotsissa yksityisen henkilön etua lupamenettelyssä valvoo julkinen asiamies. Valitusmahdollisuuksia lupamenettelyssä olisi arvioitava. Samoin tulisi arvioida kevennetyn lupamenettelyn mahdollisuutta kiiretilanteissa.

Tiedon käsittelystä

EIT on katsonut[56], että lain tasolla on riittävän täsmällisesti säädettävä tietoliikennetiedustelussa noudatettavasta menettelystä. Menettelytapasäännösten tulisi koskea ainakin tietojen tarkastamista, hyödyntämistä, säilyttämistä, luovuttamista ja tuhoamista.

Tietojen tarkastamisella tarkoitetaan automaattisten hakuehtojen perusteella suodatettujen tietojen manuaalista käsittelyä. Suuntaviivat sille, missä tilanteissa suodatetut tiedot voivat tulla manuaalisen käsittelyn kohteeksi on käsitelty edellä jaksossa 6.1.4. Samoin tietojen hyödyntämistä uhkien torjunnassa ja ylimmän valtionjohdon informoinnissa on käsitelty jaksossa 6.1.3.

Tietoliikennetiedustelussa tiedustelun tuloksena syntyvä tieto olisi osittain henkilötietoa. Henkilötietojen käsittelystä toimeksiantajaviranomaisessa sekä tietoliikennetiedusteluviranomaisessa olisi oltava perustuslain mukaisesti laintasoiset säännökset. Perustuslain 10 §:n 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla.

Tietojen luovuttamisessa olisi perustilanteessa kyse tietoliikennetiedusteluviranomaisen hankkimien tietojen luovuttamisesta toimeksiantajaviranomaiselle. Tämä lisäksi tulisi harkita,

56 Liberty and others v. Yhdistynyt kuningaskunta sekä Weber & Saravia v. Saksa

millä edellytyksillä tietoja voitaisiin luovuttaa ulkopuolisille tahoille. Tällaisia olisivat esimerkiksi yritykset, jotka ovat joutuneet tietoliikennetiedustelussa havaitun vakavan tietoverkkohyökkäyksen kohteeksi. Harkinnassa on otettava huomioon lainsäädännöstä seuraavat henkilötietojen käsittelyn rajoitukset.

Tiedustelutiedon luovuttamisen edellytyksistä kansainvälisille yhteistyötahoille tulisi olla säännökset laissa. Lähtökohtana tulisi olla se, että tietojen luovutuksella edistetään kansallista turvallisuutta eikä sillä vaarannettaisi Suomen etuja, mukaan lukien kansantaloudelliset edut.

Tiedustelussa voidaan saada myös tietoa, joka ei liity tiedustelua koskevaan toimeksiantoon. EIT on eri ratkaisuissaan käsitellyt kysymystä niin sanotun ylimääräisen tiedon käytöstä. Ratkaisukäytännöstä voidaan tehdä sellainen johtopäätös, että tällaisen tiedon käytöstä tarvitaan riittävän kattavaa ja täsmällistä sääntelyä. Vaikka ratkaisut koskevatkin rikostorjuntaa, voitaneen niistä päätellä myös, miten tällaisen tiedon käsittely tulisi tiedustelutoiminnassa järjestää. Ylimääräisen tiedon käytön tulisi olla mahdollista vähintäänkin silloin, kun tieto koskee sellaista uhkaa, jota varten tietoliikennetiedustelua olisi saatu käyttää. Tiedon luovuttamista esitutkintaviranomaiselle tutkinnan suuntaamiseksi on erikseen käsitelty mietinnön jaksossa 6.1.3.

Kysymystä tiedon hävittämisestä on tarkasteltava erikseen toimeksiannon mukaisen tiedon, kansallisen turvallisuuden kannalta merkityksellisen ylimääräisen tiedon sekä kansalliseen turvallisuuteen liittymättömän ylimääräisen tiedon osalta. Toimeksiannon mukaisen tiedon osalta olisi määriteltävä säilytysajat sekä niiden määräytyminen ja säilyttämisvelvollisuuden jakautuminen tietoliikennetiedustelunviranomaisen ja toimeksiantajaviranomaisen välillä. Kansallisen turvallisuuden kannalta merkityksellisen ylimääräinen tiedon säilyttämisen ja hävittämisen tulisi määräytyä samoin perustein.

Kansalliseen turvallisuuteen liittymätön ylimääräinen tieto tulee hävittää välittömästi, kun se on havaittu tällaiseksi.

Tietoliikennetiedustelulla ei olisi tarkoitus seurata Suomessa oleskelevien osapuolten välistä tietoliikennettä. Myöskään sellaista Suomesta tapahtuvaa ulkomailla olevaan pilvipalveluun tallentamista, johon ei sisälly viestintää, ei olisi tarkoitus seurata lukuun ottamatta haittaohjelmien aiheuttamaa liikennettä. Jatkotyössä tulisi huolehtia riittävistä säännöksistä sen varmistamiseksi, että tällainen tieto hävitettäisiin välittömästi, kun se havaittaisiin.

Oikeussuojakeinot

Jatkotyössä olisi harkittava, millaisia oikeussuojakeinoja tietoliikennetiedusteluun tulisi liittää. Tällaisia voisivat olla kantelu, välillinen tarkastusoikeus henkilön pyynnöstä henkilötietojen käsittelyn lainmukaisuudesta ja julkisen asiamiehen osallistuminen lupahakemuksen käsittelyyn. Olisi myös harkittava, tulisiko lupapäätöksestä olla valitusmahdollisuus ja miten tämä siinä tapauksessa voitaisiin toteuttaa.

Valvonta

EIT:n ratkaisukäytännön mukaan viranomaisten salaisten tarkkailutoimivaltuuksien valvonta pitää järjestää tehokkaasti. Valvontaa ei voi jättää pelkästään viranomaisten itse suorittaman sisäisen valvonnan varaan. Riippumattomankaan elimen suorittamaa laillisuusvalvontaa ei voida pitää yksinään riittävänä oikeusturvan takeena, jos sen puitteissa ei tehdä sitovia valituskelpoisia päätöksiä. EIT on antanut merkitystä sekä ulkopuoliselle tuomioistuinvalvonnalle että parlamentaariselle valvonnalle.

Perustuslain mukaan valtioneuvoston oikeuskanslerin ja eduskunnan oikeusasiamiehen valta valvoa viranomaistoiminnan lainmukaisuutta on yleinen. Tietosuojavaltuutettu valvoo henkilötietojen käsittelyn lainmukaisuutta. Tietoliikennetiedustelun valvonta saattaa edellyttää sellaista erikoistumista, että myös ulkoisen erityisvalvontaelimen perustamista tulisi harkita. Lisäksi tulisi huolehtia tietoliikennetiedusteluviranomaisen ja toimeksiantajaviranomaisten sisäisestä laillisuusvalvonnasta sekä valvonnasta, jota ohjaavat ministeriöt suorittavat.

Tietoliikennetiedustelua tulisi valvoa myös parlamentaarisesti. EIT on todennut, että kansanedustuslaitoksen osallistumisella salaisten tarkkailutoimivaltuuksien valvontaan on demokratian suojelemisen kannalta merkitystä.

6.1.7 Tietoliikennetiedustelun vaikutusarviointia

Tietoliikennetiedustelun hyötyjen ja haittojen punnintaa

Tietoliikennetiedustelun hyväksyttävyyttä harkittaessa on arvioitava sitä, onko toiminnasta kansalliselle turvallisuudelle aiheutuva hyöty suurempi kuin toiminnasta mahdollisesti aiheutuva haitta yksityisyyden suojalle sekä kansantaloudelle ja yrityksille.

Tietoliikennetiedustelun avulla tunnistettavat uhat ovat kansainvälisiä, vakavia ja kohdistuvat valtion keskeisiin turvallisuusintresseihin. Tietoliikennetiedustelun avulla tuotettaisiin kansallisen turvallisuuden kannalta merkityksellistä tietoa ulkomaisista toimijoista ja olosuhteista ylimmän valtionjohdon päätöksenteon tueksi.

Mietinnön sisältämästä kansainvälisestä vertailusta sekä avoimista lähteistä[57] käy ilmi, että tietoliikennetiedustelu on käytössä lukuisissa länsimaissa. On ilmeistä, että näissä valtioissa sitä pidetään tehokkaana tiedonhankintakeinona. Myös työryhmän luottamuksellisesti kuulemat ulkomaalaiset asiantuntijat ovat korostaneet, että tietoliikennetiedustelu on keino saada kansalliseen turvallisuuteen kohdistuvien uhkien torjumiseksi välttämätöntä tietoa ja hankkia strategista tietoa valtion ylimmän päätöksenteon pohjaksi. Kuulemisissa tuotiin esiin, että nykyaikainen ulko- ja turvallisuuspoliittinen päätöksenteko voi perustua vain ajanmukaiseen tiedustelutietoon, johon tietoliikennetiedustelu tuo olennaisen osan.

Tietoliikennetiedustelu myös täydentäisi merkittävällä tavalla Suomen suojautumista vakavimpia tietoverkkouhkia vastaan. Nykyiset järjestelmät eivät havaitse valtiollisia vakoilu- ja muita haittaohjelmia, joiden kansallista turvallisuutta vahingoittava vaikutus on erityisen suuri. Tietoliikennetiedustelusta olisi hyötyä myös elinkeinoelämän suojautumisessa kaikkein vakavimpia tietoverkkouhkia vastaan.

Toisaalta on selvää, että järjestelmä rajoittaisi perusoikeutena turvattua luottamuksellisen viestin suojaa. Mietinnön jaksossa 6.1.4 on käsitelty sitä, millä tavoin tietoliikennetiedustelu voitaisiin järjestää, jotta se mahdollisimman vähäisissä määrin rajoittaisi yksityisyyden suojaa ja olisi kansainvälisten ihmisoikeussopimusten näkökulmasta hyväksyttävä. Luottamuksellisen viestin perustuslainsuojan kannalta tietoliikennetiedustelun toteuttaminen näyttäisi tästä huolimatta olevan ongelmallista.

Tietoliikennetiedustelu rinnastuisi toiminnallisesti niihin toimintaoikeuksiin, joita tietoyhteiskunnan toimijat voivat jo nykyisin käyttää tietoturvasta huolehtimiseksi. Molemmissa on kyse hakuehtoihin perustuvasta viestinnän automaattisesta suodattamisesta. Viestin manuaaliseen käsittelyyn voidaan siirtyä siinä tapauksessa, että on ilmeistä, että viestin sisällön ja

57 Ks. esimerkiksi Euroopan parlamentin tutkimus ”National programmes for mass surveillance of personal data in EU member states and their compatibility with EU law” (http://www.europarl.europa.eu/studies).

käytetyn hakuehdon välillä on vastaavuus. Tietoliikennetiedusteluun tulisi liittää riippumaton lupamenettely ja valvonta.

Kuulemisissa on tuotu esille, että ulkomaisen ja kotimaisen tietoliikenteen erottaminen toisistaan ei teknisistä syistä ole kaikissa tilanteissa mahdollista. Näin ollen luottamuksellisen viestin suojan rajoitus voisi periaatteessa kohdistua myös kotimaiseen tietoliikenteeseen. Luottamuksellisen viestin suojasta voitaisiin näissä tilanteissa huolehtia esimerkiksi kotimaisen tietoliikenteen käsittelykiellon ja tietojen välittömän poistamisvelvoitteen avulla.

Luottamuksellisen viestin suojan näkökulmasta on otettava huomioon se, että suhtautuminen tunnistamistietoihin ja niiden paljastavuuteen saattaa olla muuttumassa. Mietinnön luvuissa 6.1.2.3 ja 6.1.2.4 on tarkasteltu EUT:n niin sanottua Data Retention -tuomiota ja perustuslakivaliokunnan huomioita siihen. On varmistettava, että tietoliikennetiedustelussa ei tallenneta tunnistamistietoja laajamittaisesti, erittelemättömästi, pitkäaikaisesti ja rajoittamattomasti. Tietoliikennetiedustelussa tulisi voida tallentaa sellaiset rajat ylittävään tietoliikenteeseen liittyvät tiedot, jotka vastaavat käytettyjä hakuehtoja ja joilla siten voidaan arvioida olevan merkitystä kansalliseen turvallisuuteen kohdistuvien uhkien torjunnassa. Tallennettavat tiedot voisivat enimmilläänkin muodostaa vain vähäisen murto-osan rajat ylittävän viestinnän kokonaismäärästä.

Kansalaisiin kohdistuvien vaikutusten lisäksi on arvioitava tietoliikennetiedustelun vaikutuksia yrityksiin ja elinkeinoelämään kokonaisuutena.

Kuulemisissa on tuotu esille, että tietoliikennetiedustelulla voi olla kielteisiä vaikutuksia Suomen kansainväliseen kilpailukykyyn sekä Suomen houkuttelevuuteen investointikohteena. Suomen houkuttelevuuden investointikohteena on näissä lausunnoissa katsottu perustuvan puhtaisiin tietoverkkoihin ja Suomen maineeseen korkean tietosuojan maana.

Arvion puhtaista tietoverkoista kyseenalaistaa Kyberturvallisuuskeskuksen raportti[58], jonka mukaan kyberhyökkäyksiä järjestelmällisesti seuraavissa länsimaissa havaitaan vuosittain kymmeniä kybervakoilutapauksia, joissa teknisenä apukeinona on käytetty kohdistettua haittaohjelmaa. Raportin mukaan uhka kohdistuu myös Suomeen. Näistä maista poiketen Suomessa ei tällä hetkellä ole järjestelmää, jolla erityisen vakavia kohdennettuja haittaohjelmahyökkäyksiä voitaisiin seurata. Näin ollen voidaan arvioida, että käsitys erityisen puhtaista tietoverkoista perustuu ainakin vakavimpien kybertekojen osalta puutteelliseen kansalliseen havaitsemiskykyyn. Suomen tietoliikennetiedustelukyvyn kehittämisen voidaan arvioida nostavan kynnystä kohdistaa maahamme kybervakoilua.

Väitettä tietoliikennetiedustelun Suomen korkeaa tietosuojaa heikentävästä vaikutuksesta tulisi arvioida niitä suuntaviivoja vastaan, jotka tälle toiminnalle on edellä kuvattu. Tietoliikennetiedustelu kohdistuisi Suomen rajat ylittävään tietoliikenteeseen. Valtaosa niistä maista, joihin Suomen nykyiset ja suunnitellut tietoliikenneyhteydet menevät, voi seurata jo nykyisin oman lainsäädäntönsä perusteella alueensa läpi kulkevaa tietoliikennettä. Tämä merkitsee sitä, että Suomen kansainvälisten verkkoyhteyksien kautta kulkeva tietoliikenne voi jo nyt olla valvonnan ja tiedustelun kohteena muiden kuin Suomen omien viranomaisten taholta.

Työryhmä on pyrkinyt selvittämään tietoliikennetiedustelua koskevan lainsäädännön mahdollisia kielteisiä vaikutuksia investointeihin. Vaikutuksia Suomen osalta on vaikea arvioida. Työryhmän tietoon ei ole tullut tutkimuksia aiheesta. Esimerkkinä maasta, joka viime vuosien aikana on säätänyt yksityiskohtaisesti ja julkisesti tietoliikennetiedustelusta on Ruotsi.

58 Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Viestintäviraston Kyberturvallisuuskeskuksen raportti. Syksy 2014

Ruotsin tietoliikennetiedustelulain (niin sanottu FRA-laki) mahdollisten investointivaikutusten selvittämiseksi puolustusministeriö teetti selvityksen Gearshift Group Oy:llä. Selvityksen kohteena olivat Ruotsiin ja Suomeen kohdistuvat ICT-alan investoinnit vuosina 2008–2013. Selvityksessä hyödynnettiin varsinaisten tutkimuslähteiden lisäksi tietoa markkinatutkimuslaitosten raporteista sekä mediaraporttien kautta löydettävistä asiantuntija-arvioista. Kokonaisuudessaan selvitys on mietinnön liitteenä 1. Selvityksen tulokset esitellään lyhyesti alla:

Vaikutukset ulkomaisiin investointeihin ja niiden edellytyksiin. Selvityksessä ei havaittu sellaista poikkeamaa ulkomaisten investointien yleisessä kehityksessä, joka voitaisiin selittää FRA-lain vaikutuksella. Selvityksen mukaan lain voimaantulolla ei ole selkeää merkitystä Ruotsiin suuntautuneiden ulkomaalaisten investointien kehitykselle verrattuna Suomeen ja Tanskaan.

Vaikutukset tutkimus- ja kehitystoimintaan. Ruotsin tutkimus ja kehitysmenot suhteessa BKT:hen laskivat hieman vuonna 2009 ja siitä eteenpäin, mutta kehitysmenojen tason laskun on vaikea nähdä johtuvan FRA-laista, koska ajanjaksoon osuu globaali taloudellinen taantuma. Rahoituslähdekehitystä toisaalta tarkasteltaessa voidaan havaita, että ulkomaiset tahot ovat jopa seleästi lisänneet panostuksiaan suhteessa Ruotsin sisältä tulevaan sekä yksityisen- että julkisen sektorin panostuksiin. Tämä antaa vahvoja viitteitä, ettei FRA-lailla ole ollut merkitystä ulkomaisten tutkimus- ja kehityspanostusten kohdentamisessa.

Vaikutukset kansainväliseen kilpailukykyyn. World Economic Forumin vertailuissa Ruotsi sijoittuu kärkikymmenikköön sekä kansainvälistä kilpailukykyä että innovaatioita arvioitaessa. Erityisesti ICT-investointien näkökulmasta eri maiden kilpailukykyä voidaan arvioida datakeskustoiminnan edellytysten kautta. Ruotsi on arvioitu vuoden 2013 *Data Center Risk Index* -vertailussa kolmanneksi parhaaksi datakeskusten sijoitusmaaksi kun taas Suomi sijoittuu samassa vertailussa sijalle yhdeksän. FRA-lailla ei arvioida olleen kielteisiä vaikutuksia datakeskusten sijoittumisen kannalta. Ruotsin kilpailukyky näkyy merkittävinä uusina datakeskushankkeina, muun muassa Facebook 2011 ja kapasiteetin laajennus 2014, KnC Miner 2014, Hydro66 2014 sekä Bahnhofin suuri laajennusprojekti Tukholmassa. Selvityksen mukaan niin sanotun Snowden-tapauksen jälkeisissä olosuhteissa Ruotsin selkeä tiedustelulainsäädäntö saattaa olla jopa kansainvälinen kilpailuetu. Suurten pitkäaikaisten investointien kohdalla riskien minimointi ja toimintaympäristön kehityksen ennakoitavuus ovat merkittäviä eri maiden kilpailukykyyn vaikuttavia tekijöitä.

Vaikutukset uuden yritystoiminnan syntyyn. Ruotsi ottaa selvän kärkisijan vertailtaessa uusien yritysten perustamisen kehittymistä Ruotsissa, Suomessa ja Tanskassa vuosina 2005 – 2012. Selvitys arvioi FRA-lain merkityksen yritysten yleisessä toimintaympäristössä hyvin vähäiseksi. Sen ei arvioida vaikuttaneen yritystoiminnan kehitykseen tai uusien yritysten syntyyn.

Selvityksen yhteenvedossa todetaan, ettei FRA-lailla voimaantulolla ole selkeää yhteyttä ICT-sektorin ulkomaisiin investointeihin. FRA-lailla selittyviä eroavaisuuksia vastaaviin investointeihin Suomessa ei selvityksessä todettu. Selvityksen arvion mukaan FRA-lain tapainen täsmällinen sääntely luo ennustettavamman toimintaympäristön kaikille ICT-sektorin toimijoille.

Edellä mainitun selvityksen tuloksia tukevat työryhmän kuulemisissa saamat tiedot. Näiden mukaan FRA-laki ei olisi vaikuttanut Ruotsin kilpailukykyyn kielteisesti eikä vähentänyt maahan suuntautuneiden investointien määrää.

Datakeskusinvestointien osalta voidaan vielä erikseen todeta, että tutkimusyhtiö Gartnerin syyskuussa 2014 julkistaman selvityksen[59] mukaan Ruotsi ja Norja koetaan houkuttelevina datakeskusten sijoituspaikkoina. Ruotsin ja Norjan tiedustelulainsäädännöt eivät nousseet tutkimuksessa esille.

Selkeä lainsäädäntö luo yritysten toiminnan suunnittelun ja investointipäätösten kannalta tärkeää ennakoitavuutta. Täsmällinen sääntely voisi olla Suomelle kansainvälinen kilpailuetu.

Elinkeinoelämä on ollut huolissaan siitä, että yksittäisten suomalaisten yritysten kilpailukykyä kansainvälisillä markkinoilla heikennettäisiin velvoittamalla niitä tietoliikennetiedustelun yhteydessä luovuttamaan salausavaimia tai asentamaan takaportteja ohjelmistoihin tai laitteistoihin. Työryhmä ei esitä elinkeinonharjoittajille tällaisia velvoitteita.

Toiminnan järjestäminen edellyttäisi, että teleyrityksille tai rajat ylittävien tietoliikennekaapeleiden omistajille asetetaan velvoite osoittaa liityntäpisteet tietoliikennetiedustelun toteuttamisesta vastaavalle viranomaiselle.

Työryhmän järjestämissä sidosryhmäkuulemisissa kiinnitettiin huomiota siihen, että tietotekninen kehitys vähentäisi tietoliikennetiedustelun tehokkuutta tulevaisuudessa. Näkemysten mukaan tähän vaikuttaisivat keskeisesti tietoliikenteen salaaminen ja tietoliikennemäärien lisääntyminen.

Kuulemisissa tuotiin esille, että salaustekniikoiden kehittymisen johdosta salauksen avaaminen ei ole tulevaisuudessa mahdollista ilman salausavaimia. Tämä vaikuttaa siihen, voidaanko tietoliikennetiedustelulla saada sellaista reaaliaikaista tietoa, jota tiedustelutoiminnassa tarvittaisiin. Tietoliikennetiedustelulla voidaan kuitenkin salauksesta huolimatta saada kansallisen turvallisuuden kannalta merkittävää tietoa esimerkiksi tunnistamistietojen perusteella. Tietoliikennetiedustelua käytettäisiin myös tietoverkkohyökkäysten havaitsemiseen, johon mahdollisella salaamisella ei ole vaikutusta. Työryhmän kuulemien teknisten asiantuntijoiden mukaan järjestelmän riittävä tehokkuus voidaan varmistaa vaatimatta yrityksiltä salausavaimia tai takaporttien asentamista.

Kuulemisissa tietoliikennetiedustelun tehokkuus kyseenalaistettiin myös sen perusteella, että tietoliikennemäärät kasvavat tulevaisuudessa. Tietoliikennemäärien kasvun ei kuitenkaan voida katsoa vähentävän tietoliikennetiedustelun tarpeellisuutta, vaan pikemminkin lisäävän sitä. Uhkien siirtymistä tietoverkkoihin on käsitelty mietinnön jaksossa 2. Tietoliikennemäärien kasvuun on voitava vastata toiminnan riittävällä resursoinnilla ja huolehtimalla siitä, että tiedusteluprosessi on riittävän valikoiva.

Yhteenveto sidosryhmien ja asiantuntijoiden kannanotoista on mietinnön liitteenä 2.

59 Gartnerin selvitys ”Save up to 50% on European Colocation by Choosing the Right Location”, julkaistu 16.9.2014.

Taloudelliset vaikutukset ja henkilöstövaikutukset

Taloudellisten vaikutusten suuruuteen vaikuttaa se, valitaanko tietoliikennetiedustelun toteuttamiseen keskitetty vai hajautettu malli. Jos tietoliikennetiedustelun toteuttamisessa päädyttäisiin mietinnössä esitettyyn keskitettyyn ratkaisuun ja tekniseksi suorittajaksi nimettäisiin puolustusvoimiin kuuluva yksikkö, kohdistuisivat resurssivaikutukset ensisijaisesti puolustusvoimiin. Kustannusten jakoperusteista toimintaan osallistuvien tahojen kesken olisi jatkotyöskentelyssä sovittava tarkemmin.

Puolustuksen pitkän aikavälin haasteita selvittänyt parlamentaarinen selvitysryhmä toteaa raportissaan (Eduskunnan kanslian julkaisu 3/2014), ettei nykyinen rahoituskehys mahdollista riittäviä voimavaroja kyberturvallisuuden kehittämiseen sen paremmin puolustushallinnossa kuin muillakaan hallinnonaloilla.

Tietoliikennetiedustelun toteuttaminen edellyttäisi lisäresursseja toiminnan järjestämistavasta ja laajuudesta riippuen. Kyse olisi ennen kaikkea järjestelmäinvestoinneista ja henkilöstövoimavaroista.

Myös tietoliikennetiedustelun toimeksiantajille aiheutuisi kustannuksia, esimerkiksi analyysi- ja käännöspalveluista.

Mahdollisille lupaviranomaisille ja valvontaviranomaisille aiheutuu kustannuksia, mutta niitä on vielä tässä vaiheessa vaikeaa arvioida.

6.2 Ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu

6.2.1 Yleistä

Suomen kansalliseen turvallisuuteen kohdistuvat vakavimmat uhat ovat lähes poikkeuksetta kansainvälistä alkuperää tai niillä on kytköksiä ulkomaille. Tämän vuoksi kaikkea suomalaisen yhteiskunnan turvallisuuteen vaikuttavaa tietoa ei ole saatavissa Suomen alueelta. Jos yhteiskuntaa halutaan menestyksellisesti turvata, suomalaisten turvallisuusviranomaisten on voitava hankkia tietoa myös ulkomaisilta toimijoilta.

Ulkomaan tiedustelulla tarkoitetaan kansallisen turvallisuuden kannalta olennaisen tiedon hankkimista ulkomaisista olosuhteista ja kohteista. Ulkomaan tiedustelun tarkoituksena on tuottaa ylimmän valtionjohdon turvallisuuspoliittisen päätöksenteon sekä vakavien ulkoisten turvallisuusuhkien torjunnan kannalta välttämätöntä tietoa.

Ulkomaan tiedustelun luonteesta johtuen toiminnan yleismaailmallisena lähtökohtana on, että tarvittavat tiedot pyritään hankkimaan kevyimmällä mahdollisella keinolla. Käytännössä tiedustelu perustuu usein yhteystoimintaa läheisesti muistuttaviin toimintamalleihin. Kyse on kahden valtion viranomaisten välisestä vapaaehtoisuuteen perustuvasta tietojen ja näkökantojen vaihdosta, joka hyödyttää molempia osapuolia. Tiedonvaihto voi koskea esimerkiksi yhteisen mielenkiinnon kohteena olevia ilmiötä, yksittäisiä tapahtumia, havaintoja tai poliittisia mielialoja, joista tietoja antava osapuoli tarjoaa oman tulkintansa pyrkien vaikuttamaan vastaanottajaosapuolen näkemyksiin. Tällaisen molemminpuolisen tiedonvaihdon ohella ulkomaan tiedustelutoiminta voi perustua tiedustelevan valtion yksipuoliseen toimintaan. Perustilanteessa toiminta pitää sisällään sen, että tiedustelevan valtion ulkomaille lähettämä henkilöstö virka-asemaansa perustuen tekee yleisiä havaintoja asemavaltion oloista sekä käy

keskusteluja asemavaltion edustajien tai kansalaisten kanssa. Vaikka kyse ei tällöin ole asemavaltion kanssa nimenomaisesti sovitusta tietojenvaihdosta, tapahtuu toiminta monesti asemavaltion hiljaisen hyväksynnän turvin. Kaikki valtiot joutuvat tosiasiassa tiettyyn rajaan saakka sietämään maaperällään tapahtuvaa tiedustelua.

Tietyissä poikkeuksellisiksi luonnehdittavissa tilanteissa edellä kuvattu yhteistyötä korostava tai hiljaiseen hyväksyntään perustuva tiedustelu ei ole riittävää. Suomen kansallisen turvallisuuden kannalta kriittisen tärkeitä tietoja olisi tällaisissa tapauksissa voitava hankkia salaisten tiedustelumenetelmien avulla. Salaisten menetelmien avulla tapahtuva ulkomaan tiedustelu voidaan jakaa ulkomaan henkilötiedusteluun ja ulkomaan tietojärjestelmätiedusteluun.

Ulkomaan henkilötiedustelulla tarkoitetaan henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin perustuvaa tiedonhankintaa. Ulkomaan henkilötiedustelua voidaan harjoittaa myös siten, että viestintä tapahtuu tietoverkon viestintäpalveluiden välityksellä Suomesta.

Henkilötiedustelu kykenee tuottamaan sellaista yksityiskohtaista ja syvää, korkeimman suojaustason tietoa, jota muilla tiedustelulajeilla on vaikea tai mahdotonta tuottaa. Henkilötiedustelun avulla voidaan luoda edellytyksiä myös muiden tiedustelulajien tehokkaalle hyödyntämiselle.

Ulkomaan tietojärjestelmätiedustelussa on kyse ulkomaisessa tietojärjestelmässä käsiteltävien tietojen hankinnasta tietoteknisin menetelmin. Ulkomaan tietojärjestelmätiedustelun ja tietoliikennetiedustelun välinen keskeinen ero on toiminnan alueellinen ulottuvuus. Ulkomaan tietojärjestelmätiedustelu tapahtuu tiedustelun kohdevaltion ja tietyissä tapauksissa kolmannen valtion alueella pääasiassa Suomesta, kun taas tietoliikennetiedustelu tapahtuu Suomen alueella.

Useat Euroopan valtiot ovat säätäneet ulkomaan tiedustelutoiminnastaan ja siinä käytettävistä toimivaltuuksista. Maittain vaihtelee, millä tarkkuudella yksittäisistä toimivaltuuksista on katsottu aiheelliseksi säätää. Yleispiirteistä sääntelymallia edustaa muun muassa Ruotsi. Ruotsin tiedustelutoiminnan toimivaltuussääntely rajoittuu säännökseen, jonka mukaan tiedustelutoimintaa harjoitetaan hankkimalla, työstämällä ja analysoimalla tietoa ja toiminnassa käytetään teknistä tiedonhankintaa ja henkilötiedonhankintaa. Esimerkkinä yksityiskohtaisemmasta sääntelytarkkuudesta voidaan mainita Alankomaat, jonka tiedustelulaki sisältää seikkaperäiset säännökset jokaisesta tiedustelupalveluiden käytössä olevasta toimivaltuudesta.

Kansainvälisesti erityisesti tietojärjestelmätiedustelun menetelmät ovat voimakkaan kehityksen kohteena. Tiedustelupalvelut keräävät tietojärjestelmätiedustelun keinoin laajasti tietoja esimerkiksi kohdevaltion toimijoista, järjestelmistä sekä sen tietoverkkojen kokoonpanoista ja haavoittuvuuksista. Ulkomaan tietojärjestelmätiedustelun tavoitteena voi olla paitsi tiedon hankkiminen myös tietojärjestelmän toiminnan häiritseminen tai sen vahingoittaminen tietoja muuttamalla tai tuhoamalla. Tällainen toiminta saatetaan kohdevaltiossa tulkita voimankäytöksi tai aseelliseen hyökkäykseen rinnastuvaksi suvereniteetin loukkaukseksi.[60] Se, onko tietojärjestelmän toiminnan häiritseminen tai vahingoittaminen tulkittavissa voimankäytöksi, riippuu sekä kohteesta että tehdyn vahingon asteesta. Pelkän tilapäisen haitan aiheuttaminen (palveluksenestohyökkäykset) ei vielä ole voimankäyttöä. Sen sijaan, jos operaation kohde on merkittävä, sen kesto pitkäaikaista ja intensiteetti korkeaa, voidaan operaatio tulkita voimankäytöksi, joskaan ei välttämättä vielä aseelliseksi hyökkäykseksi.

60 Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press 2013, ns. Tallinnan manuaali on ei-sitova arvostettujen kansainvälisen oikeuden asiantuntijoiden henkilökohtaisessa ominaisuudessaan laatima asiakirja kybersodankäyntiin sovellettavasta kansainvälisestä oikeudesta, jota käytetään epävirallisesta luonteestaan huolimatta melko yleisesti viiteaineistona.

Tässä mietinnössä ehdotettava ulkomaan tietojärjestelmätiedustelu ei olisi luonteeltaan verkkohyökkäyksiin verrattavaa, voimankäytön luonteista toimintaa, vaan kyse olisi tiedustelutiedon hankinnasta osana muuta tiedustelutoimintaa. Tietojärjestelmätiedustelun lähtökohtana olisi kerätä tietoja tietojärjestelmästä mahdollisimman huomaamattomasti eikä tarkoituksena olisi esimerkiksi kohteena olevan tietojärjestelmän toiminnan häiritseminen tai tietojärjestelmän sisältämien tietojen muuttaminen tai tuhoaminen. Vaikka tietoverkko-operaatioita koskevat oikeudelliset tulkinnat ja arviot ovat vasta muotoutumassa eikä kansainvälisessä oikeudessa ole kyetty määrittelemään tietoverkkoympäristössä tapahtuvan hyökkäysteon kynnystä, näyttää siltä, ettei tällaista tiedustelutiedon hankintaan rinnastuvaa tietojärjestelmätiedustelua voida tulkita kansainvälisen oikeuden vastaiseksi voimankäytöksi tai ainakaan hyökkäysteoksi.[61] Tämän näkemyksen puolesta puhuu se, ettei tiettävästi mikään valtio ole ryhtynyt aseellisiin puolustustoimiin siihen tietojärjestelmätiedustelua kohdistanutta valtiota kohtaan. Tietojärjestelmiin kohdistuneita toimia ei ole kansainvälisessä yhteisössä tähän mennessä kiistattomasti ja julkisesti myöskään luonnehdittu aseelliseksi hyökkäykseksi.[62]

6.2.2 Kehittämistarpeita

Suomen keskeisten turvallisuusetujen suojaamiseksi on tarpeen luoda säädösperusta kansallisesta turvallisuudesta vastaavien siviili- ja sotilasviranomaisten ulkomailla tapahtuvalle tiedustelutiedonhankinnalle. Toiminnan tarkoituksena tulisi olla tukea ylimmän valtionjohdon ulko- ja turvallisuuspoliittista päätöksentekoa sekä torjua Suomeen kohdistuvia vakavia ulkoisia turvallisuusuhkia. Näitä ovat erityisesti Suomeen kohdistuvat sotilaalliset uhkat, sellaisiin kansainvälisiin kriisinhallintaoperaatioihin, joihin Suomi osallistuu, kohdistuvat uhat, Suomeen kohdistuva kansainvälinen terrorismi, Suomeen kohdistuva ulkovaltojen tiedustelutoiminta, kansallista turvallisuutta vaarantava kansainvälinen järjestäytynyt rikollisuus, kansallista turvallisuutta vaarantava joukkotuhoaseiden, puolustustarvikkeiden ja kaksikäyttötuotteiden kehittäminen, levittäminen ja maastavienti, muut yhteiskunnan elintärkeisiin toimintoihin kohdistuvat vakavat uhkat, ennen kaikkea verkkouhkat, sellaiset vieraan vallan suunnitelmat, aikeet ja toimet, jotka saattavat vaikuttaa vahingollisesti tai haitallisesti Suomen ulko- ja turvallisuuspolitiikkaan tai joilla saattaa olla merkitystä Suomen ulko- ja turvallisuuspolitiikan kannalta.

Säädösperustaa tarvittaisiin sekä ulkomaan henkilötiedusteluun että ulkomaan tietojärjestelmätiedusteluun.

Kansainvälisen vertailun perusteella jatkotyössä olisi aiheellista harkita, tulisiko ulkomaan henkilötiedustelussa olla mahdollista käyttää henkilölähteitä sekä hankkia tietoja tekemällä suunnitelmallisesti havaintoja henkilöistä, paikoista ja muista kohteista. Samoin olisi harkittava, tulisiko tiedonhankintaa voida suojata siten, että se pidettäisiin salassa tiedon hankkijan tai tiedon luovuttajan turvallisuuden varmistamiseksi, tiedonhankinnan toteuttamisen edellyttämän luottamuksen hankkimiseksi tai tiedonhankintatoiminnan paljastumisen estämiseksi.

Ulkomaan henkilötiedustelu voisi perustua tiedonhankintaa harjoittavan virkamiehen ja ulkopuolisen henkilön väliseen henkilökohtaiseen kanssakäymiseen. Olisi harkittava, voitaisiinko henkilölähdettä paitsi pyytää luovuttamaan hallussaan olevia tietoja myös ohjeistaa

61 Tallinnan manuaali, s. 50 ja 52.

62 Tallinnan manuaali, s. 57

hankkimaan tietoja. Tiedustelua suorittavan virkamiehen henkilöllisyys ja taustaorganisaatio olisi tarpeen mukaan voitava pitää salassa.

Sen lisäksi, että henkilötiedustelua toteutettaisiin ulkomailla, sitä tulisi voida toteuttaa myös tietoverkon viestintäpalveluiden kautta Suomesta. Henkilötiedustelua tulisi voida suorittaa myös osana kriisinhallintaoperaatiota.

Ulkomaan tietojärjestelmätiedustelulla tarkoitettaisiin turvallisuusviranomaisten aktiivista toimintaa tiedon hankkimiseksi verkon välityksellä sellaisista ulkomailla oleskelevista yksittäisistä tai valtiollisista toimijoista, jotka saattavat uhata Suomen kansallista turvallisuutta tai muita yhteiskunnan elintärkeitä etuja. Tietojärjestelmätiedustelu mahdollistaisi Suomen kriittisten tietojärjestelmien suojausrakenteita ja -toimia vastaan suuntautuviin uhkiin varautumisen ja vastaamisen. Viimesijaisesti ulkomaan tietojärjestelmätiedustelun tuottamilla tiedoilla mahdollistetaan tietoverkkosodankäynnin vaikuttamisen suorituskykyjen suuntaaminen vastustajan kohteisiin osana sotilaallista voimankäyttöä kriisitilanteissa.

Tietojärjestelmätiedustelu edellyttää teknisen suojauksen ohittamista sekä toimintaa tietoverkoissa Suomen valtakunnan rajojen ulkopuolella.

Ulkomaan tiedusteluun liittyvien toimien oikeudettomuus olisi poistettava kansallisesti säätämällä. Mahdollisessa tulevassa lainvalmistelussa tulisi tarkastella muutostarpeita esimerkiksi rikos- ja virkamiesoikeudellisessa sääntelyssä. Lisäksi toiminnassa tulisi ottaa huomioon Suomea sitovat kansainväliset ihmisoikeussopimukset ja muut kansainväliset velvoitteet.

6.2.3 Kohdevaltion näkökulma

Kansainvälisen oikeuden yleisen periaatteen mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Jokainen valtio päättää itse, salliiko se ja millä ehdoilla ulkomaisten virkamiesten toimia alueellaan. Edellä on todettu, että useimmat valtiot tosiasiassa tiettyyn rajaan saakka sietävät tai jopa hyväksyvät vieraiden tiedusteluviranomaisten toiminnan maaperällään. Kyse saattaa olla molempia osapuolia hyödyttävästä tiedonvaihdosta tai siitä, ettei ulkovallan avoimesti suorittama, kohdevaltion yleisiä olosuhteita koskeva tiedonkeruu vaaranna kohdevaltion tai minkään muunkaan tahon etuja. Toisissa olosuhteissa kohdevaltio saattaa suhtautua alueellaan tapahtuvaan vieraan valtion viranomaisten toimintaan torjuvasti. Toiminta saattaa tapauskohtaisesti myös täyttää jonkin kohdevaltion rikoslainsäädännössä rangaistavaksi säädetyn teon tunnusmerkistön. Toiminnan rangaistavuuteen saattaa kohdevaltiosta riippuen vaikuttaa esimerkiksi se, kuka tietoa hankkii, mitä tietoa hankitaan ja mitä menetelmää käyttäen tiedonhankinta tapahtuu

Verrokkivaltiot eivät ole lainsäädäntönsä tasolla asettaneet ulkomaan tiedustelun ehdoksi sitä, että kohdevaltio hyväksyy toiminnan tai että sillä ei rikota kohdevaltion lainsäädäntöä. Tiedustelun säädösperustan luomista harkitessaan Suomen olisi luontevaa tarkastella asiaa samasta näkökulmasta. Ulkomaan tiedustelussa olisi kyse hyväksyttävän päämäärän (kansallisen turvallisuuden varmistaminen) saavuttamiseksi välttämättömästä toiminnasta, joka tietyissä tilanteissa saattaa sisältää riskejä. Yksi riskeistä on se, että kyse on kohdevaltion lainsäädännön vastaisesta tai muuten sen kannalta ei-hyväksyttävästä toiminnasta. Ulkomaan tiedustelussa olisi tärkeä huomioida muiden valtioiden suhtautuminen sekä niiden lainsäädäntöjen sisältö, mutta käytännön syistä huomioiminen ei voisi tapahtua toiminnasta säädettäessä vaan vasta siihen ryhdyttäessä. Tällöin kyse on sen harkitsemisesta, onko toiminnasta kansalliselle turvallisuudelle aiheutuva etu selvästi suurempi kuin siihen liittyvät riskit.

6.2.4 Kolmannen valtion näkökulma

Kansainvälisen oikeuden yleisen periaatteen mukaan jokainen suvereeni valtio nauttii alueellista koskemattomuutta ja poliittista riippumattomuutta suhteessa muihin valtioihin. Tämä pätee myös silloin, kun tiedustelu tapahtuu kolmannen valtion aluetta jollakin tavalla hyväksikäyttäen.

Lisäksi kansainvälisen oikeuden yleisen periaatteen mukaan valtio ei saa sallia sen aluetta käytettävän tekoihin, jotka haitallisesti ja laittomasti vaikuttavat toisiin valtioihin. Tekoa arvioitaessa merkitystä ei anneta pelkästään sille, aiheuttaako teko vahinkoa omaisuudelle tai henkilöille vaan riittävää voi olla se, että teko aiheuttaa ylipäänsä negatiivisia vaikutuksia.

Ulkomaan henkilötiedustelussa kolmannen valtion alueella voitaisiin tavata tietoja antavia henkilöitä tai heitä voitaisiin värvätä kolmannesta valtiosta.

Kauttakulkuvaltiota koskevan periaatteen ei voida kuitenkaan katsoa soveltuvan suoraan kansainväliseen tietoliikenteeseen, jossa normaalisti tietoliikenne liikkuu ja reititetään ennalta määrittelemättömästi sitä kautta, missä tietoliikenteen kululle ei ole esteitä.

Tiedonhankintaa voidaan joutua toteuttamaan kolmannen valtion alueella, sen kautta tai sellaisessa tietojärjestelmässä, joka sijaitsee jossakin muussa valtiossa kuin tiedonhankinnan kohteena olevan tiedon omistavat henkilöt. Asetelma koskee yhtälailla henkilötiedustelua kuin tietojärjestelmätiedusteluakin, mutta tiedonhankinnan vaikutukset kolmannen maan suvereniteettiin voidaan nähdä erilaisina. Esimerkiksi terrori-iskua länsimaihin suunnitteleva ryhmä voi kommunikoida viestintäpalvelussa, joka on vuokrattu ryhmän käyttöön kolmannesta maasta, jolla ei ole mitään muuta yhtymäkohtaa ryhmän jäseniin kuin palvelin. Vaikka tällaiseen palveluun kohdistuva tiedonhankinta tapahtuisi teknisesti kolmannen maan alueella olevassa tietoverkossa, kohdistuisivat tiedonhankinnan vaikutukset siihen maahan, jossa toimintaa harjoittavat henkilöt oleskelevat. Suvereniteettivaikutukset kohdistuisivat näin ollen ensisijaisesti toimintaa harjoittavien henkilöiden oleskelu maahan. Palvelimen sijaintimaan selvittäminen voi myös edellyttää toimimista kolmannen maan tai kolmansien maiden kautta.

Kolmannen valtion suvereniteetin loukkaamista tulee pohtia myös tilanteessa, jossa kolmannen valtion alueella olevaa palvelinta käytettäisiin kohdemaan harhauttamiseksi esimerkiksi tiedusteluohjelman viemiseksi kohdetietojärjestelmään. Merkitystä on sillä, sallivatko kolmannen valtion viranomaiset toiminnan.

6.2.5 Tiedustelutoiminta ja kansainvälinen oikeus

Kansainvälisen tuomioistuimen perussäännön 38 artiklan mukaan kansainvälisen oikeuden keskeisimmät lähteet ovat kansainväliset yleis- ja erityissopimukset, kansainvälinen tapaoikeus ja niin sanotut yleiset oikeusperiaatteet.

Rauhan ajan tiedustelutoiminnasta ei ole laadittu kansainvälisiä sopimuksia. Geneven vuoden 1949 yleissopimusten ensimmäisen lisäpöytäkirjan 46 artiklaan sisältyvillä määräyksillä sodan ajan vakoilijoiden nauttimasta suojasta taas ei ole merkitystä tässä käsiteltävän aiheen kannalta.

Vaikka tiedustelutoiminnassa on lähtökohtaisesti kyse kohdevaltion suvereniteetin loukkauksesta, ei oikeuskirjallisuudessa ole yksimielisyyttä siitä, suhtautuuko kansainvälinen oikeus tapaoikeuden ja yleisten oikeusperiaatteiden tasolla tiedustelutoimintaan hyväksyvästi vai tuo-

mitsevasti.[63] Tiedustelutoiminnalla ei voitane katsoa olevan kansainvälisoikeudellisesti yleisesti hyväksyttyä asemaa, koska valtiot toteamalla henkilön *persona non grataksi* tai muulla tavoin ei-hyväksytyksi osoittavat toistuvasti, etteivät ne hyväksy tällaista toimintaa. Toisaalta tiedustelutoimintaa ei voi pitää myöskään kansainvälisoikeudellisesti kielletyksi, koska lähes kaikki valtiot harjoittavat tätä toimintaa. Kyse on maailmanlaajuisesti vakiintuneesta toiminnasta, johon yksittäisten valtioiden asennoituminen määräytyy sen mukaan, ovatko ne kulloisessakin tapauksessa tiedustelevan valtion tai kohdevaltion roolissa.

Vaikka tiedustelutoimintaa ei olekaan säännelty, osoittavat useat kansainväliset esimerkit, että toiminnassa on hyödynnetty kansainvälisen sopimusjärjestelmän mahdollisuuksia. Toiminnassa on käytetty diplomaattisia suhteita koskevalla Wienin yleissopimuksella (SopS 3-5/1970) taattua diplomaattisen edustajan koskemattomuutta ja vapautta kohdevaltion rikosoikeudellisesta tuomiovallasta.

6.2.6 Ulkomaan tiedustelua koskeva päätöksenteko

Kansainvälisestä vertailusta voidaan havaita, että tiedonhankintaa koskeva päätöksenteko vaihtelee maittain. Päätöksenteosta voi vastata esimerkiksi tiedusteluviranomainen itse tai jokin poliittisesti vastuunalainen taho. Jos päätöksenteosta vastaa tiedusteluviranomainen, tapahtuu se valtiojohdon linjausten puitteissa.

Koska ulkomaan tiedusteluun liittyy ulkopoliittisesti sensitiivisiä elementtejä, päätöksenteko voisi Suomessa tapahtua ulko- ja turvallisuuspoliittisen johdon ohjauksessa. Suomessa esimerkiksi ulko- ja turvallisuuspolitiikkaa käsittelevä ministerivaliokunnan ja tasavallan presidentin yhteinen kokous käsittelee valmistelevasti tärkeät ulko- ja turvallisuuspolitiikkaa ja muita Suomen suhteita ulkovaltoihin koskevat asiat, näihin liittyvät tärkeät sisäisen turvallisuuden asiat sekä tärkeät kokonaismaanpuolustusta koskevat asiat. Tiedustelussa käytettävät menetelmät kohdistuvat vieraan valtion suvereniteettiin paitsi kohdemaassa, myös, kun toimitaan kolmannen valtion kanssa yhteistyössä tai kolmannen valtion kautta kohdemaahan. Tämän vuoksi ulkomaan tiedustelun poliittinen ulottuvuus korostuu. Tiedustelun mahdolliset vaikutukset ja riskit vaikuttaisivat päätöksentekomenettelyyn. Ulkomaan tiedustelun päätöksentekomenettelyä jatkotyössä arvioitaessa on tärkeää varmistaa myös päätöksentekomenettelyn toimiminen ja siihen liittyvän tiedon välittyminen kiiretilanteessa.

6.2.7 Valvonta

Sen lisäksi, että ulkomaan tiedustelutoiminnasta säädettäisiin laissa ja sitä tehtäisiin virkavastuulla, tulisi toimintaa valvoa niin oikeudellisesti kuin parlamentaarisestikin.

Oikeudellinen valvonta keskittyisi siihen, että ulkomaan tiedustelutoiminnassa noudatetaan Suomen lakia. Oikeudellista ulkopuolista valvontaa suorittaisivat ainakin niille säädettyjen tehtävien mukaisesti oikeuskansleri ja eduskunnan oikeusasiamies sekä tietosuojavaltuutettu. Tämän lisäksi voitaisiin harkita ulkoisen erityisvalvontaelimen tarvetta. Samalla tulisi huolehtia organisaatioiden sisäisestä laillisuusvalvonnasta sekä valvonnasta, jota ohjaavat ministeriöt suorittavat.

63 Ks. kansainvälistä oikeuskirjallisuutta koskevat katsaukset esim. seuraavissa lähteissä: Baker, Christopher D.: Tolerance of International Espionage: A Functional Approach (American University International Law Review vol 19 (2003) issue 5); Radsan, Afsheen John: The Unresolved Equation of Espionage and International Law (Michigan Journal of International Law vol 28 (2007) issue 597).

Ulkomaan tiedustelun tulisi toiminnan luonteen vuoksi olla parlamentaarisessa valvonnassa. Kansainvälisesti vertailusta voidaan havaita, että joissain maissa parlamentaarista valvontaa suorittaa kansanedustuslaitoksen valiokunta, kun taas toisissa maissa valvonnasta vastaa parlamentin ulkopuolinen toimielin, jossa on niin parlamentaarinen kuin oikeudellinen edustus.

6.2.8 Taloudelliset ja henkilöstövaikutukset

Taloudellisten vaikutusten suuruuteen vaikuttavat toiminnan laajuus ja kohdentaminen. Lähtökohtaisesti toiminta tapahtuisi viranomaisten määrärahakehysten puitteissa. Toimintaa kehitettäisiin asteittain.

7. JOHTOPÄÄTÖKSET

Sekä tietoliikennetiedustelun että ulkomaantiedustelun tarkoituksena olisi hankkia kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa vakavista kansainvälisistä uhista. Toiminnalla tuettaisiin valtion ylimmän johdon päätöksentekoa ja varmistettaisiin sen perustuminen oikeaan, ajantasaiseen ja luotettavaan tietoon. Toiminnalla myös mahdollistettaisiin toimivaltaisten viranomaisten ryhtyminen uhkien torjuntaan. Toiminnasta olisi säädettävä lailla.

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

7.1 Tietoliikennetiedustelu

Suomen tulisi harkita toimivaltuuksien kehittämistä rajat ylittävään tietoliikenteeseen kohdistettavasta tiedustelua varten, jotta mietinnössä kuvattuun ulkoisen turvallisuustoimintaympäristön muutokseen voidaan vastata.

Tietoliikennetiedustelu rajattaisiin koskemaan tiedon hankintaa kansallista turvallisuutta vaarantavista uhista. Uhat ovat luonteeltaan joko sotilaallisia tai siviililuontoisia ja ne voidaan toteuttaa joko reaalimaailmassa tai tietoverkkojen välityksellä.

Yhdenmukaisiin menettelytapoihin ja laillisuusvalvontaan liittyvät seikat puoltaisivat tietoliikennetiedustelun teknisen suorittamisen keskittämistä yhdelle viranomaiselle. Keskittämisen puolesta puhuvat myös taloudelliset syyt. Puolustusvoimien tiedustelulaitoksella on jo tällä hetkellä sekä toiminnan edellyttämät tekniset valmiudet että tarvittavat kansainväliset yhteistyösuhteet. Toimeksiantajina voisivat olla uhkien torjunnasta vastaavat viranomaiset sekä niiden kautta Suomen ulko-, turvallisuus- ja puolustuspoliittisesta päätöksenteosta vastaavat tahot. Tällaisessa mahdollisessa järjestelyssä tulisi puolustusvoimiin kuuluvan yksikön siviiliviranomaisia avustavista tehtävistä ja siviiliviranomaisten siihen kohdistuvasta toimeksiantovallasta säätää laissa.

Työryhmä lähtee siitä, että yritystoimijoille ei ehdotettaisi velvollisuutta luovuttaa salausavaimia tai asentaa ohjelmistoihin ja laitteistoihin takaportteja. Toiminnan järjestäminen kuitenkin edellyttäisi, että teleyrityksille tai rajat ylittävien tietoliikennekaapeleiden omistajille asetetaan velvoite osoittaa liityntäpisteet sekä antaa tämän edellyttämät tiedot tietoliikennetiedustelun toteuttamisesta vastaavalle viranomaiselle.

Perus- ja ihmisoikeudet tulee ottaa asianmukaisesti huomioon tietoliikennetiedustelua koskevan lainsäädännön valmistelua harkittaessa. Erityisesti on otettava huomioon perustuslaissa jokaiselle yksilölle turvattu luottamuksellisen viestin salaisuuden suoja ja siten se, että lailla voidaan perustuslain mukaan säätää välttämättömistä rajoituksista tällaisen viestin salaisuuteen vain yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta ei siten näyttäisi olevan mahdollista säätää perustuslakia muuttamatta, pelkästään vieraan valtion tietoliikenteeseen kohdistuvaa tiedustelua ehkä lukuun ottamatta. Jatkotyössä voitaisiin pohtia, olisiko tehokasta tietoliikennetiedustelua mahdollista toteuttaa ensivaiheessa rajoitetummin esimerkiksi kohdentamalla se tunnistamistietoihin.

Tietoliikennetiedustelun lupamenettely ja toteuttamistapa olisi kuvattava riittävän täsmällisesti. Tietoliikennetiedustelun olisi oltava selkeässä ohjauksessa sekä kattavan oikeudellisen ja parlamentaarisen valvonnan piirissä.

Tietoliikennetiedustelun vaikutuksia arvioitaessa tulee ottaa huomioon myös vaikutukset yhteiskunnan digitalisoitumiseen ja yritysten toimintaedellytyksiin. Tulevassa valmistelussa olisi otettava turvallisuuspoliittisten näkökulmien ohella huomioon myös elinkeinopoliittiset ja digitaalisen ekosysteemin kehitykseen vaikuttavat tekijät. Talouskasvun kannalta on välttämätöntä hyödyntää tieto- ja viestintäteknologian tarjoamat mahdollisuudet toimintatapojen muuttamiseen ja tuottavuuden parantamiseen. Jatkotyössä olisi myös pohdittava kattavasti tietoliikennetiedustelun eri teknisiä toteuttamistapoja ja niiden taloudellisia vaikutuksia.

7.2 Ulkomaan henkilötiedustelu ja ulkomaan tietojärjestelmätiedustelu

Tulisi harkita, että kansallisesta turvallisuudesta vastaavilla sotilas- ja siviiliviranomaisilla olisi mahdollisuus valtion ylimmän johdon päätöksentekoa tukevan ja ulkoisia turvallisuusuhkia koskevan tiedustelutiedon hankintaan. Kyse olisi tarpeellisten tietojen hankkimisesta henkilöiltä ja tietojärjestelmistä ulkomailta.

Suomea sitovat kansainväliset velvoitteet sekä sen valtion lainsäädäntö, josta tietoja on tarkoitus hankkia, tulisi ottaa huomioon harkittaessa tiedustelutoimivaltuuksien käyttöä ja arvioitaessa siihen sisältyviä riskejä.

Toiminnan luonteesta johtuen ulkomaan tiedustelua koskevassa päätöksenteossa olisi erityisesti otettava huomioon ylimmän valtionjohdon linjaukset. Ulkomaan tiedustelu on etenkin ulkopoliittisesti sensitiivistä. Toiminnan ohjaus- ja vastuusuhteet tulisi harkita mahdollisen jatkovalmistelun yhteydessä. Ulkomaan tiedustelua olisi valvottava sekä oikeudellisesti että parlamentaarisesti.

7.3 Ehdotuksia jatkotoimenpiteiksi

Tiedustelua koskevan säädösperustan luomiseksi esitetään, että käynnistettäisiin edellä kuvatuilla perusteilla lainsäädäntöhanke tai useampia lainsäädäntöhankkeita. Valmistelu voitaisiin tarvittaessa toteuttaa myös vaiheittain, mutta tällöin on otettava huomioon perustuslaista nykyisin johtuvat rajoitukset tietoliikennetiedustelun sääntelylle. Tulisi myös harkita esimerkiksi parlamentaarista tai muuta poliittisessa ohjauksessa tapahtuvaa valmistelua.

Koska sisäministeriön hallinnonalan tarpeet liittyvät kansallista turvallisuutta vaarantavien vakavien siviililuontoisten uhkien, kuten terrorismin ja vakoilun, havaitsemiseen ja niiden taustalla olevien toimijoiden tunnistamiseen, voitaisiin harkita, että siviilitiedusteluun liittyvää lainsäädäntöä valmisteltaisiin sisäministeriön johdolla.

Puolustusministeriön hallinnonalan tarpeet puolestaan koskevat puolustusvoimien tehtäviin liittyvän tilannekuvan muodostamista ja ylläpitämistä, ennakkovaroituksen antamista sekä maalittamistukea, jolloin voitaisiin harkita sotilastiedustelua koskevan lainsäädännön valmistelemista puolustusministeriön johdolla.

Koska tietoliikennetiedustelu olisi tarpeen molemmille hallinnonaloille, tulisi harkita, säädettäisiinkö tietoliikennetiedustelusta erillislakina. Tässä valmistelussa tulisi myös ottaa huomioon sidosryhmien tarpeet ja huolehtia, että elinkeinoelämän edustus olisi mukana.

Perustuslain mahdollinen tarkistaminen valmistellaan oikeusministeriön johdolla.

Jos tiedustelulainsäädäntöä valmisteltaisiin eri hallinnonaloilla toimialakohtaisesti, tulisi huolehtia siitä, että valmistelu sovitetaan yhteen.

gearshiftgroup

IT sektoriin kohdistuvien ulkomaisten investointien kehittyminen Ruotsissa ja Suomessa vuosina 2008 - 2013 ja Ruotsin ”FRA-lain” mahdolliset vaikutukset investointeihin

Sisällysluettelo

1 Tarkasteltava aihealue

1.1 Tausta ja tavoitteet

Puolustusministeriö on asettanut työryhmän, jonka tehtävä on Suomen lainsäädännön kehittäminen erityisesti turvallisuusviranomaisten tiedonhankintaa koskevan sääntelyn osalta. Tavoitteena on, että huolehdittaisiin paremmin kansallisesta turvallisuudesta tietoverkoissa esiintyvien uhkien torjumiseksi.

Tässä selvityksessä arvioidaan tätä asiaa IT sektoriin kohdistuvien ulkomaisten investointien kehittymisen näkökulmasta Ruotsissa ja Suomessa vuosina 2008 - 2013. Selvityksen lopputuloksena syntyy yhteenveto kehityksestä sekä arvio ”FRA-lain” mahdollisista vaikutuksista toteutuneeseen investointitoimintaan Ruotsissa.

Signaalitiedustelusta säädetään sitä koskevissa erityislaeissa ja -asetuksessa (Lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet, Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet ja Förordning (2008:923) om signalspaning i försvarsunderrättelseverksamhet). Signaalitiedustelua harjoittaa puolustusvoimien radiolaitos (FRA), joka on puolustusministeriön alainen siviiliorganisaatio. FRA:n tehtävänä on hankkia tiedustelutietoja saamiensa toimeksiantojen mukaisesti ja toimittaa hankkimansa tiedot toimeksiantajien käyttöön.

1.2 Selvityksen rajaukset

Tässä selvityksessä keskitytään IT sektoriin kohdistuviin ulkomaisten investointien kehittymiseen Ruotsissa ja Suomessa vuosina 2008 -2013, sekä arvioidaan Ruotsin ”FRA-lain” mahdollisia vaikutuksia investointeihin seuraavista tarkastelukulmista:

- vaikutukset investointeihin ja niiden edellytyksiin
- vaikutukset T&K toimintaan Ruotsissa
- vaikutukset kansainväliseen kilpailukykyyn Ruotsissa
- vaikutukset uuden yritystoiminnan syntyyn Ruotsissa ja Suomessa
- vaikutukset erilaisille yrityksille tai yritysryhmille Ruotsissa

1.3 Käytetyt menetelmät

Menetelmänä on käytetty kirjallisuustutkimusta ”Internet Surveillance” –lainsäädännön taloudellisista vaikutuksista. Lainsäädännön vaikutusten lisäksi on pyritty löytämään tutkimuksia aiheesta, miten seuranta on vaikuttanut investointeihin. Varsinaisten tutkimuslähteiden lisäksi on kerätty tietoa markkinatutkimuslaitosten raporteista sekä mediaraporttien kautta löydettävistä asiantuntija-arvioista. Kirjallisuustutkimuksen perusteella on arvioitu, mihin asioihin lainsäädäntö ja sen vaikutus aiheuttavat vaikutuksia sekä kuinka suuresta vaikutuksesta on kyse. Kirjallisuustutkimuksen sekä tilastollisen toimiala- yms. tiedon perusteella arvioidaan vaikutuksen suuruutta Ruotsissa sekä verrataan sitä vuosina 2008 - 2013 tapahtuneeseen todelliseen kehitykseen Suomeen verrattuna.

2 Uutisointia ennen lain voimaantuloa Ruotsissa ja Suomessa

2.1 Google Ruotsi

”Google likens Sweden to dictatorship”, Published: 30 May 2007 11:49 GMT+02:00

” Search engine giant Google has slammed Sweden's proposed wiretapping legislation as illiberal and incompatible with Western democracy”. Speaking on a visit to Sweden on Tuesday, the company's global privacy counsel, Peter Fleischer, warned that Google would rule out making any major investments in Sweden should the controversial bill become law.

"We have contacted Swedish authorities to give our view of the proposal and we have made it clear that we will never place any servers inside Sweden's borders if the proposal goes through," Fleischer told Internet World.”

2.2 Aftonbladet Ruotsi

2008-06-19, IT-företag undviker Sverige efter FRA-lag, ”Flera stora företag vill inte satsa här”

Sverige går miste om stora investeringar från multinationella IT-företag. FRA-lagen gör att de inte vill lägga sin verksamhet här, enligt myndigheten Invest in Sweden Agency. ” – Vi har fått tydliga besked från flera stora företag att de inte vill satsa här”, säger Bengt-Åke Ljudén, försäljningschef på Invest in Sweden Agency (ISA), en statlig myndighet som hjälper utländska företag till Sverige. ”Sverige lämpar sig annars särskilt väl för internetoperatörer som kräver tillgång till energi och kyla för sina servrar”, enligt Ljudén. ”– Vi får väldigt många förfrågningar från företag som vill bygga upp stora datacenter”.

IT-företaget Intel har nyligen investerat stora pengar i Sverige i utbyggnaden av fjärde generationens mobiltelefoni. Tvärtemot Invest in Sweden Agency tror Carl-Daniel Norenberg, affärsutvecklare på Intel, inte att FRA-lagen har betydelse för investeringsviljan. ”– Det här påverkar inte på något sätt vår verksamhet. Vi rullar på som vanligt”, säger han till TT.

2.3 Suomalainen keskustelu

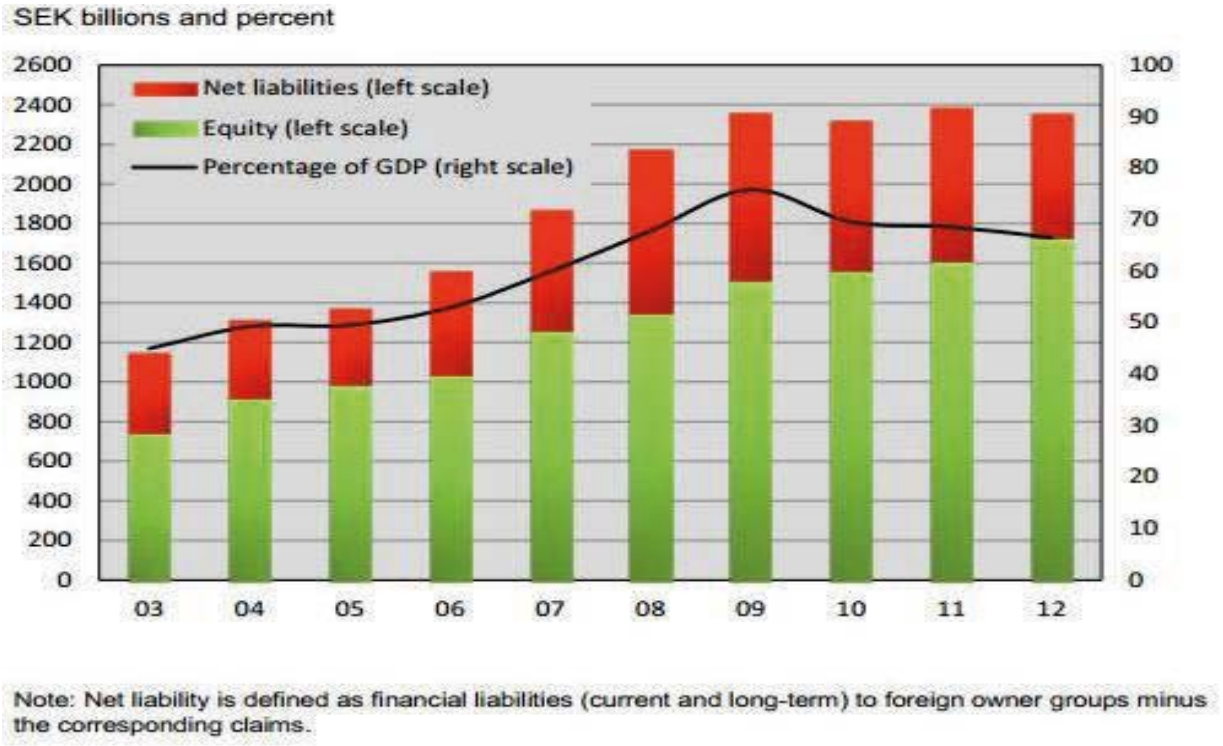
Teknologiateollisuus nousi voimakkaasti varpailleen esitetystä "massaurkintalaista".
10.3.2014 13:00, It-viikko.

”Suomen hallituksen edustajat rakentavat pilvilinnoja datakaapelihankkeista ja Suomen mahdollisesta noususta Euroopan "dataässäksi" tai "data-Sveitsiksi". Mutta samaan aikaan hallituksessa puuhataan tiedonkeruulakia, jota kriitikot nimittävät massaurkintalaiksi”. Teknologiateollisuus ry pelkää, että lakihanke poliisin toimintaedellytysten parantamiseksi digitaalisessa maailmassa pilaa Suomen maineen tietoturvallisena ja puolueettomana maana ja tappaa orastavan databisneksen alkuunsa.

3 Tarkastelun näkökulmat

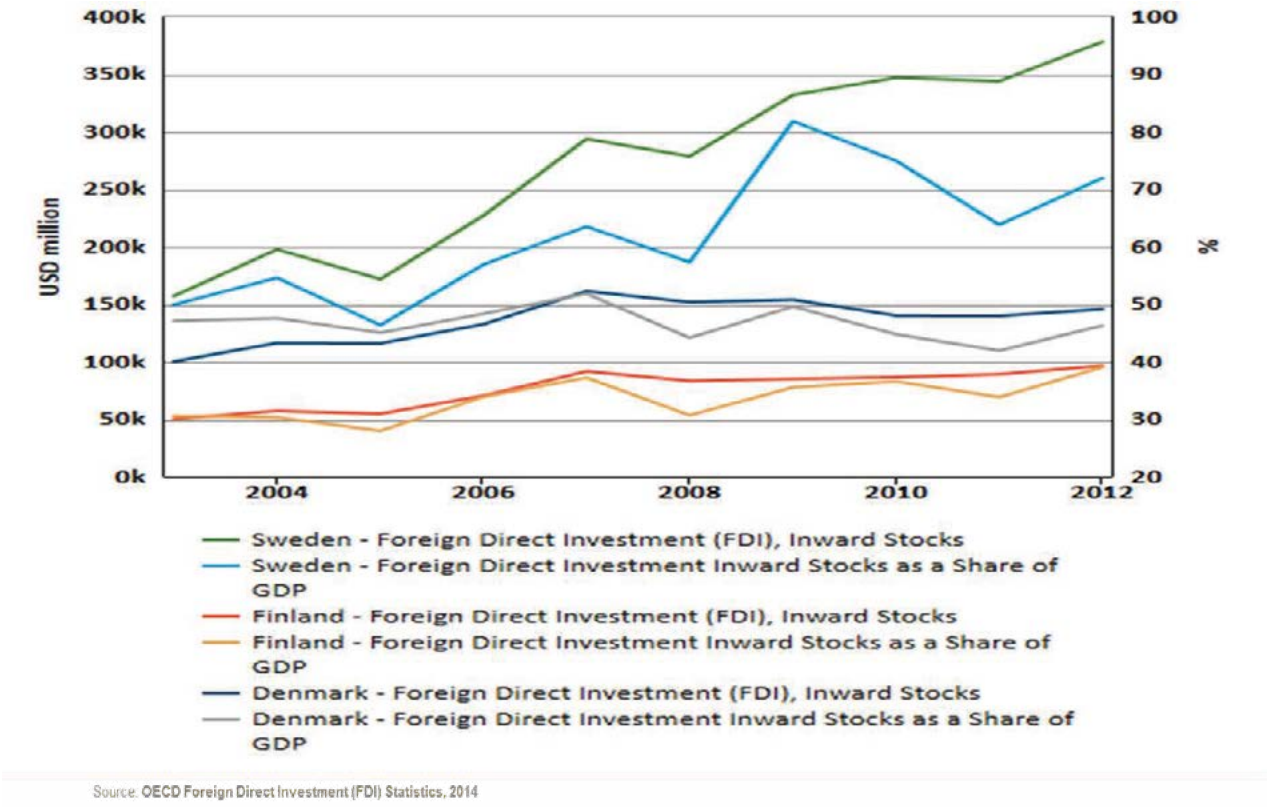
3.1 Vaikutukset investointeihin ja niiden edellytyksiin

Ulkomaisten investointien yleistä kehitystä Ruotsissa kuvaavassa kuviossa 1 ei ole sellaista poikkeamaa investointien kehityksessä lain voimaantulon jälkeen vuonna 2009, joka voitaisiin perustella FRA-lain vaikutuksella. Nousujohteisen kehittymisen taittuminen vuonna 2009 on selitettävissä koko maailmaa ravistelleella pankkikriisillä, ja siitä johtuvasta yleisestä investointien kasvun taittumisesta. Kuvio ei erikseen kerro IT-sektorin investointien määrän muutoksista, mutta niiden katsotaan seuraavan samankaltaista kehitystä pohjautuen alan asiantuntijoiden kommentteihin.



Kuvio 1. Ulkomaalaisten investointien kehitys Ruotsissa.

Laajempi kuva Ruotsin FRA-lain vaikutuksista koko ulkomaalaisten investointien kentässä saadaan, kun verrataan Ruotsin, Suomen ja Tanskan kehitystä toisiinsa. Kuviosta 2 voidaan havaita, että lain voimaantulolla ei ole selkeää merkitystä Ruotsin ulkomaalaisten investointien kehitykselle verrattuna Suomeen ja Tanskaan. Myöskään tässä kuviossa ei ole eriteltynä IT-sektorin investointeja, mutta ne ovat seuranneet yleistä kehitystä kaikissa vertailun kohteena olevissa maissa.



Kuvio 2. Ulkomaalaisten investointien suuruus miljoonissa dollareissa ja osuus BKT:sta Ruotsissa, Suomessa ja Tanskassa.

Edellisten kuvioiden pohjalta voidaan yleisellä tasolla todeta, että ulkomaalaisten investointien määrään kehittymiseen ei ole selkeää syy-seuraussuhdetta FRA-lain voimaan tulolla vuonna 2009.

3.2 Vaikutukset T&K toimintaa Ruotsissa

Tarkasteltaessa tutkimus- ja kehitysmenojen osuutta taulukossa 1 suhteessa BKT:hen Ruotsissa ja Suomessa, on vaikea nähdä mitään merkittävää poikkeamaa kehityskulussa. Ruotsin tutkimus ja kehitysmenot suhteessa BKT:hen hieman laskivat vuonna 2009 ja siitä eteenpäin, Suomessa lasku alkoi vuodesta 2011 alkaen. Huomioitavaa kuitenkin on, että myös tason laskun jälkeenkin Ruotsi ja Suomi ovat kehitysmenojen BKT osuuden suhteen kärjessä ja selkeästi korkeammalla tasolla kuin muut EU vertailuryhmän maat. Kehitysmenojen tason laskua kulkua suhteessa FRA-lakiin on vaikeaa nähdä FRA-laista johtuvaksi, kyseiseen ajankohtaan osuu globaali talouden taantuma ja talouden toimijoiden tiukempi budjetinhallinta, ja laskeva kehitys näkyy myös Suomen luvuissa pienellä viiveellä.

Taulukko 1. Tutkimus- ja kehitysmenojen osuus BKT:stä 2002 – 2010.

	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
EU-28	1.87	1.86	1.82	1.82	1.84	1.84	1.91	2.01	2.00	2.04	2.06
Euro area (EA-17)	1.88	1.87	1.85	1.84	1.87	1.88	1.96	2.06	2.07	2.12	2.14
Belgium	1.94	1.87	1.86	1.83	1.86	1.89	1.97	2.03	2.10	2.21	2.24
Bulgaria	0.48	0.48	0.49	0.46	0.46	0.45	0.47	0.53	0.60	0.57	0.64
Czech Republic	1.15	1.20	1.20	1.22	1.29	1.37	1.30	1.35	1.40	1.64	1.88
Denmark (1)	2.51	2.58	2.48	2.46	2.48	2.58	2.85	3.16	3.00	2.98	2.99
Germany	2.50	2.54	2.50	2.51	2.54	2.53	2.69	2.82	2.80	2.89	2.92
Estonia	0.72	0.77	0.85	0.93	1.13	1.08	1.28	1.41	1.62	2.37	2.18
Ireland	1.10	1.16	1.23	1.25	1.25	1.28	1.45	1.69	1.69	1.66	1.72
Greece (2)	:	0.57	0.55	0.60	0.59	0.60	:	:	:	0.67	0.69
Spain	0.99	1.05	1.06	1.12	1.20	1.27	1.35	1.39	1.40	1.36	1.30
France (3)	2.24	2.18	2.16	2.11	2.11	2.08	2.12	2.27	2.24	2.25	2.26
Croatia	0.96	0.96	1.05	0.87	0.75	0.80	0.90	0.85	0.75	0.76	0.75
Italy	1.12	1.10	1.09	1.09	1.13	1.17	1.21	1.26	1.26	1.25	1.27
Cyprus	0.30	0.35	0.37	0.41	0.43	0.44	0.43	0.49	0.50	0.50	0.47
Latvia	0.42	0.38	0.42	0.56	0.70	0.60	0.62	0.46	0.60	0.70	0.66
Lithuania	0.66	0.67	0.75	0.75	0.79	0.81	0.80	0.84	0.79	0.91	0.90
Luxembourg	:	1.65	1.63	1.56	1.66	1.58	1.66	1.74	1.51	:	:
Hungary (4)(5)	1.00	0.94	0.88	0.94	1.01	0.98	1.00	1.17	1.17	1.22	1.30
Malta (4)	0.25	0.25	0.51	0.55	0.60	0.57	0.55	0.53	0.66	0.72	0.84
Netherlands (2)	1.88	1.92	1.93	1.90	1.88	1.81	1.77	1.82	1.86	2.03	2.16
Austria	2.12	2.24	2.24	2.46	2.44	2.51	2.67	2.71	2.80	2.77	2.84
Poland	0.56	0.54	0.56	0.57	0.56	0.57	0.60	0.67	0.74	0.76	0.90
Portugal (6)	0.73	0.71	0.74	0.78	0.99	1.17	1.50	1.64	1.59	1.52	1.50
Romania (3)(7)	0.38	0.39	0.39	0.41	0.45	0.52	0.58	0.47	0.46	0.50	0.42
Slovenia (3)(6)	1.47	1.27	1.39	1.44	1.56	1.45	1.66	1.85	2.10	2.47	2.80
Slovakia	0.57	0.57	0.51	0.51	0.49	0.46	0.47	0.48	0.63	0.68	0.82
Finland	3.36	3.44	3.45	3.48	3.48	3.47	3.70	3.94	3.90	3.80	3.55
Sweden (8)	:	3.80	3.58	3.56	3.68	3.43	3.70	3.62	3.39	3.39	3.41
United Kingdom	1.78	1.73	1.67	1.70	1.72	1.75	1.75	1.82	1.77	1.78	1.72
Iceland	2.95	2.82	:	2.77	2.99	2.68	2.65	3.11	:	2.40	:
Norway	1.66	1.71	1.57	1.51	1.48	1.59	1.58	1.76	1.68	1.65	1.66
Switzerland	:	:	2.82	:	:	:	2.87	:	:	:	:
Serbia	:	:	:	:	:	:	:	0.92	0.79	0.77	0.96
Turkey	0.53	0.48	0.52	0.59	0.58	0.72	0.73	0.85	0.84	0.86	:
China (except Hong Kong)	1.07	1.13	1.23	1.32	1.39	1.40	1.47	1.70	1.76	1.84	:
Japan (6)	3.12	3.14	3.13	3.31	3.41	3.46	3.47	3.36	3.25	:	:
United States (6)	2.52	2.52	2.45	2.49	2.55	2.62	2.76	2.81	2.73	2.67	:

(1) 2007: break in series. 2009: definition differs.
(2) 2011: break in series.
(3) 2004 and 2010: break in series.
(4) 2004: break in series.
(5) 2002 and 2003: definition differs.
(6) 2008: break in series.
(7) 2012: definition differs.
(8) 2005: break in series. 2003, 2004, 2006 and 2010: definition differs.
(9) 2006: break in series. Definition differs.
Note: when definitions differ, see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/EN/rd_esms.htm.
Source: Eurostat (online data codes: t2020_20 and rd_e_gerdtot), OECD

Toisena tarkastelukulmana voidaan käyttää tutkimus- ja kehitysmenojen panostusten lähderahoituksen kehitystä. Taulukko 2 kuvaa rahoituslähteiden jakautumista tutkimus- ja kehitysmenojen kattamiseksi vuosina 2007 ja 2011. Ruotsin rahoituslähdekehityksestä voidaan havaita, että ulkomaalaiset tahot ovat jopa selkeästi lisänneet panostuksiaan vertailujakson aikana suhteessa Ruotsin sisältä tulevaan sekä yksityisen- että julkisen sektorin panostuksiin nähden. Tämä antaa vahvoja viitteitä, ettei FRA-lailla ole ollut merkitystä ulkomaalaisten tutkimus- ja kehityspanostusten kohdentamisessa. Ruotsin kehitysmenojen tason tippuminen selittyy valtaosin ruotsalaisten yhtiöiden ja julkisen puolen jarruttamisella.

Taulukko 2. Tutkimus- ja kehitysmenojen rahoituslähteet 2007 ja 2011.

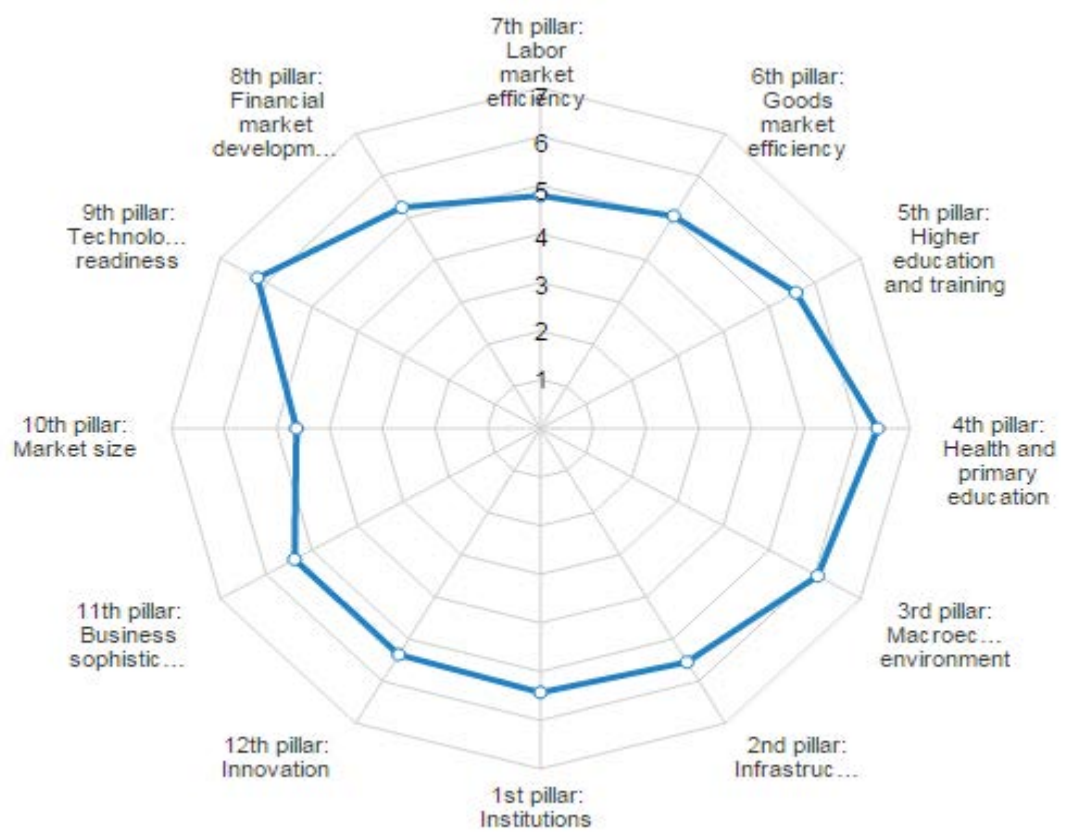
	Business enterprise sector		Government sector		Abroad	
	2007	2011	2007	2011	2007	2011
EU 28	*54.9*	*54.9*	*33.3*	*33.4*	*9.2*	*9.2*
Euro area (EA-17)	*56.7*	*56.8*	*34.0*	*33.9*	*7.4*	*7.4*
Belgium	61.4	60.2	22.2	23.4	13.0	13.0
Bulgaria	34.2	16.9	56.7	38.8	7.6	43.9
Czech Republic	47.2	37.7	44.7	41.7	7.3	19.7
Denmark (1)	61.0	60.3	25.9	28.9	9.5	7.2
Germany	68.1	65.6	27.5	29.8	4.0	4.2
Estonia	41.6	55.0	45.6	32.8	11.7	11.9
Ireland	49.5	*48.4*	32.4	*30.0*	15.0	*20.1*
Greece	:	32.7	:	49.2	:	14.8
Spain	45.5	44.3	43.7	44.5	7.0	6.7
France (2)	52.3	55.0	38.1	35.4	7.5	7.7
Croatia	35.5	38.2	50.4	48.2	10.9	11.6
Italy	42.0	45.1	44.3	41.9	9.5	9.1
Cyprus	16.4	11.0	64.6	70.6	14.5	14.1
Latvia	36.4	24.8	49.9	22.5	12.7	51.0
Lithuania	32.8	28.2	46.9	42.2	19.6	28.4
Luxembourg (3)	70.0	44.3	18.2	34.8	5.7	20.7
Hungary	43.9	47.5	44.4	38.1	11.1	13.5
Malta	51.9	51.9	25.7	29.0	22.4	16.8
Netherlands (2)	48.8	49.9	38.0	35.5	10.7	10.9
Austria	48.7	46.2	32.3	35.8	17.9	16.9
Poland	34.3	28.1	58.6	55.8	6.7	13.4
Portugal (2)	47.0	44.0	44.6	41.8	5.4	5.9
Romania (2)	26.9	37.4	67.1	49.1	4.5	12.1
Slovenia (2)	58.3	61.2	35.6	31.5	5.8	7.0
Slovakia (4)	35.6	33.9	53.9	49.8	10.2	14.2
Finland (5)	68.2	67.0	24.1	25.0	6.5	6.5
Sweden	62.8	57.3	24.6	27.7	9.6	11.1
United Kingdom	46.0	45.9	30.9	30.5	17.3	17.8
Iceland	50.4	47.5	38.8	42.3	10.0	8.4
Norway	45.0	44.2	44.9	46.5	8.5	7.8
Switzerland (6)	68.2	:	22.8	:	6.0	:
Serbia (7)	8.3	9.1	62.9	63.4	7.2	5.5
Turkey (8)	48.4	45.8	47.1	29.2	0.5	0.7
China (except Hong Kong) (9)	70.4	73.9	24.6	21.7	1.3	1.3
Japan (2)(3)(4)	77.7	75.9	15.6	17.2	0.3	0.4
United States (5)	64.9	*60.0*	29.1	33.4	:	:

(1) Government sector, 2007: definition differs.
(2) Break in series.
(3) 2010 instead of 2011.
(4) Government sector: definition differs.
(5) Government sector: break in series.
(6) 2008 instead of 2007.
(7) 2009 instead of 2007.
(8) Business enterprise and government sectors: break in series. Business enterprise and government sectors, 2007: definition differs.
(9) Definition differs.
Note: when definitions differ, see http://epp.eurostat.ec.europa.eu/cache/ITY_SDDS/EN/rd_esms.htm.
Source: Eurostat (online data code: tsc00031), OECD

Yhteenvetona tutkimus- ja kehitysmenoista voidaan todeta, että FRA-lailla ei ole ollut käytännön merkitystä tämän alueen aktiivisuuteen. Suurin selittävä tekijä muutoksissa on ollut taloudellinen kehitys ja Ruotsin vahva panostus tutkimukseen ja kehitykseen suhteessa BKT:hen mikä on jatkunut toimintaympäristön muutoksista huolimatta.

3.3 Vaikutukset kansainväliseen kilpailukykyyn Ruotsissa

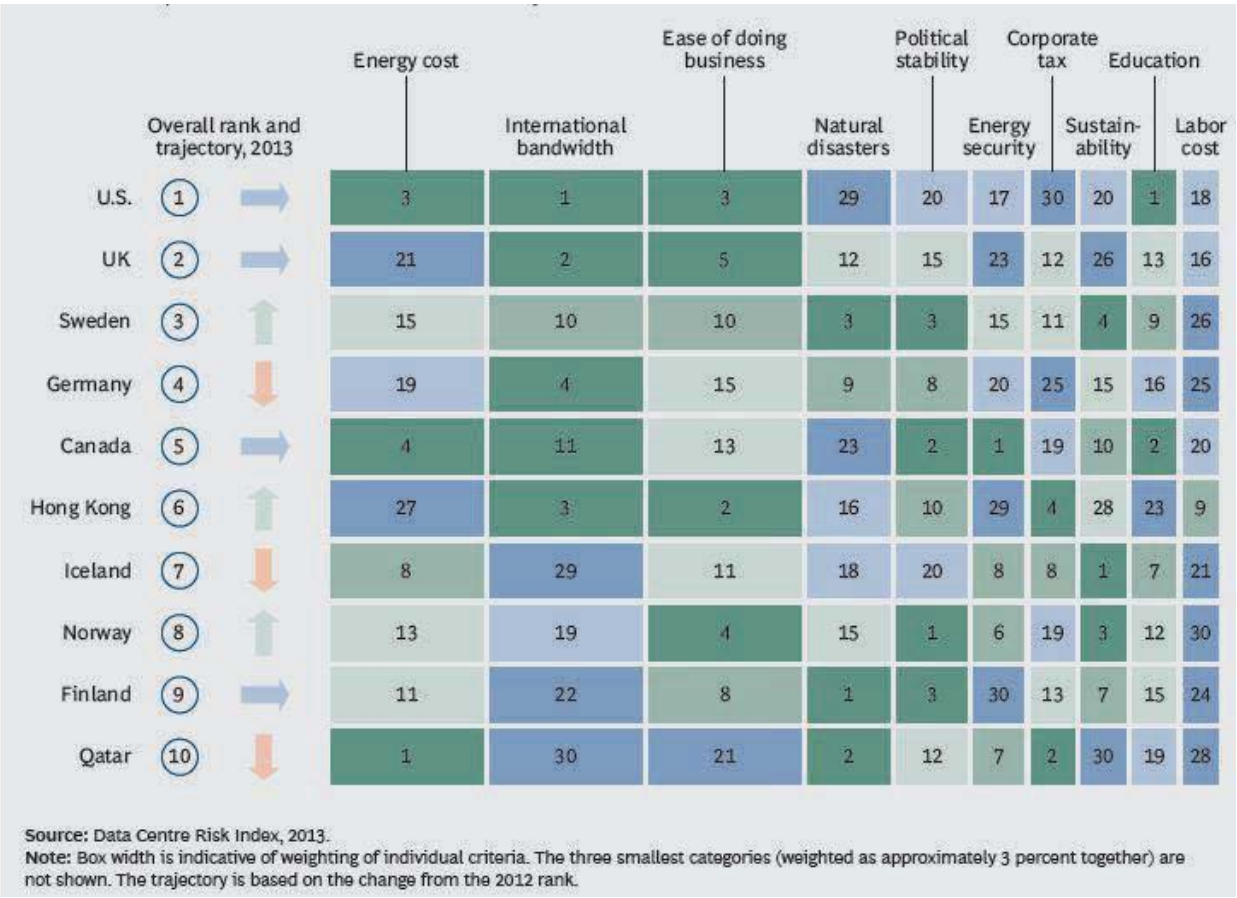
World Economic Forumin vertailuissa Ruotsi sijoittuu kärkikymmenikköön sekä kansainvälistä kilpailukykyä että innovaatioita arvioitaessa. Kuviossa 3 on kuvattu Ruotsin kilpailukykyä eri sektoreittain arvioituna. Kuviosta voidaan havaita, että maa saa varsin korkeat arviot usealla sektorilla. Näiden kilpailukykytekijöiden pohjalta FRA-lain suoraa merkitystä Ruotsin kilpailukykyyn yleisellä tasolla on vaikea todeta, mutta toisaalta infrastruktuuri ja viranomaistoiminta saavat korkeat arvosanat tässä tarkastelussa.



Kuvio 3. Ruotsin kilpailukykyarvio sektoreittain. (www.weforum.org.)

Huomattavasti selkeämmin eri maiden kilpailukykyä IT investointien näkökulmasta voidaan arvioida datakeskustoiminnan edellytysten lähtökohdista. FRA-laki on vahvasti sidoksissa datakeskusten toimintaedellytyksiin ja laitosten sijoittumispaikan arvioimiseen. Taulukossa 3 on vuosittain tehtävä kansainvälinen riskivertailu datakeskusten sijoituspaikkojen tärkeimmistä kohdemaista. Ruotsi pärjää vuoden 2013 vertailussa erinomaisesti sijoittuen kolmanneksi. Ruotsi on nostanut sijoitustaan selkeästi vuoden 2012 kahdeksannelta sijalta kolmanneksi, Suomi on vastaavasti säilyttänyt yhdeksännen sijansa molempina vuosina. FRA-lain syntyvaiheen polemiikki ei näin ollen näy sijoittumispaikkoja analysoivassa riskivertailussa. Käytännössä Ruotsin kilpailukyky tällä alueella näkyy merkittävinä uusina datakeskushankkeina, mm. Facebook 2011 ja kapasiteetin laajennus 2014, KnC Miner 2014, Hydro66 2014 sekä Bahnhofin iso laajennusprojekti Tukholmassa. Suomeen on vastaavana ajanjaksona investoinut mm. Google, toteuttaen useampia laajennuksia, Telecity sekä Yandex.

Taulukko 3. Maiden riskivertailu Datakeskuksen sijoituspaikkana.



	Overall rank and trajectory, 2013	Energy cost	International bandwidth	Ease of doing business	Natural disasters	Political stability	Energy security	Corporate tax	Sustain-ability	Education	Labor cost
U.S.	1 →	3	1	3	29	20	17	30	20	1	18
UK	2 →	21	2	5	12	15	23	12	26	13	16
Sweden	3 ↑	15	10	10	3	3	15	11	4	9	26
Germany	4 ↓	19	4	15	9	8	20	25	15	16	25
Canada	5 →	4	11	13	23	2	1	19	10	2	20
Hong Kong	6 ↑	27	3	2	16	10	29	4	28	23	9
Iceland	7 ↓	8	29	11	18	20	8	8	1	7	21
Norway	8 ↑	13	19	4	15	1	6	19	3	12	30
Finland	9 →	11	22	8	1	3	30	13	7	15	24
Qatar	10 ↓	1	30	21	2	12	7	2	30	19	28

Source: Data Centre Risk Index, 2013.
Note: Box width is indicative of weighting of individual criteria. The three smallest categories (weighted as approximately 3 percent together) are not shown. The trajectory is based on the change from the 2012 rank.

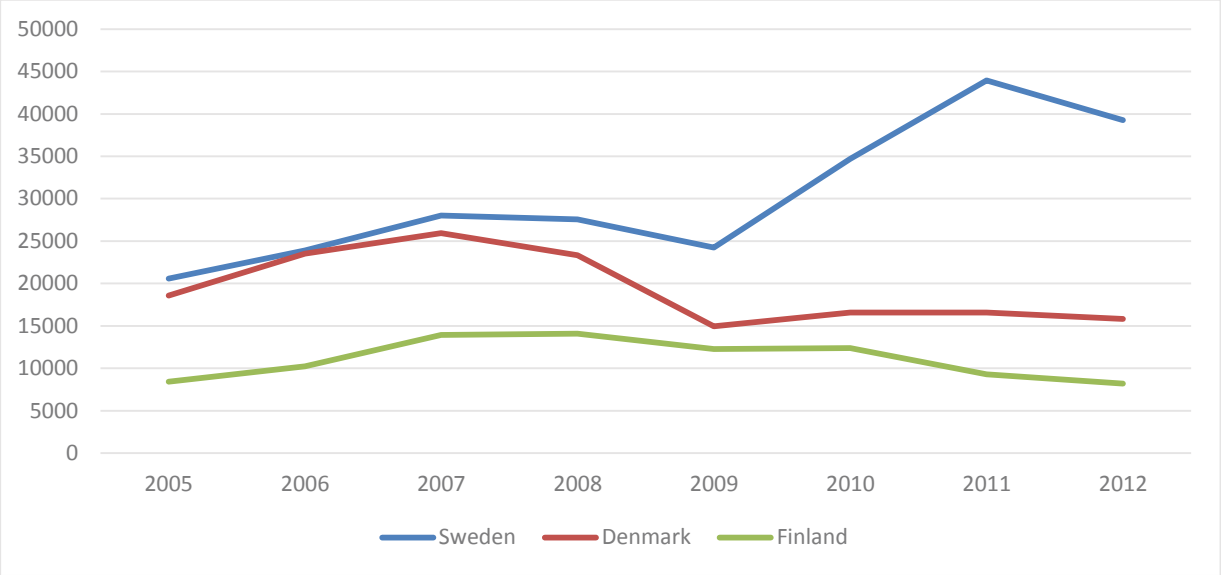
Arvioitaessa FRA-lain vaikutuksia Ruotsin kansainväliseen kilpailukykyyn, sillä ei näyttäisi olevan negatiivisia vaikutuksia, ei ainakaan datakeskusten sijoittumisen kannalta. Datakeskukset ja niiden asiakaskunta kattavat hyvin laajasti erilaiset sidosryhmät, joten tältä kannalta näkemys on kattava. Myöskään tässä datakeskusten vuosittain tehtävässä sijoituspaikkavertailussa kyseinen laki ei ole noussut esiin.

Toisaalta näyttäisi jopa siltä, että Snowden-paljastusten tuomasta tietoisuuden lisääntymisestä johtuen, Ruotsin selkeät pelisäännöt viranomaisten tiedonhankintaa koskien ovat jopa kilpailuetu nykyisessä muodossaan. Isojen pitkäaikaisten investointien kohdalla riskien minimointi ja toimintaympäristön kehityksen ennakoitavuus ovat merkittäviä eri maiden kilpailukykyyn vaikuttavia tekijöitä.

3.4 Vaikutukset uuden yritystoiminnan syntyyn Ruotsissa ja Suomessa

Ruotsin ICT-sektori on kehittynyt positiivisesti suhteessa muuhun talouteen viimeisten vuosien aikana, jonka ansiosta myös alan uudet yritykset ja yhteiskunnallinen merkittävyys ovat kasvaneet hyvää tahtia. Kun verrataan uusien yritysten perustamisen kehittymistä Ruotsissa, Suomessa ja Tanskassa vuosina 2005 – 2012 (kuvio 4), Ruotsi ottaa vertailun ehdottoman kärkipaikan. FRA-lain

merkitys yritysten yleisessä toimintaympäristössä on hyvin pieni, eikä sen voida katsoa vaikuttaneen yritystoiminnan kehitykseen tai uusien yritysten syntyyn suuntaan tai toiseen.



Kuvio 4. Perustetut yritykset 2005 – 2012.

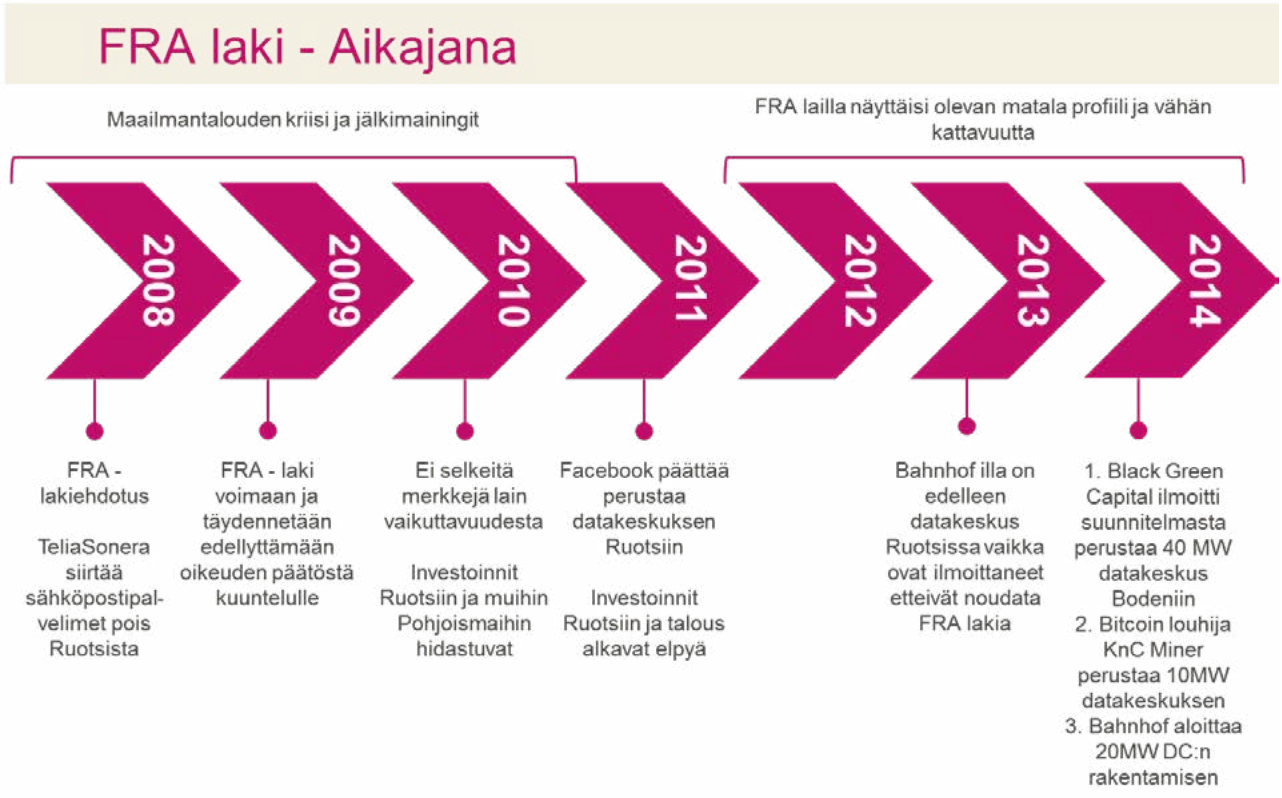
Vahvaa ICT-sektorin kehitystä kuvaa esimerkiksi Facebookin perustama suuri datakeskus, jonka alkuperäisen investointipäätöksen syntyaikana 2010 - 2011 FRA-laki on ollut voimassa. Facebook on kommentoinut FRA-lakiasiaa viittaamalla, että kaikilla valtioilla on omat keinonsa tietoliikenteen seurantaan, jonka vuoksi selvästi järjestetyllä asialla ei ole investointipäätöksessä merkitystä.

3.5 Vaikutukset erilaisille yrityksille tai yritysryhmille Ruotsissa

TeliaSonera siirsi FRA-lain syntymisen myötä sähköpostipalvelimensa Suomeen vuonna 2008, koska Suomen laki edellyttää kirjesalaisuuden säilyttämistä myös sähköpostiliikenteessä. TeliaSonera toi samalla myös Ruotsin sähköpostiliikenteen Suomessa sijaitseviin datakeskuksiin, mutta tämän jälkeen palvelun tuotantopaikasta ja sähköpostiliikenteen sisältävän datan sijainnista ei ole käytettävissä tarkempaa tietoa.

FRA-laki aiheutti keskustelua Ruotsissa myös erityisesti ICT-infrastruktuuritoimijoiden keskuudessa, joiden liiketoimintaan lailla olisi voinut olla suoranaisia tulosvaikutuksia. Lain todelliset vaikutukset liiketoimintaan ovat kuitenkin olleet vähäiset tai jääneet kokonaan toteutumatta. Snowden-paljastusten jälkeen yritysten yleinen tietoisuus tiedonhankinnasta on kasvanut.

3.6 FRA aikajana Ruotsissa



Aikajanan perusteella voi selkeästi todeta, että alkuhämmennyksen ja lain käytännön toteutukseen liittyvän epätietoisuuden jälkeen laki ei ole vaikuttanut esimerkiksi datakeskusinvestointeihin. Myös vuoden 2014 uusiin T&K investointeihin liittyneet uutisoinnit tukevat näkemystä, ettei laki ole hidastanut investointeja. Myös yritykset investoivat voimakkaasti:

2014-06-17 08:00 - CIO Sweden: ”It-investeringarna växer snabbare än någonsin”

4 Yhteenveto

FRA-lain valmisteluvaiheen voimakkaat kannanotot ja toimenpiteet yritysten taholta ovat pääosin vaimenneet. Nykyinen uutisointi liittyy enemmän kansalaisoikeuksiin, NSA paljastuksiin sekä poliittiseen keskusteluun asian ja FRA:n yleisen toiminnan ympärillä.

Yksittäisenä yrityksenä Bahnhof vastustaa edelleen julkisesti lain toimeenpanoa omassa toiminnassaan, mutta selkeästi ei koe tilannetta omaa tai asiakkaidensa liiketoimintaa haittaavaksi. Ovat kasvattaneet toimintaansa Ruotsissa voimakkaasti, ja ovat myös käynnistäneet uuden ison laajennusprojektin Tukholmassa, ”Project Green”. Tavoitteena on rakentaa vuoden 2016 loppuun mennessä uusi 20MW datakeskus ja merkittävä tietoliikenteen solmukohta Tukholman keskustaan ja hyödyntää energiantuotannon ja jäähdytyksen synergioita yhteistyössä Fortumin kanssa. Tämän kokoinen laitos on kokoluokaltaan 200 M€ investointi, jota ei tehdä ilman sitovia asiakassopimuksia.

Yhteenvetona voidaan todeta, että selkeää yhteyttä FRA-lain mahdollisista vaikutuksista IT sektorin ulkomaisiin investointeihin lain voimaantulon jälkeen tai eroavaisuuksia vastaaviin investointeihin Suomessa ei selvityksen pohjalta ole todettu.

Toisaalta on myös syntynyt näkemys, että täsmällisesti säädetty laki luo ennustettavamman toimintaympäristön kaikille IT sektorin toimijoille. Investoinnit ovat luotettavammalla pohjalla, kun yhteiset pelisäännöt ovat selvillä. Isot kansainväliset yritykset ovat myös tulleet entistä tietoisemmaksi cyber-turvallisuuden alueesta, jonka seuraamiseksi ja hyökkäysten hallitsemiseksi ovat julkisen vallan pelisäännöt tervetulleita.

5 Linkkejä

Suomi linkkejä:

http://www.etla.fi/wp-content/uploads/ETLA-Raportit-Reports-1.pdf
http://www.itviikko.fi/uutiset/2014/03/10/teknologia-ala-urkintalaki-saattaa-kostautua-kivuliaasti/20143451/7?pos=related

Ruotsi linkkejä:

http://www.thelocal.se/20070530/7452
http://www.aftonbladet.se/nyheter/article11442895.ab

Saksa linkkejä:

http://www.sueddeutsche.de/digital/bundesnachrichtendienst-aufruesten-fuer-den-cyberkampf-1.2211761

Muita linkkejä:

http://www.itworld.com/article/2845603/german-spy-agency-seeks-millions-to-monitor-social-networks-outside-germany.html#tk.rss_news

Yhteystiedot:
Vesa Weissmann
Gearshift Group Ltd.
Mannerheimintie 16, 4th Floor
FI-00100 Helsinki, Finland
Mobile +358 50 500 2120
Email vesa.weissmann@gearshiftgroup.com
Web www.gearshiftgroup.com

SIDOSRYHMIEN JA ASIANTUNTIJOIDEN KUULEMINEN

YHTEENVETO

1. Lausuntokierros työryhmän asettamispäätöksestä

Työnsä tukemiseksi työryhmä pyysi työryhmän asettamispäätöksestä lausuntoa seitsemältä taholta, jotka olivat

- Einkeinoelämän keskusliitto
- Electronic Frontier Finland (EFFI) ry
- Tietoliikenteen ja tietotekniikan keskusliitto FiCom ry
- Finnish Communication and Internet Exchange (FiCix) ry
- Huoltovarmuuskeskus
- FiSC Finnish Information Security Cluster ry ja Teknologiateollisuus ry (yhteinen lausunto)

FiCom ry toimitti lisäksi työryhmän käyttöön taustamuistion (Yritysmaailman näkökohtia turvallisuusviranomaisten tiedonhankintakyvyn kehittämiseen liittyvään lainsäädäntöhankkeeseen", versio 0.3D, 16.1.2014).

Lausunnonantajia pyydettiin esittämään näkemyksiään erityisesti työryhmän tavoitteista ja tehtävistä sekä siitä, mitä oikeudellisia ja yhteiskunnallisia näkökohtia työryhmän työssä tulisi ottaa huomioon.

Lausuntokierros ajoitettiin työskentelyn alkuvaiheeseen, jotta saatu palaute voitiin ottaa huomioon työskentelyn aikana.

Lausuntopyyntö, lausunnot ja muut kannanotot sekä lausunnoista ja työryhmälle toimitetuista muista kirjallisista huomiosta tehty erillinen yhteenveto on julkaistu puolustusministeriön Internet-sivuilla.

2. Kuulemistilaisuudet elinkeinoelämälle ja järjestöille

Työryhmä järjesti kaksi kuulemistilaisuutta elinkeinoelämälle (29.4.2014) ja järjestöille (6.5.2014). Painopiste kuulemistilaisuuksissa oli tietoliikennetiedustelu. Työryhmä varasi kutsutuille mahdollisuuden toimittaa myös kirjallisia kannanottoja.

Kirjallisen kannanoton toimittivat

- F-Secure Oyj
- Nokia Oyj ja Nokia Solutions and Networks (yhteinen kannanotto)
- TDC Oy
- Microsoft Oyj
- Keskuskauppakamari
- Internet-käyttäjät ikuisesti – IKI ry
- Finnish Communication and Internet Exchange (FiCix) ry

Kutsut, osallistujalistat ja tilaisuuksien ohjelmat sekä työryhmälle toimitetut kirjalliset kannanotot on julkaistu puolustusministeriön Internet –sivulla.

3. Taustoittamistilaisuus toimittajille

Työryhmä järjesti toimittajille taustoittamistilaisuuden 12.3.2014. Tilaisuudessa esiteltiin työryhmän toimeksiantoa ja työn tavoitteita sekä muita työskentelyssä huomioon otettavia seikkoja.

4. Työryhmän kuulemat asiantuntijat

Työryhmä kuuli työnsä aikana 26 asiantuntijaa, jotka edustivat hankkeen kannalta keskeisiä viranomaisia ja sidosryhmiä.

tilannekuvakoordinaattori, yksikön päällikkö Jarkko Korhonen, valtioneuvoston kanslia
valtioneuvoston turvallisuusjohtaja Timo Härkönen, valtioneuvoston kanslia
tietohallintojohtaja Ari Uusikartano, ulkoasiainministeriö
erityisasiantuntija Kimmo Janhunen, valtiovarainministeriö

EU:n tiedusteluanalyysikeskuksen johtaja Ilkka Salmi
EU:n sotilastiedustelun päällikkö Georgij Alafuzoff

tietosuojavaltuutettu Reijo Aarnio
oikeustieteen professori Veli-Pekka Viljanen, Turun yliopisto

varautumispäällikkö ICT Christian Fjäder, Huoltovarmuuskeskus
johtaja Kirsi Karlamaa, Viestintävirasto
turvallisuussääntelyryhmän päällikkö Jarkko Saarimäki, Kyberturvallisuuskeskus
tietoturva-asiantuntija Tomi Hasu, Kyberturvallisuuskeskus
Keskusrikospoliisin päällikkö, poliisineuvos Robin Lardot
rikoskomisario Timo Piiroinen, Keskusrikospoliisi
järjestelmäasiantuntija Pasi Paunu, Suojelupoliisi

Nordic Policy Counsel David Mothander, Google
hallinto- ja turvallisuusjohtaja Vesa Vuoti, DNA Oyj
Head of Special Network Security Krister Kaipio, TeliaSonera Finland Oyj
turvallisuusjohtaja Jaakko Wallenius, Elisa Oyj
Platform Strategy Manager Pasi Mäkinen, Microsoft Oy
Vice President Kaisa Olkkonen, Nokia Government Relations
Head of Security Technologies Gabriel Waller, Nokia Solutions and Networks
tutkimusjohtaja Mikko Hyppönen, F-Secure Oyj
teknologiajohtaja Kimmo Kasslin, F-Secure Oyj
Pk- johtaja Jyrki Hollmén, Elinkeinoelämän keskusliitto
Associate Partner Vesa Weissmann, Gearshift Group Oy

5. Yhteenveto sidosryhmien ja asiantuntijoiden kannanotoista

5.1 Hankkeen organisointi, tavoitteet ja tehtävät

Kuulemistilaisuuksissa kiinnitettiin huomiota viranomaisten tiedonhankintaa selvittävän työryhmän työhön prosessina. Etenkin elinkeinoelämän edustajat painottivat sitä, että elinkeinoelämä on otettava kiinteämmin työhön mukaan kysymyksissä, jotka eivät liity viranomaisten toimivaltajakoon tai vastaavaan.

Kohdennettu verkkotiedonhankinta olisi herkkä asia. Sitä pitäisi valmistella yhteistyössä myös elinkeinoelämän kanssa. Tuotiin esiin huolta siitä, että taloudelliset intressit eivät ole keskeistä työssä. Elinkeinoelämän on voitava luottaa viranomaisiin samoin kuin viranomaisten elinkeinoelämään.

Tietoa työryhmän työstä oli varsinkin työn alkuvaiheessa ollut saatavana niukasti. Valmistelun edellytettiin olevan avointa, laajapohjaista ja huolellista.

Työryhmälle asetettua puolen vuoden määräaikaa pidettiin liian lyhyenä laajan, yhteiskunnallisesti merkittävän ja pitkävaikutteisen hankkeen toteuttamiseksi.

Työryhmän asettamispäätös herätti keskustelua ja se, että päätöstä voi tulkita niin, ettei valtuutta kybertiedonhankintaa laajempaan tiedonhankintatarpeiden selvittämiseen välttämättä ole. Työryhmän työn tavoitteissa tulisi myös ottaa huomioon yksityisen sektorin tehtävä kyberuhkien havainnoinnissa.

Nykylainsäädännön tarkastelua pidettiin tärkeänä tavoitteena. Joidenkin näkemysten mukaan lainsäädäntö antaa jo nyt runsaasti erilaisia toimintamahdollisuuksia viranomaisille. Päällekkäisiä tai ristiriidassa olevia toiminta- ja valvontamekanismeja ei tulisi rakentaa.

Jotkut asiantuntijat totesivat, että työryhmän työn tuloksia ei pitäisi kirjoittaa hallituksen esityksen muotoon. Jatkotyön pohjaksi laadittavassa työryhmän muistiossa tulisi huomioida sektorikohtainen erityissääntely ja arvioida tiedonhankintaa koskevan sääntelyn vaikutukset ja mahdolliset soveltamisalan rajoitukset toimialoittain, esimerkiksi terveyspalvelujen ja pankkitoiminnan toimialoilla.

5.2 Internetin ja viestinnän luonne

Asiantuntijat painottivat Internetin ja viestinnän rajat ylittävää luonnetta. Useat suomalaisilta näyttävät palvelut tuotetaan tosiasiassa ulkomailta. Kansalliset rajat eivät asiantuntijoiden mukaan toimi Internetissä. Lisäksi pilvipalvelut yleistyvät, eikä enää ole niin keskeistä, missä tieto fyysisesti sijaitsee.

Internetissä liikkuu valtava määrä tietoa ja tiedon määrä kasvaa koko ajan. Kaikenkattavan valvonnan järjestäminen on tästä syystä haastavaa teknisesti ja taloudellisesti. Kuulemistilaisuuksissa pohdittiin myös sitä, että Intenet on ollut käytössä jo 20 vuotta mutta siihen liittyviä ongelmia selvitetään vasta nyt.

5.3 Tietoturvallisuuden taso ja kehittäminen

Kuulemisissa tuotiin esille, että Suomen maine hyvän tietoturvan maana on kiistanalainen. Esimerkiksi yritysmaailma ei ole kauttaaltaan hyvin suojattu, vaan on valtava määrä järjestelmiä, joissa ei ole varauduttu siihen, että joku hyökkäisi verkon kautta. Yleisesti ajatellaan, että Suomi on yksi maailman rehellisimpiä maita. Toisaalta on selvää, että rikkomuksia on ollut, mutta ne eivät ole tulleet esille.

Hyväksyttävää kyberturvatoimintaa on sidosryhmien mukaan se, että valtionhallinnon organisaatioissa valvotaan organisaation omiin tietojärjestelmiin tulevaa tietoa. Tämä koskisi esimerkiksi vain yksittäistä virastoa selvästi rajattuine toimipisteineen. Toimenpiteistä mainittiin esimerkkinä palomuurit, turvallisten ohjelmistojen hankkiminen ja organisaation päivittäisen toiminnan sisäiset tietoturvakäytännöt. Kaikki tämä on mahdollista jo nykyisen lainsäädännön nojalla.

Kuulemisissa korostettiin myös sitä, että yritysten tulee itse huolehtia tietoturvansa tasosta, viranomaisten resurssit eivät tähän riitä. Kaikkien on varauduttava kyberuhkiin. Yksittäiset toimijat voivat ehkä parhaiten havaita epämääräisen toiminnan verkkoliikenteessään.

Asiantuntijoiden mielestä valtiolla täytyy olla mahdollisuus aktiiviseen puolustautumiseen kyberhyökkäyksiä vastaan huoltovarmuuden ja muiden ydintoimintojen suojaamiseksi. Kyberpuolustustoimintaa suunniteltaessa tulisi kuitenkin ymmärtää, että kyberturvallisuustoiminta, joka voimakkaasti korostaa reaktiivista hyökkäyksen havaitsemista ja sen aktiivista rajoittamista, on riskialttiimpi perusoikeuksien toteutumisen kannalta kuin ennaltaehkäisevä ja järjestelmien hyökkäyskestävyyttä korostava strategia.

Reaktiivinen hyökkäysten havaitseminen ja verkkotiedustelu edellyttävät reaaliaikaista tietoliikenteen seurantaa ja profilointia. Proaktiivinen järjestelmien hyökkäyskestävyyden lisääminen taas keskittyy järjestelmien parantamiseen niitä kehitettäessä, jolloin järjestelmien lisääntynyt tietoturva samalla lisää myös niiden tietosuojaa.

Reaktiivinen havainnointi ja aktiiviset vastatoimet eivät välttämättä todellisessa konfliktitilanteessa auta, sillä hyökkääjä saattaa käyttää hyväksi nollapäivähaavoittuvuuksia, joita joko ei havaita tai joiden vaikutukset ovat liian nopeita, että niihin ehdittäisiin edes automaattisesti adaptoituvin keinoin pureutua. Erilaiset valvonta- ja torjuntajärjestelmät ovat kuitenkin tietoturvatuoteyritysten yritystoimintaa. Niitä edistävä lobbaus on siksi kiihkeämpää kuin ohjelmistojen turvallisen kehityksen edistäminen, joka ei välttämättä vaatisi suuria sijoituksia järjestelmiin mutta sitäkin enemmän koulutus- ja prosessi-investointeja.

Proaktiivinen turvallisuustyö, esimerkiksi uusimman VAHTI-sovelluskehitysturvallisuusohjeen (1/2013) vaatimusten mukainen työ, tehostaisi järjestelmien passiivista puolustettavuutta ja vähentäisi nollapäivähyökkäysten riskiä. Ohjelmistojen kehityksen ja sovelluskehityksen turvallisuuden nostaminen strategisesti suurempaan rooliin hyödyttäisi siis todennäköisesti sekä perusoikeuksien että paremman kyberturvallisuustilanteen toteutumista.

Tarvetta olisi myös parantaa tietoturvaloukkauksiin liittyvää viranomaisten välillä tapahtuvaa tiedonvaihtoa. Lisäksi viranomaisten tulisi pystyä kertomaan yrityksille ja yksityishenkilöille

millaisia hyökkäyksiä on käynnissä, jotta niiltä voidaan suojautua. Samalla pitäisi tapausten vakavuuden mukaan velvoittaa hyökkäysten uhreja raportoimaan heihin kohdistuneista hyökkäyksistä ja niiden tekniikoista, jotta muut voivat niiltä suojautua.

HAVARO-järjestelmästä todettiin, että se on toiminnassa ja osoittanut käyttökelpoisuutensa. Järjestelmää voitaneen asiantuntijoiden mukaan kehittää tarkemmin tiedustelutiedon tarpeisiin sopivaksi. Järjestelmän käyttöönottoa laajasti julkishallinnossa tulisi edistää. HAVARO-järjestelmän tai kaupallisesti saatavilla olevien monitorointijärjestelmien avulla tiedustelu on mahdollista kohdistaa siten, että sen piiriin ei aiheettomasti päädy sellaista viestintää, jolla ei ole itseisarvoa tai se on ristiriidassa yhteiskunnan yleisen oikeustajun kanssa. Tiedustelun kohdistaminen myös mahdollistaa kustannuskontrollin hyvinkin tarkasti ja optimaalisesti.

HAVARO-palveluita tullaan Huoltovarmuuskeskuksen mukaan jatkamaan ja vahvistamaan osana Kyberturvallisuuskeskuksen toimintaa. CERT-FI- ja HAVARO-palvelut laajenevat kattamaan myös valtionhallinnon yhteiset ICT-palvelut.

5.4 Suomi tiedon turvasatamana

Kuulemisissa korostettiin, että digitaalisessa maailmassa Suomi voi toimia kyberturvallisuuden luottamuksen takaajana. Tärkeä kansallinen visio on erottautua tulevaisuuden tietoliikenteen solmukohtana, ”Data-Sveitsinä”, joka käsittelee kansainvälistä tietoliikennettä suurella luottamuksella ja jonne voidaan turvallisesti taltioida tietoa. Suomessa on paljon teknologiaa, jonka hyödyntäminen tämän vision toteuttamisessa on mahdollista.

Maailman luottamuspula nykyisiin toimijoihin on avannut markkinatyhjiön, jossa Suomella on rajattomasti kasvumahdollisuuksia. Mahdollisuutta tukee myös suunnitellut merikaapelihankkeet, joiden keskeinen tarkoitus on mahdollistaa tietointensiivisen teollisuuden sijoittuminen Suomeen.

Maailmalla toteutunut kehitys on luonut Suomelle mahdollisuuden toimia kybermaailman oikeusvaltiona. Toimimalla oikeudenmukaisesti sekä puolustamalla yksityishenkilöiden ja yritysten oikeuksia ja riippumattomuutta Suomi voi erottautua älykkääksi digitaaliseksi yhteiskunnaksi ja maailman johtavaksi turvallisen teknologian ja yrittäjyyden keskittymäksi.

Työryhmän työssä on pystyttävä välttämään tilanne, jossa Suomea markkinoidaan turvallisena, vakaana, ennakoitavana ympäristönä, ja sijoituspäätösten tultua tehdyiksi, Suomessa otettaisiin käyttöön sellaisia menettelyjä, joiden välttämiseksi kilpailijamaamme aikanaan vaille investointeja.

Kuulemisissa pohdittiin kuitenkin myös sitä, tarkoittaako ”Suomi turvasatamana” sitä, että Suomessa ollaan turvassa viranomaisilta, joilla ei tällä hetkellä ole riittäviä toimivaltuuksia. Myös tarkoin säännelty verkkovalvonta voi olla kilpailuvaltti.

5.5 Vaikutuksista yritystoimintaan

Asiantuntijat korostivat sitä, että viranomaisten uudet toimivaltuudet tiedonhankintaan vaikuttaisivat eri yrityksissä käytännössä eri tavoin. Yrityksiä ei pidä niputtaa yhteen. Kustannusvaikutuksia tulee eritoten teleoperaattoreille.

Kustannukset ratkaisevat investoinneissa ja ne vaikuttavat suoraan siihen, minkä maan yritys valitsee toimipaikakseen. Koko maailma on nykyisin markkina-aluetta. Kustannukset tulisi selvittää etukäteen mahdollisimman tarkasti ja päättää siitä, kuka niistä vastaa.

On huomattava, että tiedonhankintatoiminta kohdistuisi yksityiseen omaisuuteen. Yrityksiltä tulisi saada suostumus toimintaan. Tiedonhankinta ei ole teleyritysten elinkeinotoimintaa. Toimialan ei tule kantaa sen kustannuksia eikä juridista tai moraalista vastuuta.

Tietoturvayritysten asiakaslupaus on ”we will proctect you” ja se perustuu luottamukseen siitä, että kyseiset yritykset pyrkivät takaamaan viestinnän luottamuksellisuuden. Voidaan nähdä, että viranomaisten tiedonhankintatoimivaltuudet vaarantavat tämän luottamuksen.

Paitsi suorat vaikutukset, on otettava huomioon myös mielikuvat, joiden perusteella kuluttajat ja yritykset valitsevat palvelunsa. Riski Suomen maineelle on tiedostettava. Ei saa tulla käsitystä, että kaikkea valvotaan, kun tällaista ei olla esittämässä.

Toisaalta tuotiin esille, että ennustettavuus on tärkeää investoijille. Suomi on ollut turvallinen ja Suomella on imagoarvoa, jota pitää varjella.

Sekä Suomessa että Ruotsissa toimivien teleyritysten edustajat totesivat oman yrityksensä puolesta, että Ruotsin FRA-laki ei ole vaikuttanut käytännön toimintaan mitenkään.

5.6 Viranomaisten toimivaltuustarpeista

Saatujen kommenttien mukaan Suomesta ulospäin suuntautuvan rikolliseen toimintaan liittyvän verkkoliikenteen kohdennettua seurantaa tulisi lisätä. Todettiin, että nykylainsäädännössä kyseessä olevan liikenteen haravointi ei ole mahdollista, vaan kaikkia tapauksia käsitellään yksittäisinä. Esimerkiksi verkkorikollisten ja valtiollisten toimijoiden käyttämien haittaohjelmien ja muiden tekniikoiden käyttäytyminen usein perustuu aktiivisiin tietoliikenneyhteyksiin maan rajojen ulkopuolelle. Kyseiseen toimintaan liittyvä verkkoliikenne olisi teknisesti mahdollista havaita ja kohdentaa ilman, että itse liikenteen sisältöä tai koko Suomen sisäistä verkkoliikennettä on tarvetta seurata.

Läpinäkyvä viranomaistoiminta nähtiin erittäin tärkeäksi, ja se kuuluu myös suomalaiseen kulttuuriin. Kaikkien tietoon on tuotava rehellisesti, mitä viranomaiset tekevät. Todettiin myös, että suomalaisten viranomaisten toiminta ulkomailla ei todennäköisesti ole ohjelmantarjoajien näkökulmasta ongelmallista.

Suomessa on jo nyt laajat telepakkokeinot ja lainsäädäntö on olemassa, niitä ei ehkä hyödynnetä riittävästi.

Jos viranomaisen tiedonhankinnasta luodaan uutta sääntelyä, viranomaisten tiedonhankintaa koskevien tehtävien ja toimivaltuuksien tulee olla yksilöityjä ja riittävän tarkkarajaisia. Tiedonhankinnalle tulee olla selkeä laillinen perusta.

Lainsäädännössä pitäisi myös määritellä, mikä liikenne on haitallista. Ylipäätään mahdollisen lainsäädännön tulee olla tarkkaa. Nähtiin, että tässä Suomi voi erottua muista maista. Laista on voitava lukea, mitä viranomaiset saavat tai eivät saa tehdä, tästä syntyy luottamus viranomaisten toimintaan. Myös tiedon jakaminen ja käyttötarkoitus on rajattava riittävästi.

Riittävän tarkka sääntely edellyttää myös kybertoimintaympäristön määrittelyä sekä tavoitteiden asettamista. Tavoitteiden asettamisen tulee perustua siihen, mitä päätöksentekoa ja toimintaa tiedustelutoiminnan on tarkoitus tukea, ketkä ovat osallistuvat tahot turvallisuusviranomaisten lisäksi ja mitkä ovat velvoitteet ja rasitteet kustannuksineen.

Viranomaisten voimavarat tuotiin myös esille. Ruotsin FRA:n budjetti on 100 miljoonaa euroa ja siellä on töissä 300 henkilöä. Hankkeen tehokkuudesta tulee vakuuttua ennen kuin se voidaan toteuttaa. Valvontaa on kuitenkin tällä hetkellä jo monessa maassa Suomen ympärilläkin.

Jouduttaneen pohtimaan sitäkin vaihtoehtoa, että viranomaisen tehtävänä ei olisikaan toimia varsinaisena palvelujen tuottajana vaan viranomaisen tehtävä muodostuisi yhteistoiminnan puitteiden luomisesta ja erilaisen tiedon välittämisestä osapuolten välillä.

5.7 Massavalvonta

Massavalvonnasta esiintyy erilaisia näkemyksiä. Kuulemisissa tuli esille se, että massavalvontana pidetään myös sitä, että tiedonhankintaa tehdään tarkoin hakuehdoin kaikesta tietoliikenteestä. Vaikka hakuehtojen ulkopuoliseen tietoon ei mentäisikään, kyse on massavalvonnasta, koska valvonta on kohdentamatonta. Esitettiin myös, että EU-tuomioistuimen data retention –ratkaisun jälkeen massavalvonta ei EU-maassa ole enää mahdollista.

Massavalvontaa ei voida määritellä viranomaispäätöksin. ”Haravointi” -käsite ymmärretään massavalvonnaksi. Viranomaisen valvottavana olisi kaikki se, mistä tieto hankitaan.

Suhteellisuus nähtiin tärkeäksi asiaksi. Olisi löydettävä tasapaino on sille, kuinka laajasti voidaan valvontaa tehdä. Kaikenkattava seuranta ei ole yleisesti hyväksyttävää.

Tietojen massakerääminen ei kuultujen asiantuntijoiden mukaan tosiasiallisesti auta kyberuhkien torjunnassa, vaan on reaktiivinen tapa, jossa ongelma huomataan vasta, kun uhka on jo toteutunut ja esimerkiksi kuluttajan laitteeseen tai viranomaisen verkkoon on jo tunkeuduttu.

5.8 Takaportit ja salauksenpurkuavaimet

Takaporttimahdollisuutta eli sitä, että viranomainen pääsee käyttäjän tietämättä tietokoneeseen, ohjelmistoon tai vastaavaan, pidettiin ongelmallisena ja tuotiin esille, että sen poissulkeminen viranomaisten keinovalikoimasta on kannatettavaa. Samoin pidettiin tärkeänä, että yrityksille ei tule velvollisuutta luoda takaportteja ja luovuttaa viranomaisille avaimia, jolla viestien salauksia voidaan purkaa. Molemmat mahdollisuudet vaikeuttaisivat asiantuntijoiden mukaan yritystoimintaa merkittävästi, kun kuluttajien luottamus yritysten tuotteisiin vaarantuisi.

5.9 Yksityisyyden suoja, luottamuksellisen viestinnän suoja ja lähdesuoja

Yksityisyyden suoja on keskeinen oikeus, kun arvioidaan viranomaisten tiedonhankintaoikeuksia. On myös huomattava, että tästä huolimatta ihmiset luovuttavat internetissä yrityksille erittäin paljon tietoa itsestään, esimerkiksi sosiaalisessa mediassa.

Yksityisyyden suojasta järjestöt totesivat myös, että yksityisyys on perusarvo; valtio ei saa kerätä tietoja, jos ihminen on nuhteeton ja toimii moitteettomasti. Tietoa ei saa kerätä, vaikka sitä ei analysoida tai tarkastellakaan. Jo tiedon keräämisellä loukataan yksityisyyttä.

Asiantuntijat toivat esille, että merkityksellisiä ovat Euroopan unionin perusoikeuskirjan 7 artikla (Yksityis- ja perhe-elämän kunnioittaminen) ja 8 artikla (Henkilötietojen suoja).

Kuulemisissa todettiin, että viestintäpalveluiden käyttäjien luottamusta viestinnän luottamuksellisuuteen ei saa heikentää ilman erityisen painavia perusteluja. Mahdollinen verkkotiedustelu (tarkoitettaneen tietoliikennetiedustelua) olisi merkittävä muutos suomalaiseen oikeusjärjestykseen ja se saattaisi murentaa käyttäjien luottamusta suomalaisten toimijoiden tarjoamiin viestintä- ja muihin palveluihin.

Kuulemissa esitettiin kannanottoja siitä, että tiedonhankinnassa ei tulisi olla mahdollisuutta journalistisen lähdesuojan murtamiseen. Lähdesuojassa painottuu luottamus, joka ei saa vaarantua.

Luottamuksellisen viestin salaisuuden suojaa koskevan perustuslakivaliokunnan vakiintuneen tulkintakäytännön soveltaminen tiedusteluun on vaikeaa. On otettava huomioon poikkeuslakien välttämisen doktriini. Jos tavoitteena on pysyvän järjestelyn luominen, poikkeuslakimenettely ei riittäisi vaan perustuslain 10 §:n 3 momentin sanamuotoa olisi arvioitava uudelleen. Tulkinnallisesti ei sanamuotoa voida laajentaa tiedusteluun.

Perusoikeuden rajoitukselle on oltava aina hyväksyttävä peruste. Esimerkiksi perustuslain 10 §:n 3 momentissa edellytetään konkreettista rikosepäilyä.

Tietoliikennetiedustelun rinnastamista oikeudellisesti toimenpiteisiin, jotka ovat mahdollisia tietoturvan toteuttamiseksi, ei nähty toimivaksi.

5.10 Vaikutukset ulkopolitiikkaan ja maiden väliset suhteet

Asiantuntijakuulemisissa tuli esille, että tiedustelulla saadun arkaluontoisen ulkovaltoja koskevan tiedon säilytys ja salassapito kansallisesti sisältää poliittisen riskin. Viime aikojen kansainväliset tapahtumat osoittavat, että kansallisilla verkkotiedusteluratkaisuilla on laajoja ulkopoliittisia vaikutuksia.

Valtioiden väliset mahdolliset ristiriidat tulee ratkaista. Jotta lainsäädännön ristiriitaisuuksilta vältyttäisiin, valtioiden tulee rakentaa kestäviä periaatteita noudattava ja läpinäkyvyyttä edistävä kehikko rajat ylittävien tietopyyntöjen hallintaan esimerkiksi vahvistamalla olemassa olevia maiden välisiä virka-apusopimuksia.

Valtioiden tulee sopia keskenään menettelytavoista, joilla ratkaistaan eri maiden lainsäädäntöjen mahdollisista ristiriitaisuuksista aiheutuvat ongelmat.

5.11 Lupa viranomaisten tiedonhankinnalle ja viranomaisten toiminnan valvonta

Työryhmän kuulemat asiantuntijat toivat esille, että toiminnalle oltava mandaatti laissa ja että toimeenpanon tulee olla luvanvaraista.

Tiedonhankinnan olisi perustuttava hyväksyttäviin kriteereihin ja koko yhteiskunnan olisi osallistuttava niiden arviointiin (parlamentaarisuus).

Asiantuntijat ovat todenneet, että viranomaisten toimintaa tulee myös tarkoin valvoa. Mitä enemmän toimivaltuuksia, sitä tehokkaampi valvonta. Valvonnan on oltava riippumatonta. Järjestelmän tulisi olla läpinäkyvä ja kontrolloitu sekä luottamusta herättävä. On myös järjestettävä riittävä neuvontaprosessi.

Mahdolliset toimeenpanovirheet on sanktioitava. Olisi myös luotava korvausvelvollisuus vahingosta. Koska toimintaa tehdään salassa, asianosaisille on luotava mahdollisuus puolustautua, jos henkilö kokee joutuneensa epäasiallisen tiedonhankinnan kohteeksi. Asianosaisella ei voi olla tietoa, vaan todistustaakka tulee asettaa tietoa hankkivalle viranomaiselle.

Todettiin myös, että jos työryhmä päätyy esittämään tiedonsaantioikeuksien laventamista, työryhmä täydentää tarkastelun piiriin kuuluvia asioita myös tiedonhankintaan liittyvien käytänteiden valvontamekanismien laatimisella. Tiedonhankinnalle on luotava tehokas ja kattava valvontajärjestelmä, johon kuuluu myös julkisuuskontrolli.

Viranomaisia avustaneilla tahoilla tulee olla oikeus julkistaa yleisen tason tietoja (esim. tilastoja) siitä, miten ne ovat avustaneet viranomaisia. Viimeksi mainittu on tärkeää erityisesti yritysten oikeusturvan kannalta. Myös Suomen kansalaisten tulee saada tietää, miten paljon verkkoseurantaa maassamme tehdään, ja minkälaisia tuloksia sillä saavutetaan.

Suomeen tulee myös luoda toimintamalli, jossa viranomaisen toimista rikosten ehkäisyssä ja selvittämisessä jää aina todisteet. Niiden avulla voidaan osoittaa, että ylilyöntejä ei ole ta-

pahtunut tai muutoin toimita vastoin yhteisiä päätöksiä. Näin toimimalla Suomi voi saavuttaa laajan kansainvälisen luottamuksen kyberturvallisena maana, jonne kannattaa investoida ja varastoida tietoa turvallisesti. On tärkeää kyetä esittämään jälkikäteen seurannan kohteeksi joutuneelle, mitä tietoja heistä on kerätty ja mihin niitä on toimitettu. Näin vältytään myös pitkäkestoisilta väärinkäytöksiltä ja taataan poikkeuksellinen tilaisuus luoda Suomesta todellinen Data-Sveitsi.

Asian luonteesta johtuen toimintaa valvovien toimielimien tulee olla itsenäisiä ja riippumattomia. Valvonnan kohteilla ja tietopyyntöjen vastaanottajilla tulee olla mahdollisuus valittaa päätöksistä.

Viranomaisten ja valvontaelinten keskeiset päätökset tulee julkistaa viivytyksettä, jotta kansalaisvalvonta olisi mahdollista.

Todettiin, että raportointi toiminnasta on tärkeää. Esimerkiksi Google julkaisee, mitä tietopyyntöjä sille on tullut. On välttämätöntä, että yritykset saavat julkaista raportteja jatkossakin. Myös viranomaisten on tarkasti raportoitava toiminnastaan ja esitettävä julkisia tilastoja. Viranomaisilla on velvollisuus julkaista tietopyyntöjen kokonaismäärä, tämä mahdollistaa aidon kansalaiskeskustelun.

5.12 Yhteenveto

Yleisesti ottaen työryhmän kuulemat asiantuntijat pitivät hyvänä, että Suomen kansallista kyberturvallisuutta kehitetään esimerkiksi selvittämällä nykyistä sääntelyä, kartoittamalla turvallisuusviranomaisten tarpeita ja ottamalla huomioon kansalaisten perusoikeudet. Lähes kaikessa saadussa palautteessa korostettiin kehittämisehdotusten vaikutusten huolellisen arvioinnin tärkeyttä.
Saadussa palautteessa kiinnitettiin paljon huomiota tietoturvallisuuteen ja sen kehittämiseen. Kyberuhkien ennaltaehkäisyn kannalta niin julkisten kuin yksityistenkin toimijoiden on tärkeää huolehtia omien verkkojensa tietoturvasta muun muassa teknisin keinoin. Viranomaisten ja toimialan keskeisten toimijoiden tiedonvaihtoa olisi kehitettävä.

Kuulemisissa otettiin kantaa lähinnä verkkovalvontaan. Tietojen niin sanottua massavalvontaa ja ohjelmistoihin rakennettavia takaportteja vastustettiin yleisesti. Turvallisuuden suojaamiseksi nähtiin kuitenkin oikeutetuksi suorittaa perusteltuja, tarkasti kohdennettuja, tilannekohtaisia toimenpiteitä kyberympäristössä.

Sidosryhmät toivat esille, että viestintäpalveluiden käyttäjien luottamusta viestinnän luottamuksellisuuteen ei saa heikentää ilman erityisen painavia perusteluja. Verkkotiedustelu saattaisi murentaa käyttäjien luottamusta suomalaisten toimijoiden tarjoamiin viestintä- ja muihin palveluihin. Toisaalta tunnistettiin, että kansallisen turvallisuuden takaamiseksi viranomaisilla tulisi olla edellytykset torjua rikollisuutta ja terrorismin uhkaa yksilön oikeuksia ja viestintäsalaisuutta kunnioittaen.

Huomioissa tuotiin esille perusoikeuksiin liittyviä näkökohtia, kuten yksityisyyden suoja ja oikeus tietoon, luottamuksellinen viestintä, elinkeinonvapaus, omaisuuden suoja ja sananvapaus.

Erityisesti oltiin huolissaan yritysten kilpailukyvystä ja Suomen maineesta tiedon turvasatamana sekä työryhmän ehdotusten vaikutuksista yritystoimintaan ja Suomeen suuntautuviin investointeihin.

Suomen maine yksityisyyden suojaa kunnioittavana maana on yksi Suomen IT-teollisuuden kilpailueduista, joka halutaan säilyttää. Suomalaisten yritysten houkuttelevuutta investointikohteena ei tulisi vahingoittaa.

Esitetyissä huomioissa korostettiin turvallisuusviranomaisten toiminnan valvontaa ja mahdollisimman suurta avoimuutta. Tiedonhankinnalle olisi luotava tehokas ja kattava valvontajärjestelmä.

Kansalaisten tulisi saada tietää, miten paljon verkkoseurantaa tehdään ja minkälaisia tuloksia sillä saavutetaan. Yritysten tulisi myös pystyä julkisesti kertomaan niihin kohdistetuista tietopyynnöistä.

Sidosryhmien edustajat kiinnittivät huomiota siihen, että kyberturvallisuuden parantaminen edellyttää yhteistyötä viranomaisten ja yksityissektorin toimijoiden välillä. Kaikkien panostusta tarvitaan.

Liikenne- ja viestintäministeriö

15.12.2014

Digitaalisen yhteiskunnan tulevaisuus

Liikenne- ja viestintäministeriön edustajan eriävä mielipide tiedonhankintalakityöryhmän mietintöön

Liikenne- ja viestintäministeriön edustaja (myöh. liikenne- ja viestintäministeriö) ei voi tällä hetkellä saatavilla olevien tietojen perusteella suosittaa verkkovalvonnan mahdollistavan lainsäädännön valmistelua.

Eriävällä mielipiteellä ministeriö haluaa tarjota vaihtoehtoisen tavan hahmottaa digitaalista toimintaympäristöä. Mielipiteessä ministeriö esittää näkökulmia, joita ei ole huomioitu riittävästi tiedonhankintalakityöryhmän mietinnössä (myöh. mietintö). Lisäksi eriävällä mielipiteellä on tarkoitus mahdollistaa laajemman yhteiskuntapoliittisen keskustelun käyminen mietinnössä käsitellyistä aiheista ja erityisesti verkkovalvonnasta.

I. Ydinviestit

1. Tietoliikennetiedustelu on verkkovalvontaa.
   - Mietinnössä esitetty tietoliikennetiedustelu on verkkovalvontaa. Verkkovalvonnasta käytettään myös nimitystä massavalvonta, sillä siinä on kyse teknisestä pääsystä kaikkeen tietoliikenteeseen.
   - Verkkovalvonta kohdistuisi käytännössä kaikkeen tietoliikenteeseen, ei pelkästään kansainväliseen. Vaikka verkkovalvonnassa pyrittäisiinkin erottamaan kotimainen ja ulkomainen tietoliikenne, niin tiedustelu kohdistuu tosiasiassa myös suomalaisten viestintään.

2. Viranomaisille voidaan antaa vain toimivaltuuksia, jotka perustuvat niiden lakisääteisiin tehtäviin.
   - Tiedonhankintatoimivaltuudet ovat hyväksyttäviä vain, jos ne ovat välttämätön ja tehokas keino jonkin viranomaiselle säädetyn tehtävän hoitamiseksi.

3. Verkkovalvonnan tehokkuutta ei ole osoitettu, eikä vaihtoehtoja arvioitu.
   - Verkkovalvonta ei tuota tulevaisuudessa tietoa, jota sillä on ehkä aikaisemmin voitu saada.
   - Salaustekniikoiden kehittyminen ja käytön lisääntyminen sekä tietoliikenteen määrän kasvu vaikeuttavat verkkovalvontaa huomattavasti. Olennaisen tiedon löytäminen ja salauksen purkaminen vaativat merkittäviä resursseja, joita Suomella ei ole.
   - Työryhmätyöskentelyn tarkoituksena on näyttänyt olevan jo ennalta päätettyjen asioiden perusteleminen. Vaihtoehtoja työryhmän ehdottamalle verkkovalvonnalle ei ole esitetty.

4. Verkkovalvonnalla voi olla merkittäviä vaikutuksia yritystoimintaan.
   - Yritysvaikutukset vaikutukset on arvioitava huolellisesti. Verkkovalvonta vaikuttaa eri tavalla erityyppisiin yrityksiin.

- Verkkovalvonnalla voi olla vaikutuksia yritysten sijoittautumispäätöksiin, erityisesti tiedon hyödyntämiseen perustuvassa liiketoiminnassa.
- Suomi voisi käyttää kilpailuetunaan sitä, ettei täällä suoriteta verkkovalvontaa.

5. Verkkovalvonnalla rajoitetaan perusoikeuksia, erityisesti oikeutta yksityisyyteen.
   - Verkkovalvontatoimivaltuuksista säätäminen edellyttää perustuslain muuttamista.
   - Perustuslakia voidaan joutua muuttamaan, vaikka verkkovalvonta keskittyisi vain tunnistamistietoihin.

6. Verkkovalvonta ei parantaisi tietoturvaa, vaan heikentäisi sitä.
   - Verkkovalvonta tarkoittaisi käytännössä sitä, että tiedonhankinnan kohteeksi valikoidun viestinnän suojaukset yritettäisiin ohittaa tai murtaa.
   - Verkkovalvonta heikentäisi kaikkien niiden henkilöiden tietoturvallisuutta, joiden viestejä välitettäisiin niissä yleisissä viestintäverkoissa, joissa verkkovalvontaa suoritettaisiin.
   - Verkkovalvonta ei parantaisi yritysten tietoturvaa.

II. Johdanto

Tiedonhankintalakityöryhmä aloitti työskentelynsä tammikuussa 2014. Alun perin hallituksen esityksen muotoon kaavaillusta loppuraportista kasvoi noin 100-sivuinen mietintö. Mietinnössä kuvataan muuttuvaa turvallisuusympäristöä ja tiedonhankintatoimivaltuuksien nykytilaa. Tämän jälkeen mietinnössä vertaillaan eri maiden lainsäädäntöä ja esitetään lainsäädännön kehittämisehdotuksia. Työryhmä ehdottaa mietinnön johtopäätöksissä, että käynnistettäisiin tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi. Käytännössä tämä tarkoittaa lainsäädännön valmistelua.

Mietinnössä käsitellään kahta tiedustelukokonaisuutta: 1) tietoliikennetiedustelua ja 2) ulkomaan tiedustelua, joista jälkimmäinen jakaantuu henkilö- ja tietojärjestelmätiedusteluun. *Tietoliikennetiedustelulla* tarkoitetaan Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua. *Ulkomaan tietojärjestelmätiedustelulla* tarkoitetaan ulkomailla sijaitsevassa tietojärjestelmässä käsiteltäviin tietoihin kohdistuvaa tietoteknisin menetelmin tapahtuvaa tiedustelua. *Ulkomaan henkilötiedustelulla* tarkoitetaan ulkomaita koskevaa tiedustelua, joka perustuu henkilökohtaiseen kanssakäymiseen taikka henkilön tai muun kohteen henkilökohtaiseen havainnointiin. Tietoliikennetiedustelu ja ulkomaan tietojärjestelmätiedustelu menevät käsitteinä helposti sekaisin. Tässä eriävässä mielipiteessä käytetään tietoliikennetiedustelusta vastedes käsitettä verkkovalvonta.

Liikenne- ja viestintäministeriö katsoo, ettei se voi yhtyä tiedonhankintalakityöryhmän mietintöön kokonaisuudessaan. Tiedonhankintalakityöryhmä suosittelee mietinnössään, että Suomen tulisi harkita verkkovalvonnan käyttöönottoa. Liikenne- ja viestintäministeriö ei voi yhtyä tähän näkemykseen. Ministeriö ei kuitenkaan sulje pois mahdollisuutta muuttaa näkemystään verkkovalvonnasta, jos myöhemmin laadittava selvitys osoittaa sen tehokkaaksi tarkoitukseensa nähden sekä edut oletettua suuremmiksi ja haitat pienemmiksi. Näin ei toistaiseksi ole tapahtunut.

Liikenne- ja viestintäministeriö ymmärtää ja hyväksyy puolustusvoimien ja poliisin esittämät huolet siitä, etteivät ne kaikilta osin saa päätöksentekonsa tueksi tarpeeksi tietoa sotilaalliseen maanpuolustukseen tai rikoksiin liittyvistä uhkista. **Tällä hetkellä käytettävissä olevan tie-**

tämyksen perusteella mietinnössä suositeltu verkkovalvonta vaikuttaa kuitenkin olevan tarkoituksiinsa nähden tehoton ja haitallinen luottamuksellisen viestinnän suojalle ja elinkeinoelämälle.

Muilta osin liikenne- ja viestintäministeriö näkee, että puolustusvoimien tiedustelukyvyn kehittäminen on tärkeää. Ministeriö katsoo, että tulisi ryhtyä lainsäädännön valmisteluun sen varmistamiseksi, että puolustusvoimilla olisi perusteltu kyky ja selkeä toimivalta hankkia tehokkaasti sotilaallisen maanpuolustuksen kannalta keskeistä tietoa Suomen rajojen ulkopuolella sijaitsevista järjestelmistä. **Liikenne- ja viestintäministeriö pitää siten mietinnössä kaavailtua ulkomaille kohdistuvaa henkilö- ja tietojärjestelmätiedustelua perusteltuna.**

Poliisilla on ministeriön näkemyksen mukaan kattavat mahdollisuudet saada rikoksiin liittyvää tietoa Suomessa sijaitsevista tietojärjestelmistä poliisi- ja pakkokeinolain mukaisessa menettelyssä. **Jos poliisin valtuudet todetaan digitalisoituneessa ympäristössä riittämättömiksi, liikenne- ja viestintäministeriö pitää perusteltuna, että näiden salaisten pakkokeinojen nykyistä alueellista soveltamisalaa tai käytön edellytyksiä arvioidaan uudelleen.**

Työryhmän toimikauden aikana on ollut havaittavissa vastakkainasettelua liikenne- ja viestintäministeriön ja turvallisuusviranomaisten välillä. Liikenne- ja viestintäministeriö haluaa korostaa, ettei se kiistä tiedonsaantitarpeiden oikeellisuutta tai tärkeyttä yhteiskunnallisesti. Ministeriö on kuitenkin painokkaasti tuonut esille, että tiedonsaantitarpeet tulee esittää selkeästi ja perustella viranomaisten lakisääteisten tehtävien kautta. Tämän jälkeen keinot, joilla näihin tarpeisiin voitaisiin vastata, tulee eritellä, osoittaa niiden tehokkuus tarkoitukseensa nähden ja arvioida kaikki niiden vaikutukset.

Työryhmän työn suurin heikkous on ollut se, että se on keskittynyt työnsä alusta asti perustelemaan verkkovalvonnan käyttöönottoa. Työryhmä ei kuitenkaan ole pystynyt tyydyttävällä tavalla perustelemaan verkkovalvonnan tehokkuutta, eikä kuvaamaan sen vaikutuksia. Myöskään vaihtoehtoisiin tiedonhankintatapoihin ei ole perehdytty riittävästi.

Kuten tiedonhankintalakityöryhmän mietinnössä todetaan, ei puolustusvoimien tiedustelutoiminnasta säädetä tällä hetkellä laissa. Tästä huolimatta työryhmän asettamiskirje ja työryhmän tavoitteet on muotoiltu keskittymään vain niin sanottuun ”kybertoimintaympäristöön”.[1] Liikenne- ja viestintäministeriön näkemyksen mukaan työryhmän olisi tullut keskittyä vielä kokonaisvaltaisemmin tiedustelua koskevan lainsäädännön kehittämistarpeisiin, sillä yleislainsäädäntö tulisi lähtökohtaisesti säätää ennen erityislainsäädäntöä. Mahdollisessa seuraavassa vaiheessa tulisikin pohtia puolustusvoimien tiedustelua koskevan lainsäädännön laatimista, eikä keskittyä pelkästään tietoverkossa käytettäviin toimivaltuuksiin.

Työryhmän työskentely on ollut intensiivistä ja kokouksia on järjestetty noin kerran viikossa. Liikenne- ja viestintäministeriö on tiukasta aikataulusta huolimatta pyrkinyt parhaansa mukaan edistämään työryhmän työtä ja tarjoamaan omaa viestintäpolitiikkaan ja sähköiseen viestintään liittyvää osaamistaan työryhmän käyttöön. **Liikenne- ja viestintäministeriön esittämiä näkökulmia on otettu osaksi mietintötekstiä vasta työryhmän lopussa eikä silloinkaan sisällöllisesti merkityksellisellä tavalla.** Tämä ei ole riittänyt ministeriön ydinviestien huomioon ottamiseksi.

[1] Etuliitteen ”kyber” yksiselitteinen määritteleminen on haastavaa, mutta kybertoimintaympäristöllä viitataan yleisesti digitaalisen toimintaympäristöön, eli esimerkiksi toimintaan tietoverkoissa.

Eriävänä mielipide on laadittu liikenne- ja viestintäministeriön ydinviestien ympärille. Jokainen ydinviesti perustellaan omassa luvussaan. Viimeisessä luvussa kerrataan aiempia toimia, joita on tehty tietoturvan parantamiseksi sekä esitellään näkemyksiä internetin luotettavuuden kehittämiseksi. **Liikenne- ja viestintäministeriön eriävä mielipide keskittyy pääosin verkkovalvontaa koskevaan mietinnön osaan.**

Seuraavassa luvussa kuvataan, miten internetin massavalvontaa koskevat paljastukset ovat vaikuttaneet kansainväliseen keskusteluun. Lisäksi luvussa tarkastellaan internetin taloudelliseen hyödyntämiseen liittyvää kehitystä.

III. Toimintaympäristö

Mietinnössä on varsin laajasti kuvattu muuttuvaa turvallisuusympäristöä ja muun muassa kansalliseen turvallisuuteen kohdistuvia tietoverkkouhkia sekä tietoverkkorikollisuutta. Toimintaympäristön kuvaus on mietinnössä erittäin uhkakeskeinen. **Liikenne- ja viestintäministeriön näkemyksen mukaan mietinnössä olisi kuitenkin tullut kuvata laajemmin tiedusteluun liittyvää kansainvälistä ilmapiiriä ja internetin kehitystä sekä niiden vaikutuksia erityisesti verkkovalvonnan tehokkuuteen.**

Mietinnössä ei kuvata sitä muutosta, joka yritysten ja kansalaisten asenneilmapiirissä on tapahtunut sen jälkeen, kun Edward Snowden kertoi kesällä 2013 julkisuuteen tietoja USA:n ja muiden maiden harjoittamasta tietoliikenteen massavalvonnasta. Itse asiassa koko tietovuotoa tai kansainvälistä keskustelua valtioiden harjoittamasta ylimitoitetuista valvonnasta ei ole tarkemmin käsitelty mietinnössä.[2]

Esimerkkeinä verkkovalvontaan liittyvistä kansainvälisistä kannanotoista voidaan mainita YK:ssa käytävä keskustelu yksityisyydestä digitaaliaikana. YK:n ihmisoikeusneuvostoon kuuluvat erityisraportoijat ovat käsitelleet oikeutta yksityisyyden suojaan ja uuden informaatioteknologian mukanaan tuomia ihmisoikeushaasteita useista näkökulmista. YK:n yleiskokous hyväksyi joulukuussa 2013 ilman äänestystä päätöslauselman oikeudesta yksityisyyteen digitaaliaikana (A/RES/68/167). Uuden aloitteen taustalla olivat Brasilia ja Saksa ja myös Suomi suhtautui siihen positiivisesti. Huomattavaa oikeudellista ja poliittista kiinnostusta herättäneellä päätöslauselmalla ilmaistaan huoli sähköisen valvonnan sekä digitaalisen viestinnän urkinnan ja henkilökohtaisten tietojen keräämisen kielteisistä vaikutuksista ihmisoikeuksiin. Päätöslauselmalla pyritään vahvistamaan oikeutta yksityisyyden suojaan. Ihmisoikeuksia tulee suojella yhtäläisesti myös sähköisessä viestinnässä. Kansallisen lainsäädännön tulee olla yhdenmukaista kansainvälisten ihmisoikeusvelvoitteiden kanssa.[3]

Toisena esimerkkinä voidaan mainita Euroopan parlamentin päätöslauselma Yhdysvaltojen kansallisen turvallisuusviraston valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa.[4] Euroopan parlamentin päätöslauselmaa tulisi peilata erityisesti tiedonhankintalakityöryhmän mietinnön kansainvälistä vertailua koskevaan osuuteen. Mietinnössä verrokki-

[2] Verkkovalvonnan vaikutusarvioinnissa on mainin ta ”Snowden-tapauksesta” ja siitä kuinka sen jälkeisissä olosuhteissa Ruotsin selkeä tiedustelulainsäädäntö saattaa olla jopa kansainvälinen kilpailuetu.
[3] Ks. http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx. Lisäksi YK:n ihmisoikeuskomissaari on antanut aiheesta raporttinsa ja suositukset (A/HRC/27/37), joita on käsitelty YK:n 69. yleiskokouksessa syyskuussa 2014.
[4] Euroopan parlamentin päätöslauselma 12. maaliskuuta 2014 Yhdysvaltojen kansallisen turvallisuusviraston valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa (2013/2188(INI)).

maiksi on valittu vain maita, jossa verkkovalvontaa harjoitetaan. Vertailua tarkasteltaessa tulisi esimerkiksi huomioida, että Euroopan parlamentti on suhtautunut varsin varauksellisesti muun muassa Ruotsin ja Alankomaiden tiedustelua koskevaan lainsäädäntöön ja katsonut, että kyseiset lainsäädännöt voivat olla ongelmallisia EU:n perusoikeuksien näkökulmasta. Euroopan parlamentti on kehottanut kaikkia EU:n jäsenvaltioita kieltämään kaikenkattavat laajamittaiset valvontatoimet ja lisäksi kehottanut kaikkia EU:n jäsenvaltioita ja etenkin Yhdistynyttä kuningaskuntaa, Ranskaa, Saksaa, Ruotsia, Alankomaita ja Puolaa varmistamaan, että niiden nykyiset tai tulevat tiedustelupalvelujen toimintaa koskevat lainsäädäntökehykset ja valvontamekanismit ovat Euroopan ihmisoikeussopimuksen määräysten ja EU:n tietosuojalainsäädännön mukaisia. Terrorismin torjunnan osalta Euroopan parlamentti toteaa uskovansa vahvasti, ettei terrorismin torjunta voi koskaan oikeuttaa kohdentamattomia, salaisia tai jopa laittomia laajamittaisen valvonnan ohjelmia. Euroopan parlamentti katsoo, että tällaiset ohjelmat ovat tarpeellisuus- ja suhteellisuusperiaatteiden vastaisia demokraattisessa yhteiskunnassa.

Snowdenin paljastusten jälkeen maailmalla on havahduttu pohtimaan sitä, mitä teknistyminen ja jokapäiväisen elämämme yhä suurempi riippuvuus sähköisistä palveluista tarkoittaa. Digitalisaatio ratkaisee monia ongelmia ja tehostaa toimintaamme. Samalla se kuitenkin synnyttää uusia haasteita. Internetin ja mobiiliteknologian hyödyntäminen mahdollistaa tietojen keräämisen ja ihmisten seuraamisen aivan uudella tavalla. Myös valtiot pystyvät hyödyntämään tätä kehitystä tiedustelutoiminnassaan.

Tilannetta, jossa Euroopan unionin jäsenmaat urkkivat toisten maiden kansalaisten ja yritysten tietoja, voidaan pitää esteenä Suomen tärkeänä pitämien digitaalisten sisämarkkinoiden synnylle. **Liikenne- ja viestintäministeriö katsoo, että verkkovalvontatoimivaltuuksien sijaan Suomen tulisi aktiivisesti edistää kansainvälistä yhteistyötä viestinnän luottamuksellisuuden säilymisen puolesta.** Esimerkiksi EU:ssa voitaisiin pyrkiä löytämään yhteinen lähestymistapa sille, minkälaisissa tilanteissa ja millä tavoin toisen jäsenvaltion alueella asuvan ja toimivan kansalaisen tai yrityksen viestinnän luottamuksellisuutta voidaan rajoittaa.

Laajasti katsottuna toimintaympäristön muutoksessa on kyse internetin hyödyntämisestä. Tiedon säilyttämisen kustannukset ovat pienentyneet ja tiedosta on entistä helpompi saada liiketoiminnallista hyötyä. Palveluiden ansaintalogiikat perustuvat yhä useammin tietojen keräämiseen, käyttöön ja myyntiin. Internet-talous ja digitaaliset palvelut ovat merkittäviä talouden kasvun katalyytteja.

Kaikki mikä voidaan digitalisoida, tullaan digitalisoimaan. Tämä vaikuttaa käytännössä kaikkiin yhteiskunnan osa-alueisiin. Myös julkishallinnon palvelut siirtyvät verkkoon. **Digitaalisuus on kaikkia yhteiskunnan sektoreita läpileikkaava teema ja kyky sen hyödyntämiseen tulee pitkälti määrittelemään kansakuntien asemaa globaalissa kilpailussa.** Tieto- ja viestintäteknologian on arvioitu olevan merkittävin Suomen talouskasvuun viidentoista viime vuoden aikana vaikuttanut yksittäinen tekijä.[5] Oikeilla tieto- ja viestintäteknologiaa koskevilla päätöksillä voidaan parantaa tuottavuutta ja nopeuttaa talouskasvua. Päätöksenteossa tulee huomioida, että toimivia ja kilpailukykyisiä digitaalisia palveluita ei nykypäivänä pystytä rakentamaan ilman luottamusta. Luottamusta ei tule horjuttaa ilman erittäin tärkeäksi katsottua perustetta.

[5] Teknologiateollisuus ry:n julkaisu 9/2014: Suomi uuteen nousuun - ICT ja digitalisaatio tuottavuuden ja talouskasvun lähteinä (kirjoittanut Matti Pohjola).

Edellä esitetyn perusteella tiedustelutoimivaltuuksia on kansalaisiin ja yrityksiin kohdistuvien vaikutusten lisäksi harkittava myös laajemman tietoyhteiskuntakehityksen ja digitalisaation näkökulmasta.

1. Tietoliikennetiedustelu on verkkovalvontaa

Tiedonhankintalakityöryhmän mietinnössä kuvataan verkoissa toteutettavan tiedonhankinnan keinoja käsitteillä ”tietoliikennetiedustelu” ja ”tietojärjestelmätiedustelu”. Liikenne- ja viestintäministeriö käyttää kuitenkin tässä eriävässä mielipiteessään tietoliikennetiedustelusta käsitettä verkkovalvonta.[6]

Myös työryhmä on työskentelynsä aikana käyttänyt tietoliikennetiedustelusta käsitettävä verkkovalvonta. Syksyllä 2014 käsitteitä kuitenkin päätettiin vaihtaa, koska verkkovalvonnan koettiin herättävän liian kielteisiä ajatuksia mietintöä luettaessa. Toiminnasta käytetyn käsitteen muuttaminen ei kuitenkaan muuta itse toimintaa. Liikenne- ja viestintäministeriö katsoo, että verkkovalvonta kuvaa hyvin mietinnön tietoliikennetiedustelulla tarkoitettua toimintaa (”rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuva tiedustelu”) ja vastaa myös julkisessa keskustelussa käytettyä käsitteistöä.

Liikenteen rajat ylittävyys

Verkkovalvonnan kohdentaminen ”rajat ylittävään tietoliikenteeseen” on vaikeaa tai käytännössä mahdotonta, koska palveluita tuotetaan nykyään entistä enemmän globaaleille markkinoille. Esimerkiksi pilvipalveluita käytettäessä tietoa tallentuu useammalle palvelimelle, jotka voivat sijaita eri puolilla maailmaa. Tämä tarkoittaa sitä, että Suomesta pilvipalvelusähköpostista (Gmail, MS Outlook) lähetetty sähköposti Suomessa olevalle vastaanottajalle saattaa kopioitua jo lähetyshetkellä useille palvelimille ympäri maailmaa.

Sen lisäksi, että tieto voi tallentua eri palvelimille, tietoliikenne myös yleensä ohjautuu reitittymään lyhintä tai nopeinta reittiä kohteeseensa. Liikenteen reitittyminen riippuu arvotetuista resursseista ja perustuu algoritmeihin. Tavallisella käyttäjällä ei lähtökohtaisesti ole mahdollisuutta vaikuttaa siihen, mitä reittiä esimerkiksi sähköpostiviestit kulkevat vastaanottajalle. Edellä mainittujen seikkojen takia **tietoliikenne on enenevässä määrin rajat ylittävää, vaikka se olisikin tarkoitettu liikkumaan vain Suomen sisällä lähettäjältä vastaanottajalle.**

Etuliitteen ”rajat ylittävä” käyttäminen mietinnössä hämärtää lukijan käsitystä siitä, mihin viestintään verkkovalvonta voisi kohdistua. Kun käytännössä ainakin tietoliikennetiedustelun ensivaiheessa (seulonta) rajat ylittävän liikenteen erottelu on vaikeaa tai mahdotonta, ei kaikkea tietoliikennetiedustelua voida katsoa kohdistuvaksi vain rajat ylittävään tietoliikenteeseen. Tämä ei tietenkään tarkoita sitä, etteikö verkkovalvontaan voitaisi säätää esimerkiksi käsittelykieltoa Suomen sisäiselle liikenteelle. Juridisesta näkökulmasta viestien rajat ylittävyydellä ei ole suurta merkitystä, sillä viestinnän luottamuksellisuuden suoja koskee kaikkea viestintää, joka on Suomen oikeudenkäytön piirissä. Vaikuttaisi siltä, että mietinnössä rajat ylittävyyden korostamisella on pyritty lähinnä hälventämään harhaanjohtavasti verkkovalvontaan kohdistuvia ennakkoluuloja, eikä niinkään kuvaamaan toimintaa itsessään.

[6] Englannin kielessä verkkovalvonnasta käytetään yleisesti nimitystä ”mass surveillance”.

Mietinnössä on kuvattu tietoteknistymisen vaikutuksia henkilöiden väliseen kanssakäymiseen. Tietoteknistyminen ja sähköisten viestintävälineiden lisääntyvä käyttö kuvataan mietinnössä lähinnä niiden muodostamien uhkien kautta.[7] Ihmisillä ja yrityksillä on Euroopan yhdentymisen ja muun globalisaatiokehityksen johdosta enemmän sosiaalisia suhteita ulkomaille. Näitä suhteita on tehokasta, helppoa ja taloudellista ylläpitää esimerkiksi sähköpostilla tai sosiaalisen median sovellusten kautta. Tämän lisäksi Suomessa harjoitetaan merkittävässä määrin kansainvälistä liiketoimintaa, jonka voidaan arvioida lisääntyvän muun muassa digitalisoitumisen ansiosta.

Viestinnän luottamuksellisuus suojaa sellaistakin viestintää, jossa vain toinen osapuoli on suomalainen. Mietinnön johtopäätöksissä esitetty ajatus siitä, että verkkovalvonta voisi vaarantamatta viestinnän luottamuksellisuuden perusoikeussuojaa kohdistua pelkästään vieraan valtion tietoliikenteeseen vaikuttaa lähinnä teoreettiselta, jos otetaan huomioon internetissä liikkuvan tietoliikenteen ominaisuudet ja valtioiden rajat ylittävä luonne.

2. Viranomaisille voidaan antaa vain toimivaltuuksia, jotka perustuvat niiden lakisääteisiin tehtäviin

Suomen perustuslaissa säädetyn oikeusvaltioperiaatteen mukaan julkisen vallan käytön tulee perustua lakiin ja kaikessa julkisessa toiminnassa on noudatettava tarkoin lakia.[8] Periaatteen toteutumisen kannalta on tärkeää, että viranomaisille esitetään ainoastaan sellaisia salaisia pakkokeinovaltuuksia tai tiedonhankintatoimivaltuuksia, joiden tarve on perusteltu kyseisen viranomaisen lakisääteisen tehtävän suorittamisen kannalta välttämättömäksi. Työryhmän mietinnössä toimivaltuuksien tarve on kuvattu epäselvästi ilman, että niitä on selkeästi sidottu kyseisten viranomaisten lakisääteisiin tehtäviin.

Mietinnössä poliisin ja puolustusvoimien tiedonhankinnan tarpeet on perusteltu sillä, että on olemassa ”yhteiskuntaa vakavasti vaarantavia uhkia”. Viranomaisten laissa määritellyt tehtävät ja mietinnössä esitetyt toimivaltuudet eivät kohtaa. Oikeusvaltioperiaatteen mukaan tiedonhankintaa koskevat uudet toimivaltuudet tulisi perustella täsmällisemmin sellaisten tietojen saannin tarpeilla, jotka ovat välttämättömiä poliisin ja puolustusvoimien laissa säädettyjen tehtävien toteuttamiseksi.

Kuten mietinnössäkin todetaan, yleinen kansainvälistymis- ja digitalisoitumiskehitys on tärkeää ja väistämätöntä. On selvää, että samalla turvallisuusympäristömme muuttuu ja monimutkaistuu. Tekniikan kehitystä voidaan käyttää hyvän lisäksi myös pahaan. Kansallista turvallisuutta vaarantavia tekoja voidaan toteuttaa entistä lyhyemmällä valmisteluajalla ja vakavammin seurauksin. Tietoverkkoja ja niiden päällä toimivia uusia teknologioita, voidaan hyödyntää paitsi suunnittelussa ja valmistelussa, myös tekovälineenä erilaisissa vakavissa turvallisuutta uhkaavissa toimissa. Tämän takia **liikenne- ja viestintäministeriö katsoo, että on tarpeellista pitää huolta siitä, että turvallisuusviranomaisillamme on riittävät ja oikeasuhtaiset toimivaltuudet kehittyvissä tietoverkoissa.**

[7] Esim. s. 18: " Kansalliseen turvallisuuteen kohdistuviin turvallisuusuhkiin liittyy globalisoitumisen seurauksena yhä useammin Suomessa ja ulkomailla olevien henkilöiden välisiä kytköksiä ja siitä seuraavaa tarvetta molemminpuoliseen kommunikointiin. Sähköisiä välineitä käytetään hyväksi uhkien taustalla olevien valtiollisten ja ei-valtiollisten tahojen viestinnässä, tehtäväksi annoissa, tehtävien toteuttamista koskevassa raportoinnissa, tekojen suunnittelussa, kohteita koskevassa tiedonhankinnassa, osallisten motivoinnissa ja radikalisoinnissa sekä uusien jäsenten rekrytoinnissa”.
[8] Suomen perustuslain (731/1999) 2 §.

Puolustusvoimien lakisääteisenä tehtävänä on muun muassa Suomen sotilaallinen puolustaminen.[9] On ilmeistä, että puolustusvoimilla on rauhan aikanakin tarve saada tietoa Suomeen kohdistuvasta aseellisen hyökkäyksen tai sitä vastaavan uhan kohdistumisesta Suomeen.

Liikenne- ja viestintäministeriö katsoo, että siviiliyhteiskuntaan kohdistuvan verkkovalvonnan sijasta tehokkaampaa ja yhteiskunnalle vähemmän vahingollista olisi hankkia tietoa kohdennetusti niistä ulkomailla sijaitsevista tietojärjestelmistä, joissa käsitellään Suomen sotilaalliseen puolustamisen kannalta olennaista tietoa aseellisen hyökkäyksen uhkasta tai siihen verrattavasta uhkasta. Kyse olisi tiedosta, joka hankittaisiin ulkomaisista sotilaallisista johtamisjärjestelmistä.

Työryhmä on käyttänyt kohdennetusta tiedonhankintakeinoista termiä *tietojärjestelmätiedustelu.* Käytännössä kyse olisi tiedonhankinnan kohteeksi määritettävien ulkomailla sijaitsevien johtamisjärjestelmiin liittyvien tietokoneiden tietoturvan loukkaamisesta sotilaallista maanpuolustusta koskevan tiedon hankkimiseksi. Teknisesti tietojärjestelmätiedustelu on toteutettavissa monella eri tavalla. Keinojen käyttöedellytyksiä ja mahdollista soveltamisalaa saattaa silti olla syytä arvioida kansainvälisen oikeuden näkökulmasta.

Liikenne- ja viestintäministeriö katsoo, että puolustusvoimille tulee turvata oikeus välttämättömiin, tehokkaisiin ja oikeasuhtaisiin toimivaltuuksiin sotilaallisen puolustamisen kannalta välttämättömien tietojen hankkimiseksi. **Liikenne- ja viestintäministeriö kuitenkin katsoo jäljempänä esitetyin perustein, ettei mietinnössä kuvattu verkkovalvonta ole välttämätön, tehokas ja oikeasuhtainen keino hankkia keskeisimpiä tietoja Suomen sotilaalliseksi puolustamiseksi.** Päinvastoin ministeriö pitää mietinnössä kuvatun kaltaista verkkovalvontaa epätehokkaana sotilaallisen puolustuksen perustellun tiedontarpeen kannalta. Lisäksi ministeriö katsoo, että verkkovalvonta voi vaikuttaa haitallisesti siviiliyhteiskunnan ja kansalaisten perusoikeuksien toteutumiseen, Suomessa toimivien yritysten toimintaedellytyksiin sekä yleiseen tietoyhteiskuntakehitykseen.

Sotilaallisen maanpuolustuksen alalla Suomeen kohdistuvaan tiedustelutoimintaan ja sotilaallisen maanpuolustuksen tarkoitusta vaarantavaan toimintaan liittyvien rikosten ennalta estämisestä ja paljastamisesta säädetään uudessa sotilaskurinpidosta ja rikostorjunnasta puolustusvoimista annetussa laissa (255/2014). Laki tuli voimaan 1.5.2014 ja siinä on määritelty ne salaiset pakkokeinot, joita puolustusvoimat voi käyttää mainittujen sen tehtäviin liittyvien rikosten tutkinnassa.[10] Työryhmän mietinnöstä ei ilmene, miltä osin nämä tutkintakeinot ovat riittämättömiä Suomen puolustamisen kannalta. Jos katsotaan, etteivät puolustusvoimien rikostorjuntaa koskevat toimivaltuudet ole riittäviä puolustusvoimien tehtävien suorittamiseksi, liikenne- ja viestintäministeriö pitää perusteltuna, että näiden pakkokeinojen nykyistä aineellista tai alueellista soveltamisalaa taikka käytön edellytyksiä arvioidaan uudelleen.

[9] Laki puolustusvoimista (551/2007) 2 §. Säännöksen mukaan Suomen sotilaalliseen puolustukseen kuuluu a) maa-alueen, vesialueen ja ilmatilan valvominen sekä alueellisen koskemattomuuden turvaaminen; b) kansan elinmahdollisuuksien, perusoikeuksien ja valtiojohdon toimintavapauden turvaaminen ja laillisen yhteiskuntajärjestyksen puolustaminen; c) sotilaskoulutuksen antaminen ja vapaaehtoisen maanpuolustuskoulutuksen ohjaaminen sekä maanpuolustustahdon edistäminen. Lain 4 §:n mukaan puolustusvoimat turvaa Suomen aluetta, kansan elinmahdollisuuksia ja valtiojohdon toimintavapautta sekä puolustaa laillista yhteiskuntajärjestystä tarvittaessa sotilaallisin voimakeinoin *aseellisen hyökkäyksen tai sitä vastaavan ulkoisen uhan* kohdistuessa Suomeen. Sotilaallisten voimakeinojen tulee olla sopusoinnussa Suomea sitovien kansainvälisten velvoitteiden kanssa. Sotilaallisilla voimakeinoilla tarkoitetaan sotilaan henkilökohtaisen aseen ja sitä voimakkaampaa asevoiman käyttöä.

[10] Lain 89 §:n mukaan puolustusvoimilla on toimivaltuudet mm. seuraaviin tutkintakeinoihin: 1) Tukiasematietojen hankkiminen; 2) suunnitelmallinen tarkkailu; 3) peitelty tiedonhankinta; 4) tekninen kuuntelu; 5) tekninen katselu; 6) tekninen seuranta; 7) teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkiminen. Pykälän mukaan puolustusvoimat saa käyttää edellä mainittuja tutkintakeinoja seuraavien rikosten paljastamisessa: 1) Suomen itsemääräämisoikeuden vaarantaminen; 2) sotaan yllyttäminen; 3) maanpetos ja törkeä maanpetos; 4) vakoilu ja törkeä vakoilu; 5) turvallisuussalaisuuden paljastaminen; sekä 6) luvaton tiedustelutoiminta.

Poliisin lakisääteisenä tehtävänä on oikeus- ja yhteiskuntajärjestyksen turvaaminen, yleisen järjestyksen ja turvallisuuden ylläpitäminen sekä rikosten ennalta estäminen, paljastaminen, selvittäminen ja syyteharkintaan saattaminen. Poliisin toiminnan tehokkuus perustuu monella tapaa järjestykseen ja rikoksiin liittyvän tiedon hankintaan. Poliisille onkin poliisi- ja pakkokeinolaeissa säädetty lukuisia välttämättömiä toimivaltuuksia poliisin lakisääteisiin tehtäviin liittyvän tiedon hankkimiseksi.

Uudistetut poliisilaki (872/2011) ja pakkokeinolaki (806/2011) tulivat voimaan 1.1.2014.[11] Lait antavat poliisille oikeuden hankkia tietoja rikoksesta epäillyn luottamuksellisesta viestinnästä ja tämän käyttämistä tietokoneista monin keinoin.[12] Lisäksi poliisi sai uutena toimivaltuutena oikeuden tehdä teknistä laitetarkkailua, joka käytännössä tarkoittaa tiedon hankkimista salaa rikoksesta epäillyn tietokoneelta loukkaamalla tämän tietoturvallisuutta. Kyse on teknisesti samankaltaisesta toiminnasta kuin tietojärjestelmätiedustelu. Työryhmä ei ole mietinnössään kattavasti arvioinut näiden lakien mukaisten salaisten tiedonhankinnan toimivaltuuksien käyttöä ja tehokkuutta, riittävyyttä tai riittämättömyyttä poliisin lakisääteisten tehtävien hoitamisessa. Liikenne- ja viestintäministeriölle on epäselvää, minkälaisten rikosten torjumiseksi poliisin käytössä olevat tiedonhankinnan keinot eivät ole riittäviä.

Liikenne- ja viestintäministeriö pitää tärkeänä, että poliisilla on kattavat mahdollisuudet saada rikoksiin liittyvää tietoa Suomessa sijaitsevista tietojärjestelmistä poliisi- ja pakkokeinolain mukaisessa menettelyssä. **Jos katsotaan, että poliisin nykyiset valtuudet eivät ole riittäviä poliisin tehtäviin nähden, liikenne- ja viestintäministeriö pitää perusteltuna että näiden salaisten pakkokeinojen nykyistä alueellista tai aineellista soveltamisalaa taikka käytön muita edellytyksiä arvioidaan uudelleen.** Tällaiset mahdolliset lainsäädännön tarkastelut tulisi tehdä normaalilla tavalla valtioneuvoston ohjesäännön mukaisesti.[13]

Liikenne- ja viestintäministeriö katsoo, että perusoikeussuojan piirissä olevien kansalaisten yksityiselämää ja viestinnän luottamuksellisuuden suojaa loukkaavien poliisin salaisten pakkokeinovaltuuksien käytön edellytyksenä on aina oltava riippumattoman tuomioistuimen konkreettisen rikosepäilyn johdosta antama lupa. Ministeriön mielestä ei ole perusteltua, että tästä lainsäädännössä ja perustuslakivaliokunnan lausuntokäytännössä vakiintuneesta käytännöstä poikettaisiin.[14] Verkkovalvontaan myönnetty lupa ei samalla tavalla kohdistuisi konkreettiseen rikosepäilyyn yksittäistapauksessa.

[11] Pakkokeinolain salaisia pakkokeinoja koskevassa 10 luvussa säädetään, että telekuuntelua, tietojen hankkimista telekuuntelun sijasta, televalvontaa, tukiasematietojen hankkimista, suunnitelmallista tarkkailua, peiteltyä tiedonhankintaa, teknistä tarkkailua (tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimista, peitetoimintaa, valeostoa, tietolähdetoimintaa ja valvottua läpilaskua voidaan käyttää *esitutkinnassa* salassa niiden kohteilta.

[12] Poliisilain salaisia tiedonhankintakeinoja koskevassa 5 luvussa säädetään telekuuntelun, tietojen hankkimisen telekuuntelun sijasta, televalvonnan, tukiasematietojen hankkimisen, suunnitelmallisen tarkkailun, peitellyn tiedonhankinnan, teknisen tarkkailun (tekninen kuuntelu, tekninen katselu, tekninen seuranta ja tekninen laitetarkkailu), teleosoitteen tai telepäätelaitteen yksilöintitietojen hankkimisen, peitetoiminnan, valeoston, tietolähdetoiminnan ja valvotun läpilaskun käyttämisestä *rikoksen estämiseen, paljastamiseen tai vaaran torjumiseen*. Näitä tiedonhankintakeinoja voidaan käyttää salassa niiden kohteilta. Lisäksi edellä mainittuja keinoja saadaan käyttää seuraavien *rikosten paljastamisessa*: 1) Suomen itsemääräämisoikeuden vaarantaminen; 2) sotaan yllyttäminen; 3) maanpetos, törkeä maanpetos; 4) vakoilu, törkeä vakoilu; 5) turvallisuussalaisuuden paljastaminen; 6) luvaton tiedustelutoiminta; 7) rikoslain 34 a luvun 1 §:n 1 momentin 2–7 kohdassa tai mainitun pykälän 2 momentissa tarkoitettu terroristisessa tarkoituksessa tehtävä rikos; 8) terroristisessa tarkoituksessa tehtävän rikoksen valmistelu; 9) terroristiryhmän johtaminen; 10) terroristiryhmän toiminnan edistäminen; 11) koulutuksen antaminen terrorismirikoksen tekemistä varten; 12) värväys terrorismirikoksen tekemiseen; 13) terrorismin rahoittaminen.

[13] Valtioneuvoston ohjesäännön (262/2003) 14 §:n mukaan oikeusministeriön toimialaan kuuluu mm. lainvalmistelu rikos- ja prosessioikeuden alalla.

[14] PeVL 8/1994 vp.

”Tiedustelu” tai ”uhkien torjunta” eivät ole puolustusvoimien tai poliisin lakisääteisiä tehtäviä. Jos tiedustelutoiminnasta on tarve säätää lailla, tulee tiedustelutoimintaa tarkastella samoin perustein kuin muitakin viranomaisten lakisääteisten toimivaltuuksien käyttöä. Liikenne- ja viestintäministeriö pitää itsestään selvänä, ettei millekään viranomaiselle ole perusteltua säätää laajempia perusoikeussuojaa loukkaavia toimivaltuuksia kuin mikä on välttämätöntä kyseisen viranomaisen lakisääteisten tehtävien suorittamisen kannalta. Liikenne- ja viestintäministeriö kehottaa oikeusministeriötä arvioimaan, onko Suomessa tarvetta yleiselle tiedustelulainsäädännölle, jossa arvioitaisiin huolellisesti poliisin ja puolustusvoimien salaiseen tiedonhankintaan liittyvien tehtävien määrittelyn tarkoituksenmukaisuutta ja vasta sen jälkeen tehtävien suorittamiseksi tarvittavia välttämättömiä ja tehokkaita tiedustelukeinoja sekä toimivaltuuksia.

3. Verkkovalvonnan tehokkuutta ei ole osoitettu, eikä vaihtoehtoja arvioitu

Kuten todettu tiedonhankintalakityöryhmän mietinnössä on käsitelty kolmea tiedustelutoimivaltuutta, eli kolmea keinoa hankkia kansallisen turvallisuuden kannalta välttämätöntä tietoa (verkkovalvonta, ulkomaan henkilö- ja tietojärjestelmätiedustelu). Mietinnössä on painotettu, ettei millään yksittäisellä tiedustelumenetelmällä saada kaikkea kansallista turvallisuutta koskevaa tietoa, vaan tieto joudutaan hankkimaan ja varmistamaan useilla toisiaan tukevilla tiedustelumenetelmillä. Myöskään mietintöön valituissa verrokkimaissa ei ole tyypillisesti säädetty vain yhdestä tiedustelumenetelmästä. Lisäksi mietinnössä todetaan, etteivät siinä esitetyt tiedustelumenetelmät korvaa toisiaan, koska ne ovat luonteeltaan osittain erilaisia.

Käytännössä mietinnössä ei ole esitetty vaihtoehtoehtoisia tiedonhankintamenetelmiä verkkovalvonnalle, eikä verkkovalvontaa ole esimerkiksi vertailtu suhteessa ulkomaan tietojärjestelmätiedusteluun. Vaikka **verkkovalvonnalla ja tietojärjestelmätiedustelulla ei kaikilta osin voitaisi vastata samaan tiedonhankintatarpeeseen, olisi verkkovalvonnalle silti pitänyt pyrkiä löytämään vaihtoehtoisia tiedonhankintamenetelmiä.** Kaiken kaikkiaan vaikuttaa siltä, ettei muita menetelmiä ole tunnistettu tai haluttu ottaa harkittavaksi.

<u>Tietoliikenteen salaaminen</u>

Suomen lainsäädäntö turvaa kaikille oikeuden suojata käytössä olevin teknisin mahdollisuuksin sähköisen viestin ja tunnistamistiedot. Viestintävirasto onkin useissa yhteyksissä kannustanut käyttäjiä salaamaan viestintänsä. Tietojen salaamista voidaan käyttää myös yhtenä keinona, kun halutaan toteuttaa henkilötietojen suojaamista koskevia velvoitteita.

Tiedonhankintalakityöryhmän työskentelyn aikana on useamman kerran kuultu, kuinka tietoliikenteen salaamisen lisääntyminen vaikeuttaa tiedonhankintaa. Salauksen lisääntymiselle on nähtävissä useita syitä. Mitä arvokkaammaksi data käy yritysten liiketoiminnalle, sitä enemmän sitä halutaan suojata. Myös suuria asiakasrekistereitä ylläpitäviin yrityksiin ja yhteisöihin kohdistuneet tietomurrot vaikuttavat innokkuuteen salata liikennettä. Salaamisen lisääntyminen ei kuitenkaan selity pelkästään edellä mainituilla. Tietovuotaja Edward Snowdenin paljastamalla laajamittaisella viranomaisten suorittamalla massavalvonnalla on merkittävä osuutensa asiaan.

Tarkasteltaessa millaisilla sivustoilla internetissä käydään kaikista eniten[15], voidaan todeta, että liikennettä ohjautuu eniten hakukoneisiin, sosiaalisen median sivustoille, videopalveluihin ja nettikauppoihin. Tämä kuvaa internetin kehitystä yhä palvelualustakeskeisemmäksi.[16] Jos paljon liikennettä keräävät sivustot ja niiden tarjoamat palvelualustat käyttävät käyttäjän ja sivuston välisessä yhteydessä esimerkiksi SSL-salausta ja salaavat palvelustaan lähtevän liikenteen, tarkoittaa tämä käytännössä sitä, että tietoon on yhä vaikeampi päästä käsiksi. Isot teknologiayritykset ovat viimeisen vuoden aikana ilmoittaneet ottavansa yhä laajemmin käyttöön liikenteen salaustekniikoita. Esimerkiksi Google Gmail, Facebook ja Yahoo salaavat kaikki lähtevät viestit.[17] Sovellusten sisäisen ja niihin kohdistuvan liikenteen salaaminen vaikeuttaa myös tunnistamistietojen keräämistä.

Snowdenin paljastusten jälkeen tietoliikenteen salaaminen on lisääntynyt erityisesti Euroopassa.[18] On myös nähtävissä, että ihmisten tietoisuus yksityisyyden suojasta ja tietoturvasta internetissä on lisääntynyt.[19] Käyttäjien lisääntyvä tietoisuus yksityisyydensuojasta internetissä luo myös yrityksille painetta salata tarjottujen palveluiden tietoliikennettä ja panostaa tietoturvaan.

Tietoliikenteen salauksia on mahdollista purkaa. Salauksen avaaminen on kuitenkin aina huomattavasti hankalampaa kuin tiedonsalaaminen. Salauksen purkaminen voi myös viedä merkittävästi aikaa. Salauksen purku ei ole ongelma, jos käytössä on salauksen purkuun tarvittavat salausavaimet. Tiedonhankintalakityöryhmän mietinnössä kuitenkin painotetaan, ettei yrityksiä velvoitettaisi luovuttamaan salausavaimia tai asentamaan takaportteja järjestelmiinsä, mitä liikenne- ja viestintäministeriö pitää erittäin hyvänä.

Liikenne- ja viestintäministeriön näkemyksen mukaan tietoliikenteen salaaminen pienentää verkkovalvonnan mahdollisuutta tuottaa päätöksenteon tueksi ajanmukaista tietoa. Lienee selvää, että Suomen sotilaallisen puolustuksen kannalta keskeiset tiedot eivät kulkisi salaamattomana yleisissä viestintäverkoissa. Päinvastoin, juuri sotilaallinen viestintä on perinteisesti ollut hyvin salattua.

Mietinnössä on todettu verkkovalvonnan osalta, että tiedustelutiedon luovuttamisen edellytyksistä kansainvälisille yhteistyötahoille tulisi olla säännökset. Mietinnön mukaan lähtökohtana voisi olla se, että tietoluovutuksella edistetään kansallista turvallisuutta eikä sillä vaarannettaisi Suomen etuja, mukaan lukien kansantaloudelliset edut. Liikenne- ja viestintäministeriön näkemyksen mukaan verkkovalvonnan tehokkuutta ja sitä kautta sen oikeasuhtaisuutta ei voida perustalla kansainvälisen yhteistyön kautta saadulla esimerkiksi salauksen purkuun liittyvällä avulla. Tiedustelutoiminnasta säädettäessä tulee ratkaista mitä tietoja voitaisiin Suomen lainsäädännön nojalla vaihtaa kansainvälisessä tiedusteluyhteistyössä. **Liikenne- ja viestintäministeriö ei pääsääntöisesti voi pitää hyväksyttävänä sitä, että käytännössä suomalaista tietoliikennettä käsiteltäisiin jossain ulkomaisessa tiedusteluorganisaatiossa.**

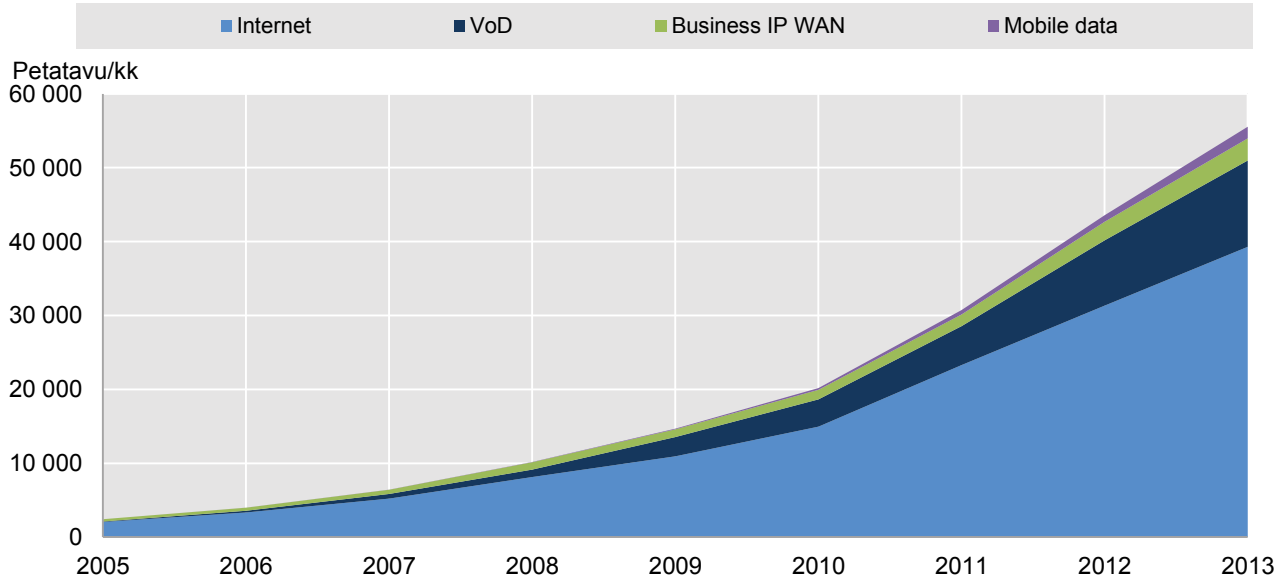
[15] Ks. esim. http://www.alexa.com/topsites, tai https://www.quantcast.com/top-sites.
[16] Alustakeskeisyydestä http://www.economist.com/news/special-report/21593583-proliferating-digital-platforms-will-be-heart-tomorrows-economy-and-even.
[17] Ks. esim. http://www.digitoday.fi/tietoturva/2014/06/04/google-facebook-ja-yahoo-salaavat-sahkopostit-comcast-ja-verizon-eivat/20147868/66.
[18] Ks. esim. http://www.wired.com/2014/05/sandvine-report/ ja https://www.sandvine.com/downloads/general/global-internet-phenomena/2014/1h-2014-global-internet-phenomena-report.pdf .
[19] Ks. esim. http://www.cigionline.org/internet-survey jossa 64 %:lla vastaajista jonkinasteinen huoli yksityisyydestä tietoverkoissa oli lisääntynyt viimeisen vuoden aikana.

Mietinnön mukaan verkkotiedustelulla voidaan salauksesta huolimatta saada kansallisen turvallisuuden kannalta merkittävää tietoa esimerkiksi tunnistamistietojen perusteella. Lisäksi salaamisella ei mietinnön mukaan ole vaikutusta tietoverkkohyökkäysten havaitsemiseen. Väitteitä ei ole perusteltu mietinnössä. Vaikka liikenne- ja viestintäministeriö on lähtökohtaisesti sitä mieltä, että tunnistamistietoja analysoimalla voidaan saada tietystä henkilöstä erittäin yksityiskohtaistakin tietoa selville, on mietinnössä esitetty väite tulkinnanvarainen. Tiettyjä tunnistamistietoja kuten sitä, mistä maasta tietty liikenne on peräisin, on jopa suhteellisen helppo salata erilaisilla palomuureilla tai hyödyntämällä salatuttuja erillisverkoja (VPN-yhteyksiä). Lisäksi esimerkiksi anonyymin verkkoselailun mahdollistavaa TOR-verkkoa käytettäessä käyttäjien anonymiteetti pyritään varmistamaan IP-osoitteita vaihtelemalla.[20] On todennäköistä, että tulevaisuudessa myös viestinnän tunnistamistietoja pyritään aktiivisemmin salaamaan.

Liikenteen määrän kasvu

Salaamisen kanssa rinnakkaisena ilmiönä tulee kiinnittää huomiota yleisissä viestintäverkoissa liikkuvan liikenteen määrän kasvuun tulevaisuudessa. Tämä selittyy paitsi internetin käytön lisääntymisellä niin myös teollisella internetillä, joka liittää yhä suuremman määrän laitteita verkkoon. On arvioitu, että vuoteen 2015 mennessä internetiin yhteydessä olevia laitteita on 25 miljardia ja että määrä kasvaa 2020 mennessä 50 miljardiin.[21] Lisäksi uutta tietoa arvioidaan syntyvän päivittäin miljardi gigatavua ja suurin osa siitä liikkuu internetissä.[22] Internetliikenteen määrän räjähdysmäistä kasvua kuvaa hyvin myös se, että liikenteen arvioidaan vuonna 2018 olevan 64-kertainen suhteessa vuoden 2005 liikennemäärään.[23] Kuten alla olevasta taulukosta ilmenee, IP-liikenteen määrä on OECD:n lukujen mukaan kovassa kasvussa.[24]

Global Internet Protocol (IP) traffic, 2005-13



OECD Science, Technology and Industry Scoreboard 2013 - © OECD 2013

[20] Internet toimii IP- eli Internet Protocol -osoitteilla. Kaikilla internetin verkko- ja päätelaitteilla, kuten tietokoneilla ja älypuhelimilla, on oma IP-osoitteensa. Osoitteet tarvitaan, jotta laitteet osaavat lähettää toisilleen viestejä. IP-osoitteita voikin verrata postiosoitteisiin. Ks. lisää http://pilvi.viestintavirasto.fi/internetpuhelin/internet/ip-osoitteet.html.
[21] http://share.cisco.com/internet-of-things.html.
[22] http://blogs.cisco.com/wp-content/uploads/GITR-2014-Cisco-Chapter.pdf.
[23] http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/VNI_Hyperconnectivity_WP.html.
[24] http://www.oecd-ilibrary.org/science-and-technology/oecd-science-technology-and-industry-scoreboard-2013_sti_scoreboard-2013-en;jsessionid=mvepxnwi8azd.x-oecd-live-02.

Tiedonhankinnan kannalta uusien laitteiden liittäminen internetiin tarkoittaa sitä, että tietoverkoissa tulee liikkumaan yhä enemmän myös koneiden välistä viestintää. Tietoliikenteen määrän kasvaessa myös potentiaalisesti hyödyllisen tiedon määrä tietoverkoissa lisääntyy. Liikenteen määrän ja salauksen lisääntymisen yhteisvaikutuksena hyödyllisen tiedon löytämisestä tulee kuitenkin yhä vaikeampaa ja se voi vaatia yhä enemmän resursseja ja kapasiteettia. Tietoliikenteen määrän huomattava kasvu edellyttäisi myös kasvavia resursseja tiedon hankintaan, käsittelyyn ja salauksen purkamiseen. Näitä ei ole mietinnössä arvioitu.

4. Verkkovalvonnalla voi olla merkittäviä vaikutuksia yritystoimintaan

Työryhmä on työskentelynsä aikana pyrkinyt selvittämään elinkeinoelämän näkemyksiä verkkotiedustelutoimivaltuuksien mahdollisista vaikutuksista. Verkkovalvonnan osalta liikenne- ja viestintäministeriö on tuonut esille, että sillä voi olla negatiivisia vaikutuksia elinkeinoelämän kilpailukykyyn ja investointien suuntautumiseen.[25]

Liikenne- ja viestintäministeriö myöntää, että lopulliset vaikutukset ovat vaikeasti arvioitavissa, mutta korostaa, että yritysvaikutuksia on silti arvioitava perusteellisesti. Arvioinnissa olisi huomioitava erityisesti Snowden-paljastusten jälkeinen aika, tietointensiivisen teollisuuden taloudellinen merkitys tulevaisuudessa ja toimialan kasvunäkymät sekä yleinen digitalisaatiokehitys ja markkinatilanne. Lisäksi tulisi huomioida, että Suomella pitkät perinteet ja paljon osaamista digitaalisen talouden alalla.

Liikenne- ja viestintäministeriö korostaa, että vaikutukset yritystoiminnalle voivat olla erilaisia riippuen muun muassa yrityksen toimialasta, koosta ja sen harjoittamasta kansainvälisestä toiminnasta. Selkeimmin verkkovalvonnan voidaan katsoa vaikuttavan teleyrityksiin, jotka joutuisivat osallistumaan verkkovalvonnan tekniseen toteuttamiseen. Teleyritysten lisäksi verkkovalvonnalla voisi olla vaikutuksia lähes kaikkiin yrityksiin, jotka jollain tavalla toimivat internetin kautta. Erityisesti sillä voi olla vaikutuksia ICT- ja tietoturvayrityksiin, joiden asiakaslupaukset sisältävät elementtejä tiedon ja viestinnän luottamuksellisuudesta. Suorien yritysvaikutusten lisäksi on otettava huomioon epäsuorat vaikutukset kulutuskäyttäytymiseen ja vaikutukset niihin mielikuviin, joiden perusteella kuluttajat käyttävät erilaisia sisältöjä ja palveluita.

Yritysvaikutuksina on huomioitava myös vaikutukset yritysten sijoittautumispäätöksiin, eli investointeihin Suomeen. Kun tietointensiivisen teollisuuden yritykset tekevät sijoittautumispäätöksiä, ne pyrkivät ennakoimaan toimintaansa kohdistuvat oikeudelliset riskit. Huomion kohteena ovat tällöin erityisesti sijoittautumisvaltion lainsäädännön soveltuminen sekä sen aikaansaamat myönteiset ja kielteiset vaikutukset yrityksen liiketoimintaan.[26]

Kun tietointensiivisen teollisuuden yritys tekee sijoittautumispäätöksiä ja liiketoimintasuunnitelmia, eli esimerkiksi päätöstä siitä sijoitetaanko tietty palvelinkeskus Suomeen, yritys huomioi sääntelyn, joka koskee ulkopuolisten tahojen kuten viranomaisten pääsyä yritysten tie-

[25] Tiedonhankintalakityöryhmän mietinnön liitteenä 2. on yhteenveto työryhmän työskentelyn aikana kuultujen sidosryhmien ja asiantuntijoiden kannanotoista. Lisäksi puolustusministeriön internet-sivuilta löytyy tietoja elinkeinoelämälle 29.4.2014 järjestetystä kuulemistilaisuudesta: http://www.defmin.fi/index.phtml?s=767.

[26] Dittmar & Indreniuksen liikenne- ja viestintäministeriölle tekemä selvitys aiheesta: Dataintensiivisen teollisuuden sijoittautumisen edellytykset, 2014.

toon.[27] Tämän lisäksi se arvioi tietosuojaan ja viestinnän luottamuksellisuuteen sekä tietoyhteiskunnan palveluntarjoajiin liittyvät säännökset ja niiden kattavuuden. Tällä hetkellä Suomen rajoitetut viranomaisvaltuudet ja -käytännöt tukevat käsitystä Suomen korkeasta tietosuojan tasosta ja palveluiden piirissä olevien tietojen luottamuksellisuudesta. Toisaalta sijoittautumispäätökset ovat kokonaisarviointeja, joissa huomioidaan myös tekijöitä kuten verotus, sähkön hinta ja saatavuus, työvoimaan liittyvät velvoitteet, yhteiskunnallinen ja poliittinen vakaus, ilmasto ja niin edelleen.

Sijoittautumispäätösten yhteydessä on huomioitava, että yleisen teknistymiskehityksen myötä myös sellaiset alat, jotka eivät perinteisesti ole nojanneet dataan liiketoiminnassaan, ottavat käyttöön analytiikkaa ja muita digitaalisen tiedon hyödyntämisen välineitä. Tämä tarkoittaa, että teollisen internetin sovellutukset ja tietointensiivinen teollisuus tulee lisääntymään lähivuosina voimakkaasti.

Työryhmän mietinnössä viitataan harhaanjohtavasti tutkimus- ja konsulttiyhtiö Gartnerin tutkimukseen. Tutkimuksen mukaan Ruotsi ja Norja koetaan houkuttelevina konesalien sijoituspaikkoina ja todetaan, ettei niiden tiedustelulainsäädäntö ole noussut tutkimuksessa esille.[28] Kyseisessä tutkimuksessa ei ole varsinaisesti eritelty eri maiden houkuttelevuutta konesali-investoinneille lainsäädännön näkökulmasta, vaan siinä on lähinnä pyritty toteamaan asioita, joita sijoittautumisessa olisi huomioitava. Lisäksi tutkimuksessa on laskettu sähkön hinnan vaikutusta konesalien ylläpitämisen kustannuksiin. Ruotsissa ja Norjassa sähkön hinta on laskenut verrattuna Keski-Eurooppaan. Yhtenä sijoittautumiseen vaikuttavana tekijänä Gartnerin tutkimuksessa on mainittu turvallisuusvaatimusten noudattaminen, jonka yksi osa on kohdemaan tietosuojasääntely.

Työryhmä viittaa mietinnössä myös Gearshift Group Oy konsulttitoimistolla teettämäänsä selvitykseen.[29] Selvityksen otsikon mukaan työssä on arvioitu tiedustelulainsäädännön kehittämisen näkökulmasta IT-sektoriin kohdistuvien ulkomaisten investointien kehittymistä ja Ruotsin signaalitiedustelua koskevan niin sanotun FRA-lain mahdollisia vaikutuksia toteutuneeseen investointitoimintaan Ruotsissa. Selvitys on rajattu vuosiin 2008–2013. Käytännössä mietintö ei siis kata Snowden-paljastusten jälkeistä aikaa.[30] Nimenomaan paljastusten jälkeiset arviot investointien suuntautumisesta, olisivat olleet verkkovalvonnan arvioinnin kannalta hyödyllisiä. Selvityksessä ei myöskään ole investointien osalta käytetty materiaalina IT-investointeihin keskittyviä tilastoja.[31] Selvityksessä investointien kehitystä on käsitelty yleisten talouden indikaattorien perusteella, eikä niistä ole yksilöitävissä digitaalista taloutta ja vasta kehittymässä olevaa tietointensiivistä teollisuutta.

Gearshift Group Oy:n selvityksen mukaan Ruotsin selkeä tiedustelulainsäädäntö saattaa olla jopa kilpailuetu.[32] Selkeä sääntely ja sääntelyn sovellettavuus ovat yritystoiminnan ennakoitavuuden kannalta tärkeä tekijä ja myös mahdollinen kilpailuvaltti. Liikenne- ja viestintäministeriön vuonna 2014 teettämän konesalien sijoittumiseen liittyvän Gearshift Group Oy:n laatiman selvityksen mukaan sen sijaan, Snowden-paljastukset voidaan katsoa yhdeksi sellaiseksi markkina-ajuriksi, joka ohjaa yritysten mielenkiintoa nimenomaan Yhdysvalloista Euroop-

[27] Ks. Dittmar & Indreniuksen liikenne- ja viestintäministeriölle tekemä selvitys aiheesta: Dataintensiivisen teollisuuden sijoittautumisen edellytykset, 2014.
[28] Lisätietoa tutkimuksesta: http://www.gartner.com/newsroom/id/2884318.
[29] Selvitys on liitteenä mietinnössä. Se on otsikoitu: ” IT sektoriin kohdistuvien ulkomaisten investointien kehittyminen Ruotsissa ja Suomessa vuosina 2008 - 2013 ja Ruotsin ”FRA-lain” mahdolliset vaikutukset investointeihin”.
[30] Selvityksessä monet esitetyistä kuvioista ja taulukoista koskevat aikaa ennen vuotta 2013. Ks. Gearshift Group Oy:n selvitys tiedonhankintalakityöryhmälle, s. 5-8, 11.
[31] Ks. Gearshift Group Oy:n selvitys tiedonhankintalakityöryhmälle, s. 5-6.
[32] Ks. Gearshift Group Oy:n selvitys tiedonhankintalakityöryhmälle, s. 10.

paan.[33] Lisäksi tieto siitä, että verkkovalvontaa ei maassa harjoiteta lisää yhtälailla yritystoiminnan ennakoitavuutta.

Investointien menetyksestä ja verkkovalvonnan mahdollisesti aiheuttamasta mainehaitasta on vaikeaa antaa kattavaa arviointia. Kuten aiemmin kuvattiin, esimerkiksi investointien suuntautuminen perustuu monipuoliseen vaikutustenarviointiin yrityksen liiketoiminnan kannalta. Kun pilvipalvelumarkkinat edelleen kasvavat, tarvitaan konesaleja kuitenkin lisää. Onkin havaittavissa, että isoja palvelinkeskusten investointipäätöksiä tehdään seuraavien vuosien aikana ja nyt tehtävät päätökset vaikuttavat toimialan kehitykseen seuraavat 15 vuotta.[34] Sijoittautumispäätökset ja konesalien rakentaminen Suomeen ovat jo itsessäänkin tavoiteltavia investointeja, mutta vielä merkittävämpänä mahdollisuutena voidaan nähdä konesalien yhteyteen muodostuvat laajemmat ekosysteemit. Pelkkien palvelimien sijaan datakeskuksen ympärille voi kehittyä muutakin toimintaa kuten lisäarvopalveluita ja tutkimus- ja tuotekehitystoimintaa.[35]

Snowdenin paljastusten jälkeen on jo ehditty arvioida, että paljastusten vaikutukset amerikkalaisten pilvipalveluyritysten liiketoimintaan voisivat alakanttiin arvioitaessakin olla yhteensä yli 20 miljardin dollarin luokkaa vuosina 2014–2016.[36] Myös amerikkalaiset yritykset ovat tuoneet julkisesti esille laajamittaisen tiedustelutoiminnan paljastumisesta yrityksilleen aiheutuneita taloudellisia ja luottamukseen liittyviä haittoja.[37]

Suomella on edellytykset pärjätä hyvin kilpailussa konesali-investoinneista. Viestinnän luottamuksellisuus ja yksityisyyden suoja on meillä korkealla tasolla, olemme liittoutumaton, luotettava ja yhteiskunnallisesti ja poliittisesti vakaa maa, eikä meillä ole odotettavissa esimerkiksi palvelinkeskuksia vaarantavia geologisia järistyksiä. Viileän ilmaston lisäksi sähkön saatavuus ja hinta ovat erityisesti datakeskusten sähköveronalennuksen jälkeen hyvällä tasolla. Meillä on myös paljon osaavaa ICT:n alan työvoimaa. **Lisäksi Suomeen on parhaillaan rakentumassa suurikapasiteettinen kansainvälinen tietoliikennekaapeliyhteys Eurooppa.** Toistaiseksi kaikki kansainvälinen liikenne on reitittynyt Ruotsin kautta, mikä on ollut Suomelle epäedullista. Tämä muuttuu kun Itämeren kaapeli valmistuu vuonna 2016. Yhdessäkään palvelinkeskusten sijaintiselvityksessä ei ole ehditty ottaa huomioon tätä Suomen kilpailuasemaan merkittävästi vaikuttavaa tekijää. Itämeren kaapelin rinnalla hallitus on sitoutunut myös edistämään aktiivisesti koillisväylän arktisen merikaapelin rakentamista. Koillisväylän kaapelin rakentaminen olisi merkittävä kilpailutekijä ja sen myötä Suomi voi vahvistaa asemaansa globaalina tietoliikenteen solmukohtaa Euroopan ja Aasian välillä.

Mietinnössä on vastattu väitteeseen verkkovalvonnan Suomen korkeaa tietosuojaa heikentävästä vaikutuksesta toteamalla, että verkkovalvonta kohdistuisi Suomen rajat ylittävään tietoliikenteeseen, joka kulkee sellaisten maiden läpi, joissa on verkkovalvontaa koskevaa lainsäädäntöä. Tämä merkitsee sitä, että Suomen kansainvälisten verkkoyhteyksien kautta kulkeva tietoliikenne voi jo nyt olla valvonnan ja tiedustelun kohteena muiden kuin Suomen viranomaisten taholta. Mietinnössä esitetty pitää ainakin osittain paikkaansa. Se, että muissa maissa suoritetaan verkkovalvontaa, ei perustele sitä, että valvonta olisi Suomessa viranomaisten

[33] Gearshift Group Oy:n Liikenne- ja viestintäministeriölle tekemä selvitys aiheesta: Konesalien rakentamisen suomalaisen kilpailukyvyn kehittäminen ”Lessions learned”, 2014, s. 7.
[34] Gearshift Group Oy:n Liikenne- ja viestintäministeriölle tekemä selvitys s. 12.
[35] Ks. lisää http://kideblogi.wordpress.com/2014/09/05/datakeskusten-ekosysteemia-rakentamassa/.
[36] Information Technology and Innovation Foundation: How Much Will PRISM Cost the U.S. Cloud Computing Industry? http://www2.itif.org/2013-cloud-computing-costs.pdf . Ks. myös http://oti.newamerica.net/sites/newamerica.net/files/policydocs/Surveilance_Costs_Final.pdf .
[37] Ks. esim. ”Cisco says NSA disclosures have affected sales” http://www.cnbc.com/id/101202361 ja https://www.youtube.com/watch?v=m-P4Q-M1tW8 .

lakisääteisten tehtävien suorittamiseksi tarpeellista ja välttämätöntä. Myös muissa maissa suoritetun verkkovalvonnan teho on nykyään kyseenalaistettu koska suojausten tasoja on olennaisesti nostettu. Suomella voisi olla mahdollisuus tulla tärkeäksi, turvallisuudesta huolehtivaksi datakeskittymäksi ja profiloida itseään maana, jossa verkkovalvontaa ei suoriteta.

5. Verkkovalvonnalla rajoitetaan perusoikeuksia, erityisesti oikeutta yksityisyyteen

Tekninen pääsy kaikkeen tietoliikenteeseen rajoittaa lähtökohtaisesti jokaisen suomalaisen perustuslailla turvattua oikeutta yksityisyyteen. Nykyisen perustuslain 10 §:n sisällöstä säädettiin jo vuoden 1995 perusoikeusuudistuksen yhteydessä säätämällä hallitusmuodon 8 §, joka siirrettiin sellaisenaan perustuslakiin vuonna 2000 (10 §). Hallitusmuodon 8 §:n perusteluissa todetaan, että **yksityiselämän suojan lähtökohtana on, että yksilöllä on oikeus elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista hänen yksityiselämäänsä.**

Yksityiselämän piirin tarkka määritteleminen on vaikeaa. Siihen kuuluu muun muassa yksilön oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään ja ruumiistaan. Yksityisyyden suojan ulottuvuuteen liittyvää rajanvetoa tullaan tekemään lähivuosina niin kotimaassa kuin kansainvälisestikin, koska sen merkitys tulee kasvamaan digitaalisen maailman ilmiöiden myötä.[38] Ihmisistä kerääntyy kiihtyvällä vauhdilla enemmän tietoa erilaisiin järjestelmiin kuin koskaan ennen. Myös tiedon analysointi ja erilaisiin suuriin tietoaineistoihin perustuvien johtopäätöksien teko kehittyy.[39]

Mietinnössä ehdotetun verkkovalvonnan arviointia suhteessa yksityisyyden suojaan voidaan hahmottaa kolmesta eri näkökulmasta:

1) Verkkovalvonta suhteessa luottamuksellisen viestinnän sisältöön
2) Verkkovalvonta suhteessa viestien tunnistamistietoihin
3) Verkkovalvonta suhteessa henkilötietojen käsittelyyn

Tiedonhankintalakityöryhmän mietinnössä on todettu, että tiedustelutarkoituksessa toteutettavasta verkkovalvonnasta ei näyttäisi olevan mahdollista säätää perustuslakia muuttamatta. Tämä johtuu siitä, ettei kansallista turvallisuutta ole mainittu perustuslain 10.3 §:ssä[40] perusteena rajoittaa viestinnän luottamuksellisuutta. **Liikenne- ja viestintäministeriö on toistuvasti esittänyt tämän myös omana näkemyksenään.**

Mietinnössä todetun lisäksi liikenne- ja viestintäministeriö haluaa erityisesti kiinnittää huomiota verkkovalvontaan suhteessa tunnistamistietoihin ja henkilötietojen käsittelyyn.

Yksityiselämän suojan kannalta merkityksellisenä voidaan pitää eduskunnan, tietoyhteiskuntakaaren säätämisen yhteydessä antamaa lausumaa. Siinä **eduskunta edellyttää, että palvelujen käyttäjien oikeuksien, kuten yksityisyyden suojan ja luottamuksellisen viestin**

[38] Näitä kuvattu esimerkiksi eriävänä mielipiteen luvussa 3.
[39] Lue lisää esim. Liikenne- ja viestintäministeriön julkaisu 20/2014: Big datan hyödyntäminen, http://www.liikenne- ja viestintäministeriö.fi/julkaisu/4417803/big-datan-hyodyntaminen .
[40] Perustuslain 10.3 §:ä ”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.”.

suojan säilymisestä sähköisissä palveluissa ja verkkoympäristössä huolehditaan kaikin keinoin ja muun muassa kyberturvallisuuden kehittämistyössä pyritään erityisesti ottamaan näiden oikeuksien toteutuminen huomioon.[41]

Suhtautuminen viestien tunnistamistietoihin (välitystiedot, metadata)[42] ja niiden paljastavuuteen on muuttunut. Tunnistamistietoja ovat tyypillisesti esimerkiksi tiedot siitä kuka puhuu puhelimessa kenenkin kanssa, ketkä lähettävät toisilleen sähköposti- tai tekstiviestejä tai millä internetsivustoilla kukin vierailee. Lisäksi tunnistamistietoja voivat olla myös teknisemmät tiedot kuten tiedot viestinnän reitityksestä, kestosta, ajankohdasta, siirrettävien tietojen määrästä, käytetystä protokollasta, tai tiedot lähettäjän tai vastaanottajan päätelaitteen sijainnista tietyn tukiaseman alueella. Sähköisen viestinnän monimuotoistuessa tunnistamistietojen tyhjentävä määrittely hankaloituu, mutta määritelmänsä mukaisesti ne ovat tietoja, jotka voidaan yhdistää oikeus- tai luonnolliseen henkilöön ja joita käsitellään viestin välittämiseksi.

Kuten mietinnössäkin todetaan perustuslakivaliokunnan vakiintuneen käytännön mukaan viestin tunnistamistiedot jäävät luottamuksellisen viestinnän suojaa koskevan perusoikeuden ydinalueen ulkopuolelle. Perustuslakivaliokunta on kuitenkin tietoyhteiskuntakaarta koskevassa lausunnossaan antanut viitteitä tulkintakäytännön muutoksesta:

”Käytännössä sähköisen viestinnän käyttöön liittyvät tunnistamistiedot sekä mahdollisuus niiden kokoamiseen ja yhdistämiseen voivat kuitenkin olla yksityiselämän suojan näkökulmasta siinä määrin ongelmallisia, että kategorinen erottelu suojan reuna- ja ydinalueeseen ei aina ole perusteltua, vaan huomiota on yleisemmin kiinnitettävä myös rajoitusten merkittävyyteen.”[43]

On siis mahdollista, että perustuslakivaliokunta voi jatkossa antaa myös tunnistamistiedoille viestinnän sisältöä vastaavaa suojaa, jos perusoikeuden rajoitus on arvioitavissa merkittäväksi. Selvää kuitenkin on, ettei tunnistamistietojen keräämistä ja erityisesti yhdistämistä muihin tietoihin, voida enää pitää kategorisesti perusoikeussuojan reuna-alueelle kohdistuvana perusoikeuden rajoituksena. **Tiedonhankintalakityöryhmä ei ole yksimielisesti pystynyt tekemään johtopäästöstä siitä, muodostavatko verkkovalvonnassa kerätyt tunnistamistiedot niin merkittävän rajoituksen perustuslain 10 §:n mukaiseen yksityiselämän suojaan, että rajoitus ulottuu perusoikeussuojan ydinalueelle ja edellyttää jo itsessään perustuslain muutosta.** Käytännössä on kyse siitä, voitaisiinko verkkovalvonta ilman perustuslain muutosta kohdistaa tunnistamistietoihin, kun viestinnän sisällön osalta tämä ei ole mahdollista.

Keskustelua tunnistamistietojen paljastavuudesta suhteessa viestinnän luottamuksellisuuteen käydään tekniikan kehityksen takia yleisesti Euroopassa ja muissa länsimaissa. Asiaan on otettu kantaa esimerkiksi EU:n tietosuojaviranomaisten muodostaman **WP29:n tietosuojatyöryhmän** lausunnossa sähköisen viestinnän tarkkailusta tiedustelua ja kansalliseen turvallisuuteen liittyviä tarkoituksia varten.[44] Lausunnossa muun muassa todetaan, että valtion virkamiehet puhuvat usein metatiedon keräämisestä antaen ymmärtää, ettei se ole yhtä vakavaa kuin sisällön kerääminen. Lisäksi lausunnossa myös todetaan, että itse asiassa metatieto paljastaa tietoja helpommin kuin viestien varsinainen sisältö. Metatietoa on helppo yhdistellä ja analy-

[41] Ks. Eduskunnan vastaus 106/2014 vp: http://www.eduskunta.fi/faktatmp/utatmp/akxtmp/ev_106_2014_p.shtml.
[42] Tietoyhteiskuntakaari (917/2014) käyttää käsitettä välitystiedot. Aiemmin sähköisen viestinnän tietosuojalaissa puhuttiin viestinnän tunnistamistiedoista ja usein kansainvälisesti puhutaan metadatasta. Välitystiedot ovat oikeus- tai luonnolliseen henkilöön yhdistettäviä tietoja, joita käsitellään viestin välittämiseksi esimerkiksi tiedot lähettäjästä ja viestin vastaanottajasta, lähetysajankohdasta ja käytetyistä osoitteista yms.
[43] PeVL 18/2014 vp, s. 6.
[44] WP29 819/14/FI, WP 215, annettu 10. huhtikuuta 2014. Erityisesti sivut 4-5. http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/index_en.htm .

soida, koska se on jäsenneltyä. Pitkälle kehitetyillä tietoteknisillä välineillä voidaan analysoida suuria tietoaineistoja ja tunnistaa niihin sisältyviä säännönmukaisuuksia ja suhteita, kuten henkilötietoja, tottumuksia ja käyttäytymistapoja. Myös YK:n ihmisoikeuskomissaarin raportissa, yhdytään WP29-työryhmän kantaan toteamalla, että yksityisyyden suojan kannalta erottelu viestin sisällön ja sitä koskevan tiedon välillä ei ole vakuuttava.[45]

Euroopan unionin tuomioistuimen tuomio tunnistamistietojen pakkotallennusdirektiivistä[46]

Yksityisyyden suoja on ollut viime aikoina esillä myös muutamissa merkittävissä Euroopan Unionin tuomioistuimen ratkaisuissa. Näistä mietinnön kannalta keskeisin on EU-tuomioistuimen 8.4.2014 antama tuomio yhdistetyissä asioissa C-293/12 ja 594/12 Digital Rights Ireland ja Seitlinger ym., jota on käsitelty mietinnössä.[47] Tuomiossa pätemättömäksi todetun direktiivin nojalla jäsenvaltioiden on pitänyt velvoittaa teleoperaattoreita tallentamaan sähköisen viestinnän tunnistamistietoja viranomaistarpeita varten.[48] Tässä liikenne- ja viestintäministeriön eriävässä mielipiteessä ei ole tarkoitus käsitellä kyseistä tuomiota laajemmin kuin mietinnössä. Sen sijaan tarkoitus on tuoda esiin huomioita, jotka puuttuvat mietinnöstä.

EU-tuomioistuin tarkastelee tuomiossaan tunnistamistietojen pakkotallennusdirektiivin säännöksiä ja toteaa, että säilytettävät tunnistamistiedot voivat yhdessä antaa hyvin tarkkaa tietoa henkilöiden yksityiselämästä, muun muassa heidän elintavoistaan, vakituisista tai tilapäisistä oleskelupaikoistaan, päivittäisestä tai muusta liikkumisestaan, tekemisistään, sosiaalisista suhteistaan ja sosiaalisesta ympäristöstään. Vaikka direktiivissä ei sallita viestinnän sisällön säilyttämistä, tunnistamistietojen säilyttäminen voi vaikuttaa siihen, miten henkilöt käyttävät direktiivissä tarkoitettuja viestintävälineitä. Toisin sanoen, vaikka direktiivi ei edellytä tietojen hankkimista sähköisen viestinnän sisällöstä, eikä näin ollen kohdistu yksityiselämän suojaa ja henkilötietojen suojaa koskevien perusoikeuksien keskeiseen sisältöön, niin silti tietojen säilyttämisellä direktiivissä tarkoitetuin tavoin siltä varalta, että toimivaltaiset kansalliset viranomaiset haluaisivat tutustua niihin, puututaan EU-tuomioistuimen mukaan erityisen vakavasti EU:n perusoikeuskirjan 7 artiklassa tarkoitettuun yksityis- ja perhe-elämän kunnioittamiseen ja perusoikeuskirjan 8 artiklassa tarkoitettuun henkilötietojen suojaan.

Tuomioistuin myös toteaa, että tietojen säilyttäminen ja myöhempi käyttäminen ilman, että siitä ilmoitetaan henkilölle, saattaa aiheuttaa tälle tunteen yksityiselämän jatkuvasta valvonnasta.

Tunnistamistietojen pakkotallennusdirektiivissä tarkoitettu tietojen tallentaminen ja mietinnössä käsitelty verkkovalvonta eivät olisi tekniseltä toteutukseltaan täysin vastaavia toimintoja. Mietinnön mukaan verkkovalvonta ei edellyttäisi perustuslakivaliokunnan lausunnossaan esiintuomaa tunnistamistietojen laajamittaista, erittelemätöntä, pitkäaikaista ja rajoittamatonta tallentamista, vaan kyse olisi hakuehtoihin perustuvasta tietoliikenteen suodattamisesta. Verkkovalvonnassa tallennettaisiin sellaiset viestintään liittyvät tiedot, jotka vastaisivat määriteltyjä

[45] A/HRC/27/37, s. 6-7. Välitystietojen paljastamista tiedoista ks. esim. Stanfordin yliopiston jatko-opiskelijoiden tutkimus (http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/).

[46] Tiedonhankintalakityöryhmän mietinnössä käytetään direktiivistä nimeä Data Retention -direktiivi, tässä eriävässä mielipiteessä puhutaan tunnistamistietojen pakkotallennusdirektiivistä. Direktiivin täydellinen nimi on ”Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta 15.3.2006 annettu Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY”. Tuomio saatavilla: http://curia.europa.eu/juris/document/document.jsf;jsessionid=9ea7d0f130d594b5070ed47541ce9786bce364f3cac9.e34KaxiLc3eQc40LaxqMbN4Obh8Re0?text=&docid=150642&pageIndex=0&doclang=FI&mode=req&dir=&occ=first&part=1&cid=8134.

[47] Luvussa 6.1.2.3.

[48] Suomen kansalliset säännökset sisältyvät 1.1.2015 voimaan tulevaan tietoyhteiskuntakaareen (917/2014).

hakuehtoja. Riippuen toimeksiannosta ja hakutermeistä, tallennettaisiin siis käsittelyä varten tietty tietoliikenne ja sen tunnistamistiedot.

Käytännössä, jotta verkkovalvontaa voitaisiin suorittaa, tarkoittaisi tämä sitä, että viranomaisilla olisi pääsy kaikkeen tietoliikenteeseen, josta aina tietty osa otettaisiin talteen hakutermien perusteella. Siinä mielessä tunnistamistietojen pakkotallennusdirektiivin mukaisten tietojen ja verkkovalvonnan välillä ei olisi merkittävää eroa, että molemmissa viranomaisella olisi tiettyjen reunaehtojen täyttyessä pääsy viestintää koskeviin tunnistamistietoihin. Verkkovalvonnassa käytettyjen hakutermien merkitys kasvaa kuitenkin suureksi. Mitä epämääräisempää tai laajempaa hakutermiä käytettäisiin, sitä enemmän liikennettä suodattuisi jatkokäsittelyyn. Tunnistamistietojen pakkotallennusdirektiivin mukaisia tietoja taas voidaan saada rikosten tutkimiseksi ja syyteharkintaan saattamiseksi käyttöön vain yksilöidyissä tapauksissa.

EU-tuomioistuimen tunnistamistietojen pakkotallennusdirektiiviä koskeva tuomio ja siinä esitetty suhteellisuusperiaatteen arviointi on otettava lähtökohdaksi, jos edes harkitaan sääntelyä verkkovalvonnasta. **Erityisesti on huomioitava se, että tuomion perusteella avoimeksi jää, kuten perustuslakivaliokuntakin totesi, merkitseekö viranomaistarpeita varten säädetyn säilyttämisvelvollisuuden ulottuminen käytännössä kaikkien sähköisiä viestimiä käyttävien ihmisten tietoihin jo yksinään oikeasuhtaisuusvaatimuksen loukkausta.** Jos näin arvioidaan, ei myöskään viranomaisten pääsyä kaikkeen tietoliikenteeseen, voida pitää oikeasuhtaisena.

Henkilötietojen suoja

Perustuslain 10.1 §:ssä, todetaan, että henkilötietojen suojasta säädetään tarkemmin lailla. Hallituksen esityksen mukaan säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä.[49] Säännöksellä myös edellytetään lainsäädännöllisiä järjestelyjä henkilötietojen suojasta.

On olennaista huomata, että tunnistamistietojen pakkotallennusdirektiiviä koskevassa tuomiossa EU-tuomioistuin katsoi, että tunnistamistietojen säilyttämisellä loukattiin myös EU perusoikeuskirjan 8 artiklassa tarkoitettua henkilötietojen suojaa. Vaikka tunnistamistiedot eivät aina välttämättä ole henkilötietoja, edellyttää tunnistamistietojen tallentaminen kuitenkin yleensä myös henkilötietojen käsittelyä. EU-tuomioistuin totesikin, että tunnistamistietojen tallentamisen tulee täyttää myös kaikki henkilötietojen suojaan liitetyt vaatimukset.

Mietinnössä on käsitelty henkilötietojen suojaa Euroopan unionin perusoikeuskirjan näkökulmasta, mutta ei Suomen perustuslain. Verkkovalvonnassa väistämättä käsiteltäisiin henkilötietoja, joten tällöin tulisi noudattaa perustuslakivaliokunnan kannanottoja henkilötietojen käsittelystä säätämisestä.

Verkkovalvontaa koskeva sääntely olisi merkityksellistä yksityiselämän ja henkilötietojen suojaa koskevan perustuslain 10 §:n kannalta. Sen 1 momentin mukaan henkilötietojen suojasta säädetään tarkemmin lailla. Perustuslakivaliokunnan vakiintuneen käytännön mukaan lainsäätäjän liikkumavaraa rajoittaa tämän säännöksen lisäksi myös se, että henkilötietojen suoja osittain sisältyy samassa momentissa turvatun yksityiselämän suojan piiriin. Kysymys on kaiken kaikkiaan siitä, että lainsäätäjän tulee turvata tämä oikeus tavalla, jota voidaan pitää hyväksyttävänä perusoikeusjärjestelmän kokonaisuudessa. Perustuslakivaliokunta on käytännös-

[49] HE 309/1993 vp. 8 §:n yksityiskohtaiset perustelut.

sään pitänyt henkilötietojen suojan kannalta tärkeinä sääntelykohteina ainakin rekisteröinnin tavoitetta, rekisteröitävien henkilötietojen sisältöä, niiden sallittuja käyttötarkoituksia mukaan luettuna tietojen luovutettavuus sekä tietojen säilytysaikaa henkilörekisterissä ja rekisteröidyn oikeusturvaa. Näiden seikkojen sääntelyn lain tasolla tulee lisäksi olla kattavaa ja yksityiskohtaista.[50]

Liikenne- ja viestintäministeriö katsoo, että mietintö on henkilötietojen käsittelyn osalta puutteellinen.

Tietoyhteiskuntakaaren 272 §[51]

Tietoyhteiskuntakaaren 272 §:ä ja sen mahdollistama tietoliikenteen seulonta tietoturvasta huolehtimiseksi on mietinnössä rinnastettu verkkovalvontaan. **Liikenne- ja viestintäministeriö katsoo, ettei tietoyhteiskuntakaaren 272 §:n käsittely verkkovalvonnan yhteydessä ole tarkoituksenmukaista.** Vaikka tietoyhteiskuntakaaren 272 §:ssä tarkoitetut toimenpiteet saattavat teknisesti olla lähellä verkkovalvontaa, ei kyseistä sääntelyä voi muilta osin verrata verkkovalvonnasta säätämiseen.

Tietoyhteiskuntakaaren 272 §:n mukaiset tietoturvatoimenpiteet ja tiedustelutarkoituksessa toteutettava verkkovalvonta olisivat sekä yksityisyydensuojaan puuttumisen että toimenpiteiden kohteeksi joutuvien organisaatioiden näkökannalta täysin erilaisia toimia. Yksityisyydensuojan osalta tietoturvatoimenpiteillä pyritään ainoastaan tietoturvaongelman selvittämiseen. Tietoa ei voida käyttää muihin tarkoituksiin. Organisaatiot arvioivat itse toimenpiteiden laajuuden ja tarpeellisuuden. Toimenpiteet käsitellään henkilöstön kanssa yhteistoimintamenettelyssä.

Perustuslain 22 §:n mukaan julkisen vallan tehtävänä on turvata perusoikeuksien ja ihmisoikeuksien toteutuminen. Yksityiselämän suojan takaamiseksi valtiolta on sen lisäksi, että se itse pidättäytyy loukkaamasta kansalaisten yksityiselämää, edellytetty aktiivisia toimenpiteitä yksityiselämän suojaamiseksi toisen yksilöiden loukkauksia vastaan. Perustuslain esitöiden mukaan myös viestinnän luottamuksellisuuden suoja edellyttää toteutuakseen lainsäädäntöä, joka tehokkaasti turvaa luottamuksellista viestintää sekä viranomaisten että muiden ulkopuolisten loukkauksilta.[52] **Tietoyhteiskuntakaaren 272 §:ssä on kyse tällaisesta aktiivisesta toimenpiteestä luottamuksellisen viestinnän suojaamiseksi.** Sen sijaan verkkovalvontaa koskeva sääntely ei ole perusteltavissa luottamuksellisen viestinnän suojaamisella, eikä siinä siten ole samalla tavalla kyse perusoikeuden toteutumista turvaavasta välttämättömästä sääntelystä kuin tietoyhteiskuntakaaren 272 §:ssä. Sen tarkoitus on päinvastaisesti tiedon luottamuksellisuuden murtaminen.

[50] Ks. koko kappaleen osalta esim. PeVL 14/2009 vp , s. 2, PeVL 11/2008 vp , s. 3/I ja PeVL 51/2002 vp , s. 1-2, PeVL 14/2002 vp , s. 2/II.
[51] Tietoyhteiskuntakaari (917/2014) tulee voimaan 1.1.2015, 272 § vastaa sisällöltään sähköisen viestinnän tietosuojalain (516/2004) 20 §:ää.
[52] HE 209/1993 vp.

6. Verkkovalvonta ei parantaisi tietoturvaa, vaan heikentäisi sitä

Tietoturvallisuudella tarkoitetaan vakiintuneesti toimenpiteitä, joilla turvataan jonkin tiedon luottamuksellisuus, eheys ja käytettävyys.[53] Työryhmän tarkastelemilla tiedustelukeinoilla pyrittäisiin ohittamaan tai murtamaan tiedonhankinnan kohteena olevan henkilön tai hänen käyttämänsä tietojärjestelmän tietoturvallisuutta varmistavat suojaukset ja hankkimaan tiedonhankintaa suorittavalle viranomaiselle sellaista tietoa, johon kohde ei ole oikeuttanut ulkopuolisia pääsemään käsiksi. **On selvää, että mietinnössä tarkasteltu verkkovalvonta heikentäisi kaikkien niiden henkilöiden tietoturvallisuutta, joiden viestejä välitettäisiin verkkovalvonnan kohteena olevissa viestintäverkoissa.**

Liikenne- ja viestintäministeriö katsoo, että sen perustuslaista johtuvana tehtävänä on nimenomaisesti edistää yksityisyyden suojan ja viestinnän luottamuksellisuuden toteutumisesta tietoturvallisesti sähköisessä viestinnässä.[54] Perusoikeuksien toteutumisen turvaamiseksi on tärkeää, että kansalaisten, yritysten ja muiden yhteisöjen käytettävissä on korkealaatuisia, luotettavia ja tietoturvallisia viestintäpalveluja.[55] Ministeriö pyrkii ohjauskeinoillaan edistämään viestintäpalvelujen luotettavuutta ja turvallisuutta sekä viestintäpalveluja käyttävien kansalaisten ja yhteisöjen kykyä huolehtia omien verkkoon liitettyjen tietojärjestelmiensä tietoturvasta.

Suomessa on liikenne- ja viestintäministeriön arvion mukaan kansainvälisesti vertaillen erittäin hyvin ja kattavasti toimiva yhteistoimintamalli tietoturvaloukkausten havaitsemiseksi, estämiseksi ja selvittämiseksi. Kaikilla viestintäverkkojen ja palveluiden suunnittelijoilla, rakentajilla ja ylläpitäjillä on 1.1.2015 voimaan tulevan tietoyhteiskuntakaaren mukaan oikeus ja velvollisuus huolehtia verkkojensa ja palveluidensa laadusta ja turvallisuudesta sekä velvollisuus huolehtia muun muassa siitä, että verkkoihin ja palveluihin kohdistuvat tietoturvaloukkaukset ja niiden uhkat voidaan havaita. Valtaosa tietoturvallisuutta edistävistä toimenpiteistä voidaan tehdä ilman erityisiä toimivaltuuksia, mutta teleyrityksille, yhteisötilaajille ja lisäarvopalvelun tarjoajille on säädetty eduskunnan lokakuussa 2014 hyväksymässä tietoyhteiskuntakaaressa erityisiä oikeuksia ryhtyä välttämättömiin toimenpiteisiin tietoturvasta huolehtimiseksi.[56]

Viestintäverkkojen suunnittelevat, rakentavat tai ylläpitävät tahot tai niiden käyttäjinä toimivat asiakasyhteisöt eivät millään tavalla nostaneet esiin tarvetta parantaa tietoturvaa verkkovalvonnan tai muidenkaan tiedusteluvaltuuksien keinoin tietoyhteiskuntakaaren erittäin laajaalaisen ja avoimen valmistelun tai eduskuntakäsittelyn yhteydessä. **Liikenne- ja viestintäministeriö huomauttaa, ettei mietinnössä ole konkreettisesti esitetty, missä mielessä tai minkälaisella toimintamallilla yrityksille voisi olla hyötyä verkkovalvonnasta.**

---

[53] 1.1.2015 voimaan tulevassa tietoyhteiskuntakaaren (917/2014) 3 §:ssä tietoturvallisuudella tarkoitetaan *toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä.* Tietoturvallisuuden oikeudellisesta määritelmästä tarkemmin esim. Saarenpää (toim): Tietoturvallisuus ja laki, 1997.

[54] Perustuslain 23 § ja Valtioneuvoston ohjesäännön 20 §.

[55] Tietoyhteiskuntakaaren 1 § ja HE 221/2013 vp.

[56] Kyseistä tietoyhteiskuntakaaren säännöstä on käytetty mietinnössä ikään kuin perusteluna sille, ettei verkkovalvonnasta säädettäessä tarvitsisi muuttaa perustuslakia. Liikenne- ja viestintäministeriö katsoo, ettei tietoyhteiskuntakaaren 272 §:n käsittely tässä tarkoituksessa ole ymmärrettävää. Tietoyhteiskuntakaaren 272 §:ssä on kyse perustuslain 23 §:n mukaisesta aktiivisesta lainsäädäntötoimesta, jolla nimenomaisesti pyritään edistämään kansalaisten luottamuksellisen viestinnän suojaa. Sen sijaan verkkovalvontaa koskevaa sääntely ei ole perusteltavissa luottamuksellisen viestinnän suojaamisella, eikä siinä olisi kyse perusoikeuden toteutumista turvaavasta välttämättömästä sääntelystä.

Työryhmän mietinnössä tiedustelun tarvetta on perusteltu muun muassa tarpeella parantaa tietoturvallisuutta. Liikenne- ja viestintäministeriö on kuullut laaja-alaisesti viestintäpalvelujen tarjoajia, ja tullut mietinnöstä poiketen siihen käsitykseen, ettei poliisin tai puolustusvoimien tiedustelutoimivaltuuksien tarvetta voida perustella yleisten viestintäverkkojen tai niiden käyttäjien tietoturvan parantamisen tarpeella. **Liikenne- ja viestintäministeriö katsoo, että niin julkisten kuin yksityistenkin yhteisöjen tietoturvallisuuden kehittämiseen on huomattavasti tarpeellisempia, tehokkaampia ja oikeasuhtaisempia keinoja kuin mitä poliisin tai puolustusvoimien tiedustelutoimivaltuuksia lisäämällä voitaisiin saavuttaa.**

Mietinnössä on viitattu Kyberturvallisuuskeskuksen raporttiin[57], jossa todetaan että myös suomalaisiin sekä myös muihin länsimaalaisiin verkkoihin kohdistuu kybervakoilutapauksia, joissa teknisenä apukeinona on käytetty muun muassa kohdistettuja haittaohjelmia. Viittauksella raporttiin on pyritty kyseenalaistamaan väitettä suomalaisten tietoverkkojen puhtaudesta. Vain se, että uhka vakoilusta kohdistuu myös Suomeen, ei vielä kerro Suomen verkkojen puhtaudesta. Suomi on nimenomaan pärjännyt hyvin esimerkiksi Microsoftin tekemissä vertailuissa verkkojen puhtaudesta.[58]

7. Suomen toimenpiteitä tietoturvan kehittämiseksi

Suomen sähköisen viestinnän tietoturvaa koskevia säännöksiä on vastikään uudistettu vuoden 2015 alusta voimaan tulevassa tietoyhteiskuntakaaressa (917/2014). Viestinnän välittäjän on tietoyhteiskuntakaaren 247 §:n mukaan viestejä välittäessään huolehdittava palvelujensa, viestien, välitystietojen ja lisäarvopalvelujen tietoturvasta. Lisäksi tietoyhteiskuntakaaren 243 §:n mukaan kaikki viestintäverkot ja viestintäpalvelut on Suomessa lain mukaan suunniteltava, rakennettava ja ylläpidettävä siten, että sähköinen viestintä on tietoturvallista eikä kenenkään tietosuoja, tietoturva tai muut oikeudet vaarannu. Verkot ja palvelut on niin ikään suunniteltava, rakennettava ja ylläpidettävä siten, että niihin kohdistuvat merkittävät tietoturvaloukkaukset ja tietoturvauhat sekä niiden toimivuutta merkittävästi häiritsevät viat ja häiriöt voidaan havaita.

Lisäksi tietoturvan kehittämiseksi on viime vuosina tehty useita toimenpiteitä. Niistä keskeisimmät käydään seuraavaksi lyhyesti läpi.

Tietoturvastrategiat

Ensimmäinen poikkiyhteiskunnallinen **kansallinen tietoturvastrategia** hyväksyttiin valtioneuvoston periaatepäätöksenä 4.9.2003. Strategia oli Euroopassa ja ilmeisesti maailmassakin ensimmäinen laatuaan. Julkinen ja yksityinen sektori laativat yhdessä strategian, jonka valmistelun ja toimeenpanon koordinoinnista vastasi liikenne- ja viestintäministeriö. Strategiassa todettiin, että kansalaisten ja yritysten luottamusta tietoyhteiskuntaan voidaan lisätä erityisesti tietoturvallisuutta ja yksityisyyden suojaa parantamalla. Strategialla pyrittiin torjumaan tietoturvallisuuden uhkia sekä toisaalta hyödyntämään korkeatasoisen tietoturvallisuuden tarjoamia mahdollisuuksia.

[57] Kohdistettujen haittaohjelmahyökkäyksien uhka on otettava vakavasti. Viestintäviraston Kyberturvallisuuskeskuksen raportti. Syksy 2014: https://www.viestintavirasto.fi/tietoturva/tietoturvanyt/2014/08/ttn201408281226.html .
[58] Väitettä verkkojen puhtaudesta tukee mm. Microsoftin SIR-raportti nro 17, 2014. http://www.microsoft.com/en-us/download/confirmation.aspx?id=44937.

Tietoyhteiskuntaohjelman osana **toinen kansallinen tietoturvastrategia** hyväksyttiin valtioneuvoston periaatepäätöksenä 4.12.2008. Strategian visiona on, että kansalaiset ja yritykset voivat luottaa tietojensa turvallisuuteen sekä tieto- ja viestintäverkoissa että niihin liittyvissä palveluissa. Strategialla on kolme painopistealuetta. Näitä olivat perustaidot arjen tietoyhteiskunnassa, tietoihin liittyvien riskien hallinta ja toimintavarmuus sekä kilpailukyky ja kansainvälinen verkostoyhteistyö. Liikenne- ja viestintäministeriö koordinoi strategian valmistelua ja toteuttamista eri hallinnonaloilla. Toisen tietoturvastrategian tavoitteiden toteuttamiseksi laadittiin vuonna 2009 yhteensä yhdeksän erillistä hanketta käynnistänyt toimenpideohjelma, joka hyväksyttiin valtioneuvoston periaatepäätöksenä.

Vuonna 2013 laadittiin valtioneuvoston periaatepäätöksenä hyväksytty **kansallinen kyberturvallisuusstrategia**, jonka visiona on, että 1) Suomi kykenee suojaamaan elintärkeät toimintonsa kaikissa tilanteissa kyberuhkaa vastaan; 2) kansalaisilla viranomaisilla ja yrityksillä on mahdollisuus tehokkaasti hyödyntää turvallista kybertoimintaympäristöä ja sen suojaamiseen syntyvää osaamista sekä kansallisesti että kansainvälisesti ja että 3) vuonna 2016 Suomi on maailmanlaajuinen edelläkävijä kyberuhkiin varautumisessa ja niiden aiheuttamien häiriötilanteiden hallitsemisessa. Strategian toimeenpanemiseksi laadittiin virkamiestasolla toimeenpano-ohjelma.

Esimerkkejä kansainvälisen tiedustelun kansallisesta käsittelystä

Vuonna 2008 liikenne- ja viestintäministeriössä arvioitiin Ruotsin signaalitiedustelulain (FRA) vaikutuksia suomalaisten viestintäpalvelujen tietoturvaan. Viestintävirasto laati ja julkaisi ohjeistuksen viestinnän salaamisesta vuonna 2009.

Valtioneuvosto käsitteli 19.6.2013 verkkovakoilua ja massatiedustelua koskeneita uutisia Edward Snowdenin paljastuksista sekä niitä toimenpiteitä, joihin tapauksen johdosta ryhdyttiin kansallisesti ja kansainvälisissä yhteyksissä.

Kesäkuussa 2014 Viestintävirasto julkaisi ohjeita ja suosituksia siitä, kuinka suomalaisten tulisi suojautua joutumasta ulkomaisten tiedusteluorganisaatioiden harjoittaman verkkovalvonnan kohteeksi.[59]

Viestintäviraston kyberturvallisuuskeskus

Viestintävirastoon perustettiin vuoden 2014 alussa kyberturvallisuuskeskus valtioneuvoston periaatepäätöksellä. Kyberturvallisuuskeskuksen kautta Viestintävirasto tuottaa tietoturvapalveluita koko yhteiskunnalle ja edistää Suomen varautumista kyberuhkiin ja niiden aiheuttamien häiriötilanteiden hallintaan. Kyberturvallisuuskeskuksen tehtäviin kuuluu tietoturvauhkien- ja loukkausten havainnointi ja selvittäminen sekä kyberturvallisuuden tilannekuvan ylläpito.

Tammikuussa 2014 Viestintävirasto ja valtiovarainministeriö sopivat, että Viestintävirasto tuottaa tietoturvaloukkausten ennaltaehkäisyyn, havainnointiin ja ratkaisuun tähtääviä palveluita[60] valtiovarainministeriölle osana valtiovarainministeriön ympärivuorokautisen tietoturvatoiminnan kehittämishanketta.

NIS-direktiivi

[59] Viestintäviraston suositus 205/2014 S.
[60] ns. GovCERT- ja GovHAVARO-palvelut (lyhenteet tulevat sanoista Governmental Computer Emergency Response Team ja Tietoturvaloukkausten HAvainnointi ja VAROitusjärjestelmä).

EU:n komissio on vuonna 2013 antanut ehdotuksen direktiiviksi verkko- ja tietoturvan korkean tason varmistamiseksi EU:n alueella (**EU:n verkko- ja tietoturvadirektiivi**), jota käsitellään parhaillaan Euroopan parlamentissa ja neuvostossa. Direktiiviehdotuksella luotaisiin yhtäältä velvoitteita verkko- ja tietoturvan parantamisesta jäsenvaltioissa sekä toisaalta jäsenvaltioiden välinen yhteistyömekanismi tietoturvapoikkeamiin liittyvän tiedonvaihdon ja muun yhteistoiminnan järjestämiseksi. Kolmanneksi direktiivi velvoittaisi eräiden soveltamisalaan kuuluvien yhteiskunnan keskeisten alojen (rahoituspalvelut, liikenne, energia, terveys) kriittisten infrastruktuurien ylläpitäjät sekä keskeisimmät tietoyhteiskunnan internetpalveluiden tarjoajat ja julkishallinnot ottamaan käyttöön riskinhallintakäytänteitä ja raportoimaan ylläpitämiinsä keskeisiin palveluihin kohdistuvista merkittävistä tietoturvapoikkeamista.

8. Kansalaisten luottamusta tietoyhteiskuntaan ja internetiin kannattaa vahvistaa

Päätöksenteossa on tärkeä huomioida, ettei toimivia ja kilpailukykyisiä digitaalisia palveluita pystytä nykypäivänä rakentamaan ilman luottamusta. Luottamuksen merkitys näyttäisi jatkuvasti vahvistuvan kansalaisten verkkovalvontaan ja tietoturvauhkiin liittyvien uutisten paljastuessa.

Perinteisissä palveluissa luottamuksen merkitys on itsestään selvää. Harvat haluavat astua turvattomaan lentokoneeseen, antaa rahojaan epäluotettavalle pankille tai laittaa kirjeitään epäluotettavan kuriirin matkaan. Myös digitaalisissa palveluissa käyttäjien luottamus palveluun tulee käyttökokemuksen ohella yhä useammin ratkaisemaan palvelun elinkelpoisuuden ja menestyksen. Jos palveluja tuottavat yritykset haluavat pärjätä kilpailussa, on niiden annettava asiakaslupauksia palveluidensa korkeasta luotettavuudesta.

Suomella on nyt tilaisuus profiloitua maana, jossa valtio pitää osaltaan huolen siitä, ettei asiakkaiden luottamusta ja yritysten kykyä pitää asiakaslupauksensa vaaranneta. Samalla Suomella on yleisemmälläkin tasolla erinomaiset edellytykset kehittyä maailman osaavimmaksi ja luotettavimmaksi maaksi internetissä. Tämän päämäärän voimme saavuttaa, jos pidämme huolta siitä, että yksityisyyden ja luottamuksellisen viestinnän suojaa vaaliva lainsäädäntömme pysyy jatkossakin korkealla tasolla.

Jos Suomi haluaa lunastaa digitalisaation ja internet-talouden avaamat mahdollisuudet, sen tulee kiinnittää erityistä huomiota ainakin seuraaviin seikkoihin:

1. Tieto- ja viestintäteknisten hyödykkeiden käyttäjillä on oltava riittävät valmiudet ja nykyistä parempi ymmärrys tuotteiden käyttöön liittyvistä mahdollisuuksista ja riskeistä. Tuotteiden turvallisuus- ja suojausominaisuuksien sekä käyttöehtojen tulee olla nykyistä läpinäkyvämpiä siten, että asiakas voi verrata eri tuotteiden luotettavuutta ja käyttää halutessaan apuna ulkopuolisia arvioitsijoita. Viranomaisilla ja arviointilaitoksilla voisi olla merkittävä rooli sen todentamisessa, että kuluttajien käyttämät laitteet ja palvelut vastaavat suomalaisia tai eurooppalaisia tietoturvavaatimuksia.

2. Tutkimus-, kehitys- ja opetustyöhön tulee kiinnittää nykyistä enemmän huomiota. Riittävän tutkimus- ja kehitystyön avulla tietoturvallisten tuotteiden ja palveluiden markkinoita on mahdollista kehittää siten, että tieto- ja viestintäteknologiset hyödykkeet vas-

taisivat entistä paremmin käyttäjien tarpeita ja odotuksia erityisesti palveluiden luotettavuuden osalta. Hyviä kehitystyön kohteita ovat esimeriksi ohjelmointi, data-analyysi ja erilaiset salausmenetelmät.

3. Markkinoille täytyy saada uusia, eurooppalaisista lähtökohdista tuotettua palveluita. Markkinoilla on tilausta erityisesti erilaisille ”internetin päällä” toimiville palveluille (ns. Over The Top -palvelut), joilla tarkoitetaan muun muassa viestintäohjelmistoja, selaimia, hakukoneita, tallennuspalveluita ja sosiaalisen median alustoja. Nämä palvelut ovat arvonmuodostuksen kannalta olennaisia liiketoiminnan alueita, sillä monessa tapauksessa ne pystyvät kerryttämään tuloa myös niiden päälle luotujen palveluiden tarjonnasta (esimerkiksi Google Mapsin perustalle luodut palvelut).

IV. Lopuksi

Liikenne- ja viestintäministeriö haluaa kiittää mahdollisuudesta osallistua tiedonhankintalakityöryhmän työskentelyyn. Eriävästä mielipiteestä huolimatta ministeriö katsoo, että työryhmässä on pyritty tekemään työtä entistä paremman ja turvallisemman tulevaisuuden puolesta. Kuten edellä on käynyt ilmi, ministeriö suhtautuu erittäin vakavasti niihin huoliin, joita poliisi ja puolustusvoimat ovat esittäneet toimivaltuuksiensa riittämättömyydestä muuttuvassa maailmassa. Tästä huolimatta ministeriö katsoo, ettei verkkovalvonta ole oikea keino vastata näihin huoliin.

Päivi Antikainen
viestintäneuvos, internetpalvelut -yksikön päällikkö

Laura Tarhonen
neuvotteleva virkamies

TYÖ- JA ELINKEINOMINISTERIÖ
ARBETS- OCH NÄRINGSMINISTERIET
MINISTRY OF EMPLOYMENT AND THE ECONOMY

TEM/2491/00.05.01/2013

16.12.2014

Puolustusministeriö

Lausuma tiedonhankintalakityöryhmän mietintöön

Suomen kyberturvallisuusstrategiasta 24.1.2013 annetun valtioneuvoston periaatepäätöksen mukaan ministeriön kyberturvallisuustehtävät ovat Yhteiskunnan turvallisuusstrategiassa määritettyihin strategisiin tehtäviin liittyviä ministeriöiden tehtäviä. Työ- ja elinkeinoministeriö (TEM) vastaa osana valtioneuvostoa muun muassa Suomen yrittäjyyden ja innovaatiotoiminnan toimintaympäristöstä. TEM:n kyberturvallisuustehtävänä on muun muassa (3) tukea elinkeinoelämän häiriön- ja jatkuvuudenhallintaa TEM:n päätöksenteko- ja ohjausjärjestelyillä, viranomaistoimenpiteet investointimyönteisen ja turvallisen toimintaympäristön luomiseksi ja ylläpitämiseksi yritystoiminnalle ml. ulkomaiset palvelinkeskukset.

Tasavallan Presidentti ja valtioneuvoston ulko- ja turvallisuuspoliittinen ministerivaliokunta (UTVA) keskustelivat kokouksessaan 7.11.2013 muun muassa kansallisen kyberturvallisuuden kehittämistarpeista. Osana Suomen kyberturvallisuusstrategian toimeenpanoa UTVA linjasi, että välittömästi aloitetaan työ Suomen lainsäädännön kehittämiseksi (toimeenpano-ohjelman toimenpide nro 42 ja sen ehdotus vastuutahoksi ja yhteistyötahoiksi). Edelliseen liittyen puolustusministeriö vastuutahona asetti 13.12.2013 yhteistyötahoista koostuneen virkamiestyöryhmän, tiedonhankintalakityöryhmän, jonka työhön myös TEM on osallistunut. Tiedonhankintalakityöryhmä esittää mietinnössään kehittämisehdotuksia tiedustelua koskeviksi uusiksi toimivaltuuksiksi, jotka koskevat tietoliikennetiedustelua sekä ulkomaantiedustelua (ulkomaan henkilötiedustelua ja ulkomaan tietojärjestelmätiedustelua).

TEM ymmärtää ja hyväksyy tiedonhankintalakityöryhmän asettamispäätöksen taustat, tavoitteet ja tehtävän, samoin kuin puolustusvoimien ja poliisin suorituskykyjen kokonaisvaltaisen kehittämisen tarpeet.

TEM:n vastuualueen kannalta erityisesti elinkeinopoliittiset näkökulmat, kuten elinkeinoelämän yleiset toimintaedellytykset, yritysten kilpailukyvyn turvaaminen ja liiallisen hallinnollisen taakan välttäminen, digitaalisen ekosysteemin kehitykseen vaikuttavat tekijät sekä ulkomaisten investointien edistäminen ovat turvallisuuspoliittisten ja kansalaisyhteiskunnan näkökulmien rinnalla työryhmätyön kannalta merkityksellisiä kokonaisuuksia.

TYÖ- JA ELINKEINOMINISTERIÖ
PL 32 (Aleksanterinkatu 4)
00023 Valtioneuvosto • Puh. 029 506 0000
Faksi (09) 1606 2160 • www.tem.fi

ARBETS- OCH NÄRINGSMINISTERIET
PB 32 (Alexandersgatan 4)
00023 Statsrådet • Tfn 029 506 0000
Fax (09) 1606 2160 • www.tem.fi

MINISTRY OF EMPLOYMENT AND THE ECONOMY
P.O. Box 32 (Aleksanterinkatu 4)
FI-00023 Government • Tel + 358 29 506 0000
Fax + 358 9 1606 2160 • www.tem.fi

TEM:n lausuma kohdistuu mietinnön tietoliikennetiedustelua koskeviin johtopäätöksiin ja kehittämisehdotuksiin. Tältä osin TEM yhtyy liikenne- ja viestintäministeriön (LVM) eriävään mielipiteeseen sen 4. kohdan (Verkkovalvonnalla voi olla merkittäviä vaikutuksia yritystoimintaan) osalta. Kohdassa on todettu, että tietoliikennetiedustelulla ja sen toimivaltuuksilla voi myös olla negatiivisia vaikutuksia elinkeinoelämän kilpailukykyyn ja investointien suuntautumiseen. Esimerkiksi pääministeri Stubbin hallitusohjelmassa on asetettu tavoitteeksi kehittää Suomea kansainväliseksi dataliikennekeskukseksi, jolloin tavoitteen toteutumisen kannalta kysymys on Suomen edellytyksistä pärjätä kilvassa ulkomaisista investoinneista. Pääministeri on myös todennut, että kyberturvallisuutta koskevaa lainsäädäntöä tullaan tarkastelemaan seuraavassa hallitusohjelmassa ja seuraavalla hallituskaudella.

TEM katsookin, että aiheen suuren elinkeinopoliittisen ja muun yhteiskunnallisen merkityksen vuoksi vasta virkamiestyöryhmää laaja-alaisemman ja –pohjaisemman valmistelutyön kautta, johon osallistuvat varsinaisina jäseninä myös elinkeinoelämän edustajat, on mahdollista uskottavasti tarkastella, arvioida ja ottaa kantaa tietoliikennetiedustelun hyötyjen ja haittojen väliseen suhteeseen sekä tehdä sen pohjalta varsinaiset lainsäädännön kehittämistä koskevat johtopäätökset ja ehdotukset.

TEM:n nimeämänä tiedonhankintalakityöryhmän jäsenenä

Kari Mäkinen
henkilöstö- ja hallintojohtaja, valmiuspäällikkö

POLIISI
POLIISIHALLITUS

Lausunto ID-1555035541 1 (4)

16.12.2014 POL-2014-16707

Puolustusministeriö

Poliisijohtaja Tomi Vuoren lausuma tiedonhankintalakityöryhmän mietintöön

Puolustusministeriö asetti 13.12.2013 nyt mietintönsä jättävän työryhmän, jonka tehtäväksi asetettiin Suomen lainsäädännön kehittäminen erityisesti turvallisuusviranomaisten tiedonhankintaa koskevan lainsäädännön osalta. Tavoitteeksi asetettiin se, että Suomessa pyrittäisiin huolehtimaan paremmin kansallisesta turvallisuudesta erityisesti tietoverkoissa esiintyvien uhkien torjumiseksi. Työryhmän kokoonpanoon kuului sekä sisäisen että ulkoisen turvallisuuden keskeisten viranomaisten edustajat samoin kuin niiden muiden ministeriöiden edustajat, joille valtioneuvoston toimialajaossa kuuluu työryhmän toimeksiannon alan asioita.

Viime vuosien turvallisuuskehitystä on leimannut perinteisen sotilaallisten ja siviiliuhkien välisen rajanvedon hämärtyminen. Suomessa tämä ilmenee muun muassa siinä, että käyttöön on otettu laaja-alainen turvallisuuskäsitys. Erityisesti tietoverkkoihin kohdistuvien uhkien osalta on ainakin alkuvaiheissa usein mahdotonta sanoa, kumman luonteisesta uhasta on kysymys. On hyvin tärkeää, että turvallisuusviranomaisten tilannekuva muodostuu riittäväksi, vaikka liikuttaisiin perinteisen uhkamallijaon ulkopuolella, harmaalla alueella.

Työryhmän työn oli tarkoitus kohdistua nimenomaan tietoverkkouhkiin, joita on myös kutsuttu kyberuhiksi. Työryhmän työn kanssa osittain päällekkäisenä työnä pohdittiin ministeri Päivi Räsäsen asettamassa hankkeessa Suojelupoliisin hallinnollista asemaa ja toimivaltuuksia. Siltä osin kuin nyt esillä olevan työryhmän työssä päädyttiin myöhemmässä vaiheessa pohtimaan laajemminkin tietoverkkoihin kuulumattomia ulkomaantiedusteluvaltuuksia, katson, että olen ollut sidottu edellä mainitun sisäministeriön hankkeen lopputulokseen erityisesti siitä syystä, että poliisin edustajana tuossa ryhmässä oli esimieheni poliisiylijohtaja Mikko Paatero, ja myös siksi, ettei asia kuulunut tämän työryhmän alkuperäiseen toimeksiantoon.

Digitalisaatio on yhteiskunnan eri toiminnot läpitunkevaa. Samalla kun palvelut siirtyvät tietoverkkoihin, siirtyvät sinne valitettavasti myös uhat. Kehitys on kuitenkin väistämätöntä. Asiantuntijakuulemisissa on tuotu vahvasti esille toisaalta tarve turvata ihmisten, yritysten ja laajemminkin koko yhteiskunnan toimintaympäristö tietoverkoissa olevilta uhilta, mutta toisaalta on

POLIISIHALLITUS
Vuorikatu 20 A, PL 302, 00101 HELSINKI
kirjaamo.poliisihallitus@poliisi.fi
Puh. +358 295 480 181, Faksi +358 295 411 780
poliisi.fi

myös korostettu viestinnän vapauden tärkeyttä. Tehtävänanto on siten äärimmäisen ajankohtainen, mutta samalla hyvin vaikea. Lopputuloksena tulisi olla järjestelmä, jolla perusoikeudet otetaan huomioon, mutta jolla turvattaisiin kaikkia niin sisäisen kuin ulkoisen turvallisuuden uhilta.

Työryhmän toimeksianto koskee sisäministeriön hallinnonalalla lähtökohtaisesti vain poliisia, Suojelupoliisi siihen mukaan luettuna. Oikeusministeriö ja sisäministeriö asettivat 12.3.2007 toimikunnan (esitutkinta- ja pakkokeinotoimikunta), jonka tehtäväksi annettiin esitutkintalain, pakkokeinolain ja poliisilain kokonaisuudistuksen valmistelu. Erityistä huomiota oli määrä kiinnittää mm. etsinnän toimittamiseen tietoverkoissa tai tietoverkon kautta. Varsinaisena painopistealueena ei sen sijaan ollut poliisin ja muiden lainvalvontaviranomaisten tiedonhankinta tietoverkoissa. Asiasta käytiin toimikunnassa kyllä keskustelua, mutta vasta tuon mietinnön (Oikeusministeriö, Komiteanmietintö 2009:2) 17.4.2009 tapahtuneen jättämisen jälkeen teknisen ja yhteiskunnallinen kehitys on tehnyt ilmeiseksi, että asiaan pitää nyt määrätietoisesti paneutua. Allekirjoittanut oli toimikunnan jäsenenä ainoana nyt mietintönsä jättävän työryhmän jäsenistä. Uusi esitutkintalaki, pakkokeinolaki ja poliisilaki tulivat voimaan vuoden 2014 alussa. Poliisin nykyinen - Suojelupoliisi mukaan luettuna - salainen tiedonhankinta perustuu tähän lakipakettiin.

Nyt mietintönsä jättävän työryhmän työn osalta totean, että poliisissa ymmärretään laajemminkin hyvin ne perusteet, joiden johdosta työhön on puolustusministeriön hallinnonalalla ryhdytty. Suojelupoliisin tiedonhankintatarpeiden uudistamiselle, siltä osin kuin ne poikkeavat muun poliisin tilanteesta, on niin ikään hyvät perusteet. Vaikka sisäisellä ja ulkoisella turvallisuudella on selkeästi erottaviakin piirteitä, on viime kädessä kyse kuitenkin kokonaisuudesta, jota voidaan jäsentää laajan turvallisuuskäsityksen pohjalta. Työryhmässä tehdyn työn perusteella näyttää siltä, että asian ratkaisumallit saattavat olla lainsäädännöllisesti erilaisia poliisin ja puolustusvoimien kohdalla. Tämä koskee myös osaa Suojelupoliisin tehtävistä. Kysymyksenasettelu johtuu siitä, että tietoverkkouhissa on pääsääntöisesti - joskaan ei aivan aina - kyse epäillyistä rikoksista. Poliisi on rikostorjunnan yleistoimivaltainen viranomainen.

Turvallisuudesta vastaavilla viranomaisilla on täysin perusteltu tarve saada tietoverkoista tietoa, joka liittyy niiden toimialaan kuuluvien uhkien torjuntaan. Virustorjunnalla tai vastaavilla sinänsä täysin välttämättömillä teknisillä keinoilla ei tietoverkkouhkia voida kokonaan torjua. Itse asiassa niiden jälkeen jää jäljelle kaikkein vakavimmat uhat. Suomi ei voi kansainvälisestikään olla tässä suhteessa poikkeus. Itsestään selvästi tässä liikutaan kuitenkin hyvin herkällä alueella, sillä kysymys on pohjimmiltaan siitä, missä raja viranomaisten tiedonsaannin ja yksityisyyden suojan välillä kulkee. Tämä asia ratkeaa valtiosääntöoikeudellisin perustein, jos ei haluta mennä niin pitkälle, että asiassa ryhdytään perustuslain muuttamiseen.

Jatkotyössä tulee mielestäni siis ottaa huomioon se, että puolustushallinnon ja poliisihallinnon tiedonsaantitarpeet voidaan mahdollisesti tyydyttää eri menettelytavoin. Suojelupoliisi on tässä mielessä vedenjakajalla; osa sen toimivaltuusvajeista voidaan täyttää yhdessä muun poliisin kanssa, osaa taas pitää tarkastella muussa yhteydessä. Poliisin toimialalla voitaisiin asiassa käsitykseni mukaan edetä pääsääntöisesti perustuslain 10 §:n lakivarauksen puitteissa tarkastelemalla asiaa normaalissa rikosprosessuaalisessa säädösvalmistelujärjestyksessä. Tämä on juuri se asia, joka tavallaan jäi esitutkinta- ja pakkokeinotoimikunnan työssä tekemättä, mutta jonka selvittämisen tarpeellisuuden erityisesti aivan viime aikojen kehitys on osoittanut olevan välttämätöntä. Korostettakoon, että toimikunnan työssä pyrittiin hyvin laajalti myös Suojelupoliisin tiedonhankintatarpeiden huomioon ottamiseen.

Kuten todettu, osa Suojelupoliisin toimivaltuuksista tulisi tarkastella erillään muun poliisin tarpeista. Tämä koskee tapauksia, joissa kyse on muusta kuin (laajasti ottaen) rikospohjaisesta tiedustelusta, kuten strategisten ilmiö- ja uhka-arvioiden tekemisestä. Näissä tilanteissa toimivaltuus ei voi perustua edellä kuvatulla tavalla rikokseen, koska niissä liikutaan lakivarauksen ulkopuolella. On joka tapauksessa aivan ilmeisestä, että myös siviilitiedustelulla - sotilastiedustelun lisäksi - tulee Suomessa olla valmiudet kuvattuun muuhun kuin rikosperusteiseen tiedonhankintaan.

Poliisille on tärkeätä, ettei rikostorjunnan kokonaisuutta pilkota, ja että toimivaltuudet ulottuvat kaikkiin poliisin toimialalla esiintyviin tilanteisiin. Työryhmän työn kuluessa on käynyt ilmeiseksi, että on yksityiskohtaisemmin selvitettävä, mihin poliisilain salaiset pakkokeinot tällä saralla riittävät, ja mihin uusia tiedusteluvaltuuksia konkreettisesti tarvittaisiin. Haluan kiinnittää huomiota siihen, ettei tiedonhankintalakityöryhmän mietinnön valmistelun yhteydessä ole voitu antaa riittävää painoarvoa rikosprosessin ja rikostorjunnan kokonaisuuden hahmottamiselle. Tiedustelu on eräs tiedonhankintakeino, ja poliisin näkökulmasta siten yksi osa rikostorjunnan kokonaisuutta.

Vaikuttaisi siten siltä, että poliisin tarpeet - tällä kertaa Suojelupoliisi siis osin pois lukien - tietoverkoissa tapahtuvan tiedonhankinnan tehostamiseksi voitaisiin tyydyttää perustuslain puitteissa pysyen tarkastelemalla rikosten tunnusmerkistöjä ja niiden valmistelutekojen kriminalisointia. Yhteiskunnan turvallisuutta vaarantavien rikosten kriminalisointia voitaisiin kenties laajentaa terrorismirikosten tapaan. Joissakin valmistelurikoksissa on kriminalisoitu suunnittelu, rekrytoiminen ja vastaavat toimet, toisissa taas edellytetään konkreettisia tekoja, kuten erilaisten tavaroiden tai aseiden hankintaa taikka vastaavia toimia. On ilmeistä, että tällä tavoin voitaisiin lakivarauksen puitteissa pysyen turvata rikosperusteinen tiedonsaanti niissäkin tilanteissa, joissa epäilty rikos ei vielä kohdennu tiettyyn henkilöön (tuntematon uhka), mutta jossa alkuvaiheessa olevan rikoksen suunnittelusta

tai vastaavasta alkuteosta on sellaista näyttöä, että tiedonhankintaan voitaisiin antaa lupa.

Poliisin rikosperusteisella verkkorikostorjunnan tiedonhankinnan tehostamisella on kiire. Tämän tiedonhankinnan mahdollistavan lainsäädännön valmistelu, jolla siis katettaisiin myös osa Suojelupoliisin toimivaltuustarpeesta, tulisi voida aloittaa viipymättä.

Poliisijohtaja Tomi Vuori

Asiakirja on sähköisesti allekirjoitettu Aspo-asianhallintajärjestelmässä. Poliisihallitus 16.12.2014 klo 11.20. Allekirjoituksen oikeellisuuden voi todentaa kirjaamosta.

Liitteet -

Jakelu Puolustusministeriö

Tiedoksi Poliisiylijohtaja Mikko Paatero

Puolustusministeriö
Eteläinen Makasiinikatu 8
PL 31, 00131 HELSINKI

www.defmin.fi

ISBN: 978-951-25-2626-9 nid.
ISBN: 978-951-25-2626-6 pdf