Aalto-yliopisto
Perustieteiden korkeakoulu
Tietotekniikan koulutusohjelma

Irina Kitinprami

Suomi, tiedon turvasatama?

Diplomityö
Helsinki 4. maaliskuuta 2016

Valvoja: Professori Martti Mäntylä
Ohjaaja: VTT Nomi Byström

Aalto-yliopisto
Insinööritieteiden
korkeakoulu

Aalto-yliopisto, PL 11000, 00076 AALTO
www.aalto.fi

Diplomityön tiivistelmä

Tekijä Irina Kitinprami

Työn nimi Suomi, tiedon turvasatama?

Koulutusohjelma Tietotekniikka, Ohjelmistotuotanto ja -liiketoiminta

Pää-/sivuaine Ohjelmistotuotanto ja -liiketoiminta **Koodi** T3003

Työn valvoja prof. Martti Mäntylä

Työn ohjaaja(t) VTT Nomi Byström

Päivämäärä 4.3.2016 **Sivumäärä** 77 **Kieli** suomi

Tiivistelmä

Tutkimuksen aiheena on pohtia, voiko Suomesta tulla tiedon turvasatama eli millainen sijoittumisvaltio Suomi on verkkotietopalveluja tarjoaville yrityksille. Tutkimuskohteena on tietosuojaan ja tietoturvaan vaikuttava lainsäädäntö verkkotietopalveluja tarjoavien yritysten näkökulmasta. Tutkimuksen tarkoituksena on selvittää, miten erityisesti vireillä olevat lainsäädäntöuudistukset: tietosuoja-asetus, NIS-direktiivi sekä kansallinen verkkotiedustelulainsäädäntö mahdollisesti vaikuttavat verkkotietopalveluyritysten sijoittumispäätöksiin. Yksityisyydensuoja, turvallisuus ja toisaalta liiketoimintaan liittyvät kaupalliset tavoitteet ovat kaikki lainsäädäntöä ohjaavia tekijöitä, jotka usein ovat keskenään ristiriitaisia. Tutkimuksessa keskeistä on tarkastella, miten nämä päällekkäiset ja jopa eri suuntiin vievät intressit ovat sovitettavissa siten, että Suomi on houkutteleva sijoittautumismaan verkkotietopalveluyrityksille. Tutkimustuloksena todetaan, että Suomella on sinänsä hyvät mahdollisuudet tulla tiedon turvasatamaksi, mutta se edellyttää, että löydetään tasapaino kaikkien näiden kriteerien välille ja lainsäädännössä johdonmukaisesti pyritään tähän tavoitteeseen. Verkkotietopalveluyritysten kannalta on tärkeää, että sääntelyssä toteutuvat kustannustehokkuus, sääntelyn ennakoitavuus ja asiakkaiden luottamuksen turvaaminen siihen, että heidän tietojansa käsitellään turvallisesti ja tietosuoja säilyttäen.

Avainsanat tietosuoja, tietoturva, kyberturvallisuus, pilvipalvelu, yksityisyys, tiedustelu, tietosuojasääntely

Aalto University
School of Engineering

Aalto University, P.O. BOX 11000, 00076
AALTO
www.aalto.fi

Abstract of master's thesis

Author Irina Kitinprami		
Title of thesis Finland, Safe Harbor of Data?		
Degree programme Computer Science and Engineering		
Major Technology Law		**Code** 231251
Thesis supervisor proff. Martti Mäntylä		
Thesis advisor(s) VTT Nomi Byström		
Date 4.3.2016	**Number of pages** 77	**Language** Finnish

Abstract

The purpose of this research is to evaluate if Finland could become a safe harbor of data i.e. which kind of place Finland is to companies operating in the area of information transfer and cloud services. The focus of the research is in the privacy and data protection legislation from the perspective of those companies that provide services related to network data storing and transferring. In addition to the effective legislation there is three ongoing regulation initiatives: reform of data protection regulation, NIS directive and new Finnish data surveillance legislation initiative. The research aims to find out, how those pending regulation reforms will possibly affect to data network service companies' willingness to establish business in Finland. Privacy, security and on the other hand business related commercial aims are all such often conflicting factors that have an influence to new legislation. In this research it is essential to evaluate, how these overlapping and sometimes even contradictory interests can be combined so that Finland will be an attractive place to start business for companies providing network data services. The result of this research is that Finland has good possibilities to become a safe harbor of data, but it is possible only if it can be found a balance between privacy, security and commercial interests. From legislative viewpoint it also important that new legal reformation acts are consistent with this aim. For network data companies it is essential that legislation is cost-effective, foreseeable and will strengthen customers trust that processing of their data is secure and protects privacy.

Keywords data protection, data security, cyber security, cloud service, privacy, privacy legislation, surveillance

Alkusanat

Työ on tehty opinnäytteeksi Aalto-yliopiston perustieteiden korkeakoululle. Aiheen työhön sain OTK, FT, Ville Oksaselta, joka myös antoi vinkkejä työn sisällön ja rakenteen suunnittelussa. Työn valvojana toimi professori Martti Mäntylä. Työtä ohjasi VTT Nomi Byström. Kiitos kaikille heille arvokkaista neuvoista ja kannustuksesta sekä kaikesta ajasta, joka tämän työn tukemiseen ja tapaamisiin aina järjestyi.

Kiitos myös puolisolleni Lassille oikoluvusta ja kommenteista sekä uskon luomisesta työn valmistumiseen.

Helsingissä 4.3.2016

Irina Kitinprami

Sisällysluettelo

1 Johdanto

1.1 Tutkimuksen tausta

Kansainväliset Julian Assangen Wikileaksista ja Edward Snowdenin paljastuksista alkunsa saaneet tietourkintaskandaalit ja jatkuvasti yltyvä Eurooppaankin kohdistuva vakava terrorismi ovat lisänneet tarvetta kyberturvallisille tietoratkaisuille. Samanaikaisesti pitkään jatkunut taloudellinen taantuma on tuonut vaateen löytää uusia kilpailuvaltteja globalisoituvassa maailmassa. Yksi selkeä, uusi liiketoiminta-ala on kyberturvallisuus ja siihen liittyvät palvelut, kuten tiedon turvallinen siirtäminen ja käsittely. Tiedon jatkuva lisääntyminen ja siihen liittyvä voimistuva tarve suurten tietomassojen siirtämiseen ja säilytykseen on kasvattanut erilaisten verkkotietopalvelujen tarjontaa. Sekä palveluja tarjoavien yritysten että niiden asiakkaiden toiveena on tiedon säilyminen suojassa sivullisilta.

Profiloitumalla kyberturvallisuuden keskittymäksi valtion on mahdollista houkutella maahan investointeja ja uutta verkkotietopalveluihin liittyvää liiketoimintaa, eli saada yksi taloudellinen kasvutekijä lisää valtioiden välisessä taloudellisessa kilpailussa. Teknologian lisäksi toinen verkkotietopalveluihin ja tiedon suojaamiseen olennaisesti vaikuttava tekijä on tiedon siirtoon ja säilytykseen sovellettava lainsäädäntö. Jotta valtiosta voi muodostua kyberturvallisuuden keskittymä tai tiedon turvasatama, on kansallisen lainsäädännön tuettava tätä tavoitetta. Tällöin on huomioitava myös soveltuva eurooppaoikeus sekä kansainväliset sopimukset, joihin valtio on sitoutunut.

Suomi on yksi niistä valtioista, joista voi muodostua tällainen kyberturvallinen tietokeskittymä tai tiedonsiirron solmukohta. Tämän mahdollistaa moni eri tekijä. Suomi on ensinnäkin maantieteellisesti Yhdysvaltojen ja Länsi-Euroopan sekä Venäjän ja Kiinan välissä, mikä mahdollistaa valokuitukaapeleiden rakentamisen ja tietoyhteyksien solmupisteenä toimimisen. Suomessa on jo nyt olemassa erittäin hyvät idän ja lännen väliset runkoverkkoyhteydet, joita kilpailevilla mailla ei ole tarjota. Lisäksi pohjoinen sijainti ja kylmä ilmasto tekevät datasalien jäähdyttämisen huomattavasti halvemmaksi kuin kilpailevissa valtioissa. Suomesta löytyy myös teknologista osaamista kyberturvallisten järjestelmien ja huippuluokan

tietokapasiteettien rakentamiseen. Suomen houkuttelevuutta yritysten sijaintivaltiona lisää myös Suomen vakaus, vähäinen korruptio ja sotilaallinen liittoutumattomuus.

Markkinoiden kannalta digitaalisuus on yksi Suomen hallituksen viidestä kärkihankkeesta, mikä lisää myös kotimaista tarvetta verkkotietopalveluille ja tiedon turvalliselle säilytykselle ja käsittelylle. Tällä hetkellä Suomessa ja EU:ssa on vireillä muutama tietosuojaa ja kyberturvallisuutta koskeva lainsäädäntöhanke sekä -aloite. Laajamittaisesti Suomessa ei ole kuitenkaan tutkittu, miten tietosuojaa ja tietoturvaa koskeva lainsäädäntö vaikuttaa verkkotietopalveluja tarjoaviin, tietointensiivisiin yrityksiin ja voiko Suomesta olla tiedon turvasatamaksi tällaisille yrityksille.

1.2 Tutkimuksen tavoitteet, tutkimustehtävät ja tutkimuskysymykset

Suomen erityispiirteet kylmä, pohjoinen sijainti, teknologian osaaminen, sotilaallinen liittoutumattomuus ja hyvät tietoyhteydet mahdollistavat parhaimmillaan Suomen profiloitumisen verkkotietopalvelujen kuten erilaisten pilvipalvelujen ja tietoliikennepalvelujen kilpailukykyisenä sijaintivaltiona. Tämän tavoitteen saavuttaminen edellyttää, että myös lainsäädännöllä tuetaan verkkotietopalveluyritysten sijoittautumista Suomeen.

Tutkimuksen tarkoituksena on selvittää, millä edellytyksillä Suomeen saataisiin houkuteltua lisää verkkotietopalveluja tarjoavia yrityksiä. Mikä on lainsäädännön takaama tietosuojan ja tietoturvan taso Suomessa tällä hetkellä. Miten lainsäädäntöön suunnitteilla olevat muutokset vaikuttavat tietosuojaan ja tietoturvaan Suomessa ja miten verkkotietopalveluja tarjoavien yritysten toimintaedellytykset mahdollisesti muuttuvat? Onko yksityisyyden ja turvallisuuden välille löydettävissä tasapainoa, joka mahdollistaa verkkotietopalveluja tarjoavien yritysten sijoittumisen Suomeen? Voiko Suomesta tulla tiedon turvasatama?

1.3 Tutkimusmenetelmät ja -aineistot sekä tutkimusrajaukset

Tutkimuksessa keskitytään pääasiassa tulevien lainsäädäntöhankkeiden analysointiin, mutta siinä käsitellään myös nykyisin voimassa olevaa tietosuoja- ja tietoturvalainsäädäntöä erityisesti siitä näkökulmasta, miten ne vaikuttavat verkkotietopalveluyritysten toimintaan ja sijoittautumiseen Suomeen. EU:n

jäsenvaltioiden välisten tietosuoja- ja tietoturvalainsäädännön eroavaisuuksien ohella lainsäädäntötarkastelua kohdistetaan tutkimuksessa viranomaisten toimivaltuuksien laajuuteen eli erityisesti siihen, millä edellytyksillä viranomaisilla on pääsy erilaisiin tietosisältöihin ja oikeus suorittaa verkkotiedustelua. Vireillä olevista uusista lainsäädäntöhankkeista tutkimuksessa käsitellään parhaillaan EU:ssa neuvoteltavaa tietosuoja-asetusta ja kyberturvallisuuteen liittyvää NIS-direktiiviä sekä Suomessa valmistelussa olevaa verkkovalvontalainsäädäntöä.

Tutkimuksen ydinkysymys on tietosuojaa ja tietoturvaa koskevan lainsäädännön merkitys verkkotietopalveluja tarjoavien yritysten sijoittautumispäätöksiin, mistä syystä työn ulkopuolelle on tarkoitus rajata pelkästään yksityishenkilöitä koskevat yleiset yksityisyydensuojakysymykset, kuten viestinnän yksityisyys ihmisoikeutena. Työn ulkopuolelle rajataan myös yritystoiminnan yleisiä edellytyksiä koskeva pohdinta sekä verotusta koskeva lainsäädäntötutkimus, joista kumpikaan ei liity tietosuojaan tai tietoturvaan.

Verkkotietopalveluita tarjoavat yritykset eivät ole homogeeninen joukko, vaan kooltaan, palveluiltaan ja muilta erityispiirteiltään toisistaan poikkeava ryhmä yrityksiä. Sama koskee niiden asiakaskuntia, joissa voi olla yrityksestä ja tarjotuista palveluista riippuen hyvinkin erilaisia asiakkaita, kuten muita yrityksiä, valtio- tai kuntatoimijoita taikka kuluttaja-asiakkaita, tai niiden asiakaskunnat voivat koostua kaikista näistä edellä mainituista. Vastaavasti myöskään tietosuoja- tai tietoturvalainsäädännön vaikutukset eivät välttämättä ole täysin yhtenevät kaikille yrityksille. Pilvipalveluita tarjoavan yrityksen toimintaan saattaa liittyä erilaisia lainsäädännöllisiä haasteita kuin tiedonsiirtoa tarjoaviin yrityksiin. Verkkotietopalveluita tarjoavia yrityksiä tarkastellaan tässä tutkimuksessa kuitenkin yhtenäisenä joukkona, sillä yleisellä tasolla niiden toimintaa koskevat samat tietosuoja- ja tietoturvasäännökset.

1.4 Tutkimuksen sisältö ja rakenne

Tutkimus rakentuu kuudesta luvusta siten, että johdantoluvun jälkeen käsitellään ensin sitä, mitä tässä tutkimuksessa tarkoitetaan käsitteellä tiedon turvasatama. Näkökulmasta ja tarkastelutavasta riippuen tiedon turvasatama voi saada eri merkityksiä ja erilaisia painotuksia. Seuraavaksi luvussa pohditaan yleisesti verkkotietopalveluihin liittyviä tiedonhallinnan haasteita kuten heikosta tietosuojasta johtuvia verkkotietopalveluiden käyttöönoton esteitä. Luvun lopuksi keskitytään

pohtimaan sitä, mitkä lainsäädännölliset tekijät vaikuttavat yritysten sijoittautumispäätöksiin.

Tutkimuksen kolmas luku käsittelee tämänhetkistä tietosuoja ja tietoturvalainsäädäntöä verkkotietopalveluyrityksen näkökulmasta. Luvussa käydään läpi tämänhetkistä lainsäädäntöä sekä erityisesti verkkotietopalveluyritykselle lainsäädännössä asetettuja tietosuojaan ja tietoturvaan liittyviä vastuita. Luvun lopussa analysoidaan tietosuojalainsäädännön nykytilannetta erityisesti siltä kannalta, voidaanko Suomi jo nyt katsoa tiedon turvasatamaksi vai tarvitaanko tietosuojalainsäädäntöön jotakin oleellista muutosta.

Neljännessä luvussa tarkastellaan verkkotiedustelulainsäädännön nykytilaa Suomessa ja vertaillaan säädäntöä Ruotsin vastaavaan sääntelyyn. Viidennessä luvussa tarkastellaan lähemmin suunnitteilla olevia lainsäädäntöuudistuksia ja pohditaan uudistusten tuomia uhkia ja mahdollisuuksia verkkotietopalveluyritysten toiminnalle ja sijoittautumiselle Suomeen.

Kuudennen luvun tarkoituksena on vastata keskeisiin johdannossa esitettyihin tutkimuskysymyksiin. Viimeinen eli seitsemäs luku koostuu kokoavista näkökulmista. Luvussa pohditaan muun muassa tulevaisuudessa tehtävissä tietosuojaan- ja tietoturvaan liittyvissä sääntelyuudistuksissa huomioitavia seikkoja erityisesti siitä näkökulmasta, millaiset mahdollisuudet Suomella on profiloitua tiedon turvasatamana nyt ja tulevaisuudessa.

2 Tiedon turvasatama

2.1 Tiedon turvasataman käsitteestä

Pohjoismaiden yhteinen, julkilausuttu tavoite on pyrkiä toimimaan korkean tietosuojan alueena[1]. Tämä mahdollistaa pilvipalveluiden sekä muiden verkkotietopalvelujen tarjonnan kasvun sekä kannustaa muun muassa datakeskusten perustamiseen, mikä on tärkeää erityisesti työllisyyden edistämisen näkökulmasta. Entinen viestintäministeri Kiuru on kannanotossaan todennut, että Suomen halutaan olevan sekä kyberturvallisuuden että digitaalisen talouden johtavia maita ja on tärkeää, että Suomen maine houkuttelee kansainvälisiä sijoittajia nyt ja tulevaisuudessa[2].

Tällä hetkellä maailmalla vallitsee tiedusteluvuodoista johtuva luottamuspula nykyisiin erityisesti Yhdysvalloissa toimiviin verkkotietopalveluyrityksiin[3]. Tämä on avannut Suomen vallattavaksi markkinatyhjiön, jossa kasvumahdollisuuksien voidaan olettaa olevan rajattomat.[4] Markkinoiden ottaminen haltuun edellyttää kuitenkin, että tänne onnistutaan houkuttelemaan merkittäviä haastajia Yhdysvalloissa toimiville palveluntarjoajille.[12] Tätä tavoitetta tukevat suunnitteilla olevat merikaapelihankkeet, joiden tarkoituksena on mahdollistaa tietointensiivisen teollisuuden toimiminen Suomessa.

Yksi taktiikka nostaa Suomen kiinnostavuutta kansainvälisten sijoittajien ja yritysten silmissä on lainsäädännön keinoin vahvistaa Suomen asemaa eräänlaisena tiedon turvasatamana. Toteutuessaan tämä tavoite tarkoittaa sitä, että Suomesta voi tulla keskeinen tietoliikenteen solmukohta vastaavasti kuin Suomi on pitkään ollut Euroopan ja Aasian väliselle lentoliikenteelle. Tällöin Suomessa taattaisiin lainsäädännöllä vahva tietosuoja ja kyberturvallisuus moninaisissa digitaalisissa

[1] Nordic Council of Ministers: Nordic Public Sector Cloud Computing - a discussion paper, 2012, http://www.norden.org/fi/julkaisut/julkaisut/2011-566.
[2] Kiuru, 2014, Network surveillance will not improve information security, s.1.
[3] Yksin Snowdenin tekemien paljastusten aiheuttaman kriisin on arvioitu maksaneen Yhdysvaltojen teollisuudelle noin 35 miljardia dollaria menetettyinä kassavirtoina.
[4] Suomalaisen tiedustelulainsäädännön suuntaviivoja, s.101.

ympäristöissä. Tiedon turvasatama tarkoittaisi siten sellaista valtiota, jonka kautta tietoliikenne voitaisiin ohjata ja tietoa käsitellä turvallisesti, ilman pelkoa tiedon joutumisesta kolmansien haltuun.

Tiedon turvasatama tai tietosuojan Sveitsi, kuten moni asiaa kutsuu, on käsite, joka saa erilaisia sisältöjä puhujasta ja asiayhteydestä riippuen. Jos asiaa ajatellaan ensisijaisesti kuluttajien luottamuksen turvaamisen kannalta, tiedon turvasatama on valtio, jossa kansalaisten yksityisyydensuoja turvataan vähintään kansainvälisten ihmisoikeussopimusten vaatimalla tavalla[5]. Viestinnän valvontaa koskevan lainsäädännön osalta tämä edellyttää ensinnäkin, että viestinnän valvonnasta säädetään aina selkeästi ja täsmällisesti julkisesti saatavilla olevassa laissa. Pääsääntöisesti kaikesta tiedustelutoiminnasta tulee tehdä etukäteisilmoitus valvonnan kohteelle. Lisäksi valvontatoiminnan on oltava oikeassa suhteessa tiedustelun tarkoitukseen ja sitä voidaan harjoittaa vain tiettyjen, nimettyjen viranomaisten toimesta.

Tiedustelutoiminnan harjoittaminen ihmisoikeuksia loukkaamattomasti edellyttää, että sillä pyritään saavuttamaan valtion tai sen kansalaisten näkökulmasta jokin oikeutettu tavoite. Tällaisia tavoitteita ovat Euroopan ihmisoikeussopimuksessa mainitut mahdolliset poikkeusperusteet yksityisyyden suojasta esimerkiksi kansallisen ja yleisen turvallisuuden takaaminen. Jotta tiedustelutoiminta täyttää myös objektiivisesti arvioiden ihmisoikeussopimusten takaaman yksityisyydensuojan tulee toimintaa valvoa riittävän tehokkaasti. Yksityisyyden suojan toteutumisen kannalta on suositeltavaa, että tiedusteluluvan myöntää ja tiedustelua valvoo julkisesti jokin puolueeton ja riippumaton viranomainen. Toiminnan asianmukainen ja riittävä valvonta edellyttää myös avointa tiedottamista valvontatoimista ja niiden laajuudesta.

[5] Ks tällaisesta tulkintatavasta lisää esimerkiksi kansainvälisiä sääntöjä ihmisoikeuksien noudattamisesta viestinnän valvonnassa, International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/. Säännöt on laadittu yhteistyöprojektissa, jota on johtanut Privacy International, Access ja Electronic Frontier Foundation. Työtä konsultoimassa on ollut yhteiskunnan, yksityisyydensuojan ja teknologian ammattilaisia, ja säännöt on allekirjoituksellaan hyväksynyt yli sata alan organisaatiota eri puolilta maailmaa.

Sekä kuluttajien yksityisyyden että verkkotietopalvelun tarjoajien näkökulmasta on tärkeää säilyttää viestinnän koskemattomuus. Tämä tarkoittaa sitä, että valtio ei saa tiedustelulainsäädännöllä pakottaa palvelujen tarjoajia tai laitteistojen tai ohjelmistotoimittajia rakentamaan valvonta- tai tarkkailumahdollisuutta omiin järjestelmiinsä, tai keräämään tai säilyttämään tietoja puhtaasti valtion viestinnän valvonnan tarkoituksiin. Puhtaasti yksityisyydensuojalähtöisessä määrittelyssä tiedon turvasatama on valtio, jossa tietojen säilyttämistä tai keruuta ei vaadita palveluntarjoajilta missään tilanteessa. Vastaavasti tällaisessa tiedon turvasatamassa lainsäädännöllä ei voida vaatia palveluntarjoajilta pakollista käyttäjätunnistusta, vaan jokaisella on oikeus ilmaista mielipiteensä nimettömästi.

Yhteenvetona tiedon turvasatama voi olla vain valtio, jonka harjoittama tiedustelutoiminta on tarkoin sääntöjen mukaisesti säännelty ja tätä sääntelyä myös noudatetaan. Tiukka peruskonsepti tällaiselle yksilön suojasta lähtevälle tiedon turvasatamalle on tiedoille ja pilvipalveluille turvallinen valtio, jossa tietosuojaa valvotaan aggressiivisesti eikä tietovakoilua sallita missään olosuhteissa. Viranomaisilla on pääsy tietoihin vain vakavien rikosten selvittämiseksi, mikä on toteutettu täysin kaksipuolisella läpinäkyvyydellä. Tietopyyntöjen ehtona on, että ne on aina käsiteltävä oikeudessa.[6] Käsitteellä tiedon turvasatama tarkoitetaan tällöin tiivistetysti valtiota, jossa tiedonvaihto turvataan viranomaisilta. Ongelmallista tällaisen käsitteen käytössä on se, että siinä ei huomioida digitaalisen ympäristön eri toimijoita ja niiden toisistaan ehkä poikkeaviakin tarpeita. Tällaisia toimijoita ovat esimerkiksi verkkotietopalveluiden tuottajat, heidän asiakkaansa ja näiden asiakkaiden palveluja käyttävät kuluttajat.

Valtion suorittaman tiedustelun lisäksi tiedon salassapysymiseen kohdistuu myös muita uhkia kuten tietomurrot ja tiedon käsittelyssä tapahtuvat tietovuodot. Tästä syystä tiedon turvasatama -käsitteen tulee kattaa laajasti sekä tietosuoja että tietoturva. Sekä verkkotietopalveluita tarjoaville yrityksille että erityisesti heidän kuluttaja- ja yritysasiakkailleen on tärkeää voida suojata käsiteltävä tieto kaikenlaisilta tietomurroilta ja tietovuodoilta. Luottamuksen ja sitä myötä asiakaskunnan ja liikevaihdon syntyminen verkkotietopalveluyrityksille edellyttää vahvaa lainsäädännön takaamaa kyberturvallisuutta.

[6] Oksanen 2014, s.20.

Oma lukunsa on tiedon turvasatama -käsitteen ajatteleminen tietomurtautujan tai -vuotajan näkökulmasta. Tiedon turvasatamaksi katsotaan tällöin valtio, jossa tietoturvahyökkäykset ja muut tietojen luvattomaan hankkimiseen tähtäävät teot on tiukasti ja kattavasti kriminalisoitu ja teoista säädettävät rangaistukset ovat sellaisia, että ne ehkäisevät tietoturvaan kohdistuvaa rikollista toimintaa tehokkaasti. Tällaisessa valtiossa rikollista toimintaa myös valvotaan ja selvitetään laajasti ja onnistuneesti runsain resurssein.

Hyvä kysymys on, onko kaikista näkökulmista katsottuna täysin tietoturvallisen valtion olemassaolo edes mahdollista. Todennäköisesti vastaus kysymykseen on kielteinen, sillä tiedon siirtoon ja käsittelyyn kohdistuva toiminta on tavallisesti valtioiden rajat ylittävää. Lisäksi tällaiseen toimintaan soveltuvat usein toimijoista ja käsittelypaikoista riippuen eri valtioiden säännökset samanaikaisesti. Toisaalta myös kyberturvallisuus sisältää erilaisia asioita kuten tiedon turvallisuus, tiedon siirron ja tietoverkkojen turvallisuus, yksityisyydensuoja ja eri toimijoiden turvallisuus. Tietosuojaan ja tietoturvaan voidaan puuttua valtiollisesta esimerkiksi kansalliseen turvallisuuteen liittyvistä tavoitteista tai sitten puuttuminen voi olla tietomurron tapaista rikollista toimintaa.

Tässä tutkimuksessa käsitteellä tiedon turvasatama tarkoitetaan valtiota, jonne verkkotietopalveluja tarjoavan yrityksen kannattaa sijoittautua. Tämä edellyttää lainsäädännöltä sitä, että tietosuoja toteutuu kuluttajanäkökulmasta ja että tietoturva on taattu myös yritysten näkökulmasta riittävällä tasolla. Asiakkaiden luottamuksen lisäksi yritysten toimintapäätöksiin vaikuttavat myös tietosuojan ja tietoturvallisuuden kustannustekijät, mikä osaltaan monimutkaistaa sääntelyn kehittämistä.

2.2 Verkkotietopalveluihin liittyvät tiedonhallinnan haasteet

Syyskuussa 2012 Euroopan unionin komissio julkaisi poliittisen kannanoton pilvipalveluiden käytön edistämisestä Euroopassa[7]. Komission strategisena tavoitteena on mahdollistaa pilvipalveluiden käyttöönotto kaikilla sellaisilla talouden aloilla, joilla tieto- ja viestintäkuluja voidaan leikata ja joilla pilvipalvelut yhdessä uusien

[7] KOM(2012) 529 lopullinen, Komission tiedonanto Euroopan parliamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Pilvipalveluiden potentiaali käyttöön Euroopassa.

digitaalisten toimintamallien kanssa voivat tukea työllisyyttä, kasvua ja tuottavuutta Euroopassa. Kannanotossa analysoidaan pilvipalveluihin liittyviä haasteita ja esitetään tärkeimmät kiireelliset toimenpiteet, joilla palveluiden käyttöä voidaan Euroopan Unionin taholta edistää komission strategian mukaisesti.

Komissio nostaa kannanotossaan esiin kolme keskeistä toimenpiteitä kaipaavaa osa-aluetta: digitaalisten sisämarkkinoiden hajanaisuus, sopimusongelmat sekä standardiviidakko. Samat haasteet koskevat pilvipalveluiden lisäksi myös muita verkkotietopalveluita.[8]

Komission mukaan pilvipalveluiden potentiaalisten käyttäjien ja palveluntarjoajien suurimpia huolenaiheita olivat erilaisista kansallisista oikeudellisista puitteista johtuva digitaalisten sisämarkkinoiden hajanaisuus sekä epätietoisuus sovellettavasta lainsäädännöstä ja digitaalisen sisällön ja datan sijainnista. Useille lainkäyttöalueille ulottuvia palveluja ja käyttötapoja on monimutkaista hallinnoida. Kysymys liittyy erityisesti luottamukseen ja varmuuteen tietosuojan, sopimusten, kuluttajansuojan ja rikosoikeuden alalla.[9] Käytännössä tämä tarkoittaa sitä, että kasvattaakseen asiakaskuntaansa verkkotietopalvelu tarvitsee asiakaskunnan luottamusta, mikä taas edellyttää lainsäädännöltä selkeyttä sekä sisällön että soveltamisalan suhteen. Lisäksi lainsäädännöllä on turvattava tiedon luottamuksellinen käsittely ja siirto siten, että siihen ei ole pääsyä kolmansilla. Tämä edellyttää, että kyberrikollisuus saadaan lainsäädännöllisin keinoin estettyä ja vähimmilläänkin minimoitua aiheutuneet vahingot.

Sopimusongelmat liittyvät erityisesti huoleen datan saatavuudesta ja siirrettävyydestä sekä muutoshallinnasta ja datan omistajuudesta. Kuluttajille ja palveluntarjoajille on epäselvää, miten vastuu ja korvaukset jakautuvat ongelmatapauksissa, mitkä ovat käyttäjien oikeudet järjestelmäpäivityksissä, joista päättää yksipuolisesti palveluntarjoaja, kuka omistaa pilvipalveluissa luotavan datan ja mitkä ovat riidanratkaisumenetelmät.[10] Tämä on erityisesti verkkotietopalveluiden vastuulla oleva

[8] KOM(2012) 529 lopullinen, Komission tiedonanto Euroopan parliamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Pilvipalveluiden potentiaali käyttöön Euroopassa, s.5-6.
[9] KOM(2012) 529 lopullinen, Komission tiedonanto Euroopan parliamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Pilvipalveluiden potentiaali käyttöön Euroopassa, s.6.
[10] Sama.

asia, sillä ne määrittelevät lopulta ehdot, joilla palveluita tarjotaan. Kansallisilla ohjeistuksilla ja erilaisilla mallilausekkeilla mahdollisia sopimusepäselvyyksiä voidaan kuitenkin pyrkiä poistamaan.

Standardien osalta haasteet liittyvät erityisesti standardien liialliseen määrään sekä epävarmuuteen siitä, mitkä standardit takaavat dataformaattien riittävän yhteentoimivuuden tiedon siirrettävyyden mahdollistamiseksi. Lisäksi epätietoisuutta on siitä, saavatko henkilötiedot riittävää suojaa ja ongelmana nähdään myös tietojen luvaton käyttö ja suojautuminen verkkohyökkäyksiltä.[11] Nämä epätietoisuudet ovat myös osaltaan seurauksena lainsäädännön ja soveltamisalan epäselvyyksille[12]. Useiden toisistaan poikkeavien tietosuojasäännösten soveltuminen samaan tietoon samanaikaisesti tekee lopulta sekä asiakkaan että palveluntarjoajan epävarmaksi tietosuojan toteutumisesta todellisuudessa.

Komission kannanotossa korostetaan, että yksi vakavimpia pilvipalveluiden käyttöönoton esteitä liittyy tietosuojaan, mistä syystä kannanotossa pidetään erittäin tärkeänä, että Euroopan unionin tietosuojalainsäädäntöä harmonisoiva tietosuoja-asetus tulee voimaan mahdollisimman nopealla aikataululla.[13] Toteutuessaan tietosuoja-asetus tulee kaventamaan ja poistamaan eroja kansallisten tietosuojalakien välillä. Täysin yhtenevää sääntely ei tule jäsenvaltioissa uudistuksenkaan jälkeen olemaan johtuen kansallisesta harkintavallasta.

Pilvipalveluratkaisuja kohtaan tunnetun luottamuksen kasvattamiseksi tarvitaan komission mukaan tukitoimenpiteiden ketjua. Nämä komissio tiivistää kannanotossaan kolmeen päämäärään. Ensinnäkin Euroopan unionin laajuinen standardien sertifiointi, mikä varmistaa palveluiden yhteentoimivuuden sekä tietojen siirtomahdollisuuden ja palautettavuuden eli riippumattomuuden yhdestä palveluntarjoajasta. Standardeihin voidaan myös viitata sopimusehdoissa, jolloin palveluntarjoajat ja käyttäjät voivat varmistua sopimuksen juridisesta pätevyydestä ja luotettavat tarjoajat ovat helposti tunnistettavissa.[14]

---

[11] Sama.
[12] Ks. soveltamisalan epäselvyyksistä esim. Hon, w Kuan - Hörnle, Julia - Millard, Christopher: Which Law(s) Apply to Personal Data in Clouds? Teoksessa Cloud Computing Law (toim. Millard, Christopher), Oxford University Press 2013, s.231-244.
[13] KOM(2012) 529 lopullinen, s.8.
[14] Voutilainen, Tomi – Galkin, Denis, s. 372.

Toinen komission kannanotossaan kertomista ja sittemmin myös toteutuneista päämääristä oli luoda turvalliset ja oikeudenmukaiset mallisopimusehdot, joissa selkeästi todetaan osapuolten oikeudet ja velvollisuudet. Parhaiden käytäntöjen tukeminen ja levittäminen mallisopimuslausekkein edesauttaa luottamusta pilvipalveluihin edistäen siten niiden käyttöönottoa.[15]

Kolmantena päämääränä komissio mainitsee kannanotossaan eurooppalaisen pilvipalvelukumppanuuden perustamisen, joka muodostaa katto-organisaation vastaaville jäsenvaltiotason aloitteille. Organisaation tavoitteena on kartoittaa pilvipalveluiden käyttäjien vaatimukset ja varmistaa, että kaupallinen pilvipalvelutarjonta Euroopassa vastaa näitä eurooppalaisia tarpeita.[16]

Verkkotietopalveluihin liittyviä tietosuojariskejä on käsitelty myös WP 29 tietosuojaryhmässä, joka on perustettu unionin henkilötietodirektiivin (95/46/EY) 29 artiklalla. Tietosuojatyöryhmän mukaan pilvipalveluiden käyttöönotto voi johtaa useisiin tietosuojaan liittyviin riskeihin, kuten puutteelliseen henkilötietojen valvontaan ja riittämättömiin tietoihin siitä, miten ja missä henkilötietoja käsitellään tai käsitelläänkö niitä alihankintana. Henkilötietojen käsittelyn avoimuus ei tällöin toteudu lainsäädännön vaatimalla tavalla.[17]

Tietosuojatyöryhmä korostaa suosituksissaan asiakkaan vastuuta henkilötietojen käytön valvonnasta. Suosituksena on, että asiakas arvioi verkkotietopalvelujen hankintavaiheessa pilvipalveluiden käyttöön ja henkilötietojen käsittelyyn liittyvät riskit. Näin ollen asiakkaan on valittava palveluntarjoaja, joka takaa EU:n tietosuojalainsäädännön noudattamisen. Tietosuojatyöryhmän mukaan palvelusopimuksessa on lisäksi annettava riittävät takeet teknisistä ja organisatorisista tietosuojatoimenpiteistä. Asiakkaan on myös varmistettava, voiko verkkotietopalvelujen tarjoaja taata kaikkien kansainvälisten tiedonsiirtojen laillisuuden.[18]

[15] KOM(2012) 529 lopullinen, s.12-13.
[16] KOM(2012) 529 lopullinen, s.14.
[17] 01037/12/FI, WP 196. Lausunto 5/2012 tietotekniikan resurssipalveluista.s.2.
[18] Sama.

Tietosuojatyöryhmän antaman lausunnon mukaan verkkotietopalvelujen tarjoamisen on perustuttava etenkin turvallisuuteen, avoimuuteen ja asiakkaiden oikeusvarmuuteen.[19]

2.3 Yritysten sijoittaumispäätösten taustaa

2.3.1 Sijoittautumisharkintaan vaikuttavat seikat

Pilviteknologioiden kasvava hyödyntäminen ja erilaisten verkkotietopalveluiden yleistyminen on osaltaan aiheuttanut ICT-palveluiden toimintamallissa merkittävän muutoksen. Yritysten toiminta ei ole enää sidottu tiettyyn maantieteelliseen alueeseen tai valtioihin, sillä maailmanlaajuisessa tietoverkossa operointi mahdollistaa sijainnin valinnan sen mukaan, missä yrityksen kulloinkin hallitsema tieto fyysisesti sijaitsee.[20] Käytännössä nämä uudet verkkotietopalveluihin perustuvat toimintamallit ovat johtaneet siihen, että yritykset ovat herkästi sijoittautuneet useisiin eri valtioihin samanaikaisesti.

Sijoittautuminen ja yritysrakenne ovat verkkotietopalveluita tarjoavan yrityksen välineitä ennakoida toimintaansa kohdistuvaa oikeudellista riskiä. Sijoittautumisratkaisussa harkitaan erityisesti sijoittautumisvaltion lainsäädännön soveltumista sekä sen aiheuttamia positiivisia ja negatiivisia vaikutuksia yrityksen liiketoiminnalle. Sijoittautumisvaltion valinta sekä yritysrakenne auttavat hallitsemaan liiketoiminnasta mahdollisesti aiheutuvia oikeudellisia ja taloudellisia vastuita sekä velvoitteita. Tätä suunnittelua kutsutaan forum shopping -ilmiöksi.[21]

Sijoittautumispäätöksessä painavat erityisesti liiketaloudelliseen asemaan vaikuttavien oikeudellisten riskien ennakoitavuus sekä lainsäädännön soveltamiskäytäntöjen ja -säännösten läpinäkyvyys. Lainsäädännön osalta yritykset tyypillisesti arvoivat kolmea asiaa:

1) Soveltamiskynnyksen määräytyminen eli mikä piirre yrityksen toiminnassa aiheuttaa sijoittautumisvaltion lainsäädännön soveltumisen.
2) Sijoittautumisvaltion lainsäädännön sisältö verrattuna erityisesti vaihtoehtoisten sijoittautumisvaltioiden lainsäädäntöön.

[19] Sama.
[20] Kaho, Julå, Kara ja Iike, 2014, 2014, s 2.
[21] Sama

3) Lainsäädännön tosiasiallinen ulottuvuus eli vaikutus yrityksen toimintaan sijoittautumisvaltiossa ja sen ulkopuolella.[22]

2.3.2 Lain soveltamisalue

Verkkotietopalvelulle on tyypillistä, että tietoa käsitellään useassa eri yrityksessä laitteistoilla, jotka sijaitsevat useassa eri maassa. Käsiteltävä tieto puolestaan koskee usein monen valtion kansalaisia ja useassa maassa vakituisesti asuvia yksityisiä henkilöitä. Näiden erityispiirteiden seurauksena verkkotietopalveluja tarjoavaan yritykseen soveltuu samanaikaisesti useita eri soveltumisperiaatteiden mukaisesti valikoituvia säännöksiä. Lainsäätäjän määräämät soveltamissäännökset ratkaisevat sen, missä laajuudessa ja mihin tahoihin lainsäädännössä asetetut velvoitteet kohdistuvat, jotta lainsäädännöllä tavoiteltava suoja toteutuu parhaalla mahdollisella tavalla. Epäselvyys soveltamissäännöissä vähentää yrityksen toiminnan ennakoituvuutta, mikä puolestaan vaikuttaa kielteisesti yrityksen päätökseen sijoittautua soveltamisvaltioon. Selkeillä Suomen lain soveltumista koskevilla linjauksilla on todennäköisesti merkittävä vaikutus Suomeen datakeskusinvestointeja tai verkkopalveluiden tarjoamista suunnittelevan yrityksen sijoittautumispäätöksiin.[23]

Yritysten tavoittelemaa lainsäädännön ennakoitavuutta lisää rinnakkaisten lainsäädäntöjen huomioiminen myös lakitekstitasolla sekä lainsäädännön soveltamiskynnysten yhdenmukaisuus kansallisella ja ylikansallisella tasolla. Soveltamissääntöjen selkeys korostuu verkkotietopalveluja tarjoavien yritysten toiminnassa, sillä tietojen lähde- tai kohdevaltioiden lainsäädännöissä saattaa olla ristiriitoja yrityksen sijaintivaltion lainsäädännön kanssa. Tietoja voidaan esimerkiksi käsitellä Suomessa, vaikka rekisterinpitäjänä on ulkomainen taho tai tiedot kohdistuvat vakituisesti ulkomailla asuviin yksityishenkilöihin. Kansallisen lain soveltamisalaa määritettäessä tulisikin löytää tarkoituksenmukainen tasapaino yritysten velvollisuuksien ja niiden hallittavuuden kohtuullisuuden sekä yksityisyydensuojan riittävän tehokkaan turvaamisen välille.[24]

[22] Kaho, Julå, Kara ja Iike, 2014, 2014, s 2-3.
[23] Kaho, Julå, Kara ja Iike, 2014, 2014, s 4-5. Ks. esimerkkinä henkilötietolain ja tietoyhteiskuntakaaren soveltamissäännöt.
[24] Kaho, Julå, Kara ja Iike, 2014, 2014, s 5-6.

Soveltamisalan rajauksilla lainsäätäjä voi kohdentaa lain tarjoaman oikeussuojan halutuille tahoille ja samalla rajata soveltamisalan ulkopuolelle sellaiset yritykset, joiden toiminta ei välittömästi vaikuta suojattavien oikeuksiin. Verkkotietopalvelua tarjoavien yritysten sijoittautumiseen Suomeen vaikuttaa olennaisesti se, kuinka laajasti Suomen lakeja sovelletaan yrityksen kansainväliseen toimintaan. Voiko kansainvälinen yritys esimerkiksi sijoittaa datakeskuksensa Suomeen ilman, että Suomen lakia sovelletaan henkilötietoihin, vaikka niitä käsitellään henkilötietolain tarkoittamalla tavalla? Tiedoilla sinänsä ei välttämättä ole palvelinkeskuksen sijaintia lukuun ottamatta mitään liityntää Suomeen.[25] Voimassa olevan tietosuojadirektiiviin (95/46/EY) perustuvan sääntelyn mukaan vastaus kysymykseen on sekä Suomen että muiden Euroopan Unioniin kuuluvien valtioiden osalta epäselvä ja riippuvainen lakiteknisistä tekijöistä, jotka tuskin edustavat kansallisille säädöksille asetettuja tietosuojatavoitteita.[26]

Henkilötietodirektiivin 4 artiklan mukaan sovellettava jäsenvaltion lainsäädäntö määräytyy kolmen eri periaatteen mukaisesti: rekisterinpitäjän toimipaikka, kansainvälisen julkisoikeuden säännöt ja henkilötietojen käsittelyyn käytettävien välineiden sijainti. Lisäksi artiklan 17.3 mukaisesti tietojen käsittelijän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi sijaintivaltionsa lainsäädännön asettamien vaatimusten mukaisesti. Tämä johtaa esimerkiksi pilvipalveluiden osalta siihen, että tiedon suojaamiseksi on sovellettava sekä tiedon käsittelyä tilaavan rekisterinpitäjän että tiedonkäsittelijänä toimivan verkkotietopalveluyrityksen sijaintivaltion suojaussääntöjä. Jos käsittelijöitä on useita eri valtioissa, tulee tiedon käsittelyyn sovellettavaksi näiden kaikkien valtioiden suojaussäännöt. Tällainen on esimerkiksi tilanne, jossa tietoa liikutellaan tai säilytetään useissa eri valtioissa sijaitsevissa datakeskuksissa.

Asian tekee vaikeaksi se, että suojausvaatimukset eri EU-jäsenmaissa eivät ole keskenään samanlaiset. Esimerkiksi Iso-Britanniassa vaatimus on yksinkertaisesti toteuttaa tarvittavat tekniset ja organisatoriset keinot tietojen suojaamiseksi, kun taas

[25] Kaho, Julå, Kara ja Iike, 2014, 2014, s 6-7. Henkilötietolaki tulee myös ulkomaisen yrityksen sovellettavaksi, jos sillä on palvelimia Suomessa. Ulkomainen verkkotietopalveluyritys, jolla on palvelinkapasiteettia Suomessa, joutuu henkilötietolain 4.2 §:n mukaan nimeämään Suomeen edustajan.

[26] Hon, w Kuan - Hörnle, Julia - Millard, Christopher: Which Law(s) Apply to Personal Data in Clouds? Teoksessa Cloud Computing Law (toim. Millard, Christopher), Oxford University Press 2013, s.231-244.

Italiassa on tarkat ja yksityiskohtaiset määritelmät tietojen suojaamiselle kuten pääsylle tärkeisiin salasanoihin ja säilytysmedioiden uudelleenkäyttöön.[27] Ristiriitatilanteissa noudatettavaksi tulee WP29 tietosuojatyöryhmän mukaan noudatettavaksi käsittelijän sijaintivaltion laki myös silloin, kun rekisterinpitäjän sijaintivaltion laki on vaatimuksiltaan tiukempi[28].

2.3.3 Yrityksen hallinnolliset velvollisuudet ja vastuut

Tietosuojaa ylläpidetään asettamalla yrityksille hallinnollisia velvollisuuksia. Tällaisia velvollisuuksia ovat esimerkiksi velvollisuus dokumentoida tiedon turvaamiseen liittyvien velvoitteiden toteuttaminen ja erilaiset tiedon salaamisvelvoitteet, kuten kielto siirtää henkilötietoja muuten kuin salatussa muodossa.

Samalla, kun tietosuojan avulla suojataan yksityisten henkilöiden ja oikeushenkilöiden tietojen luottamuksellisuutta, aiheutetaan väistämättä taloudellisia kustannuksia ja riskejä yrityksille, joille velvollisuuksia luodaan. Verkkopalveluita tarjoaville yrityksille ei ole Suomessa säädetty kansallisia, toimintaan nimenomaisesti kohdistuvia erityisvelvoitteita. Kansainvälisesti vertaillen tämä on Suomelle merkittävä etu. Yleiset toimialaliitännäiset velvoitteet määräytyvät tietosuoja, tietoturva- ja viestintälainsäädännön perusteella.[29]

Euroopan Unionissa tietosuoja- ja viestintälainsäädäntöä on yhdenmukaistettu useilla direktiiveillä, jotka on implementoitu osaksi kansallista lainsäädäntöä. Suomessa esimerkiksi tietosuojadirektiivi on implementoitu osaksi henkilötietolakia ja sähköisen viestinnän tietosuojadirektiivi (2002/58/EY) ja sähkökauppadirektiivi (2000/31/EY) osaksi tietoyhteiskuntakaarta.[30] Direktiivien sisällä jäsenvaltioilla on kuitenkin huomattavaa liikkumavaraa, direktiivien muodostaessa lähinnä lainsäädännöllisen kehikon[31]. Tästä on aiheutunut huomattavia eroavaisuuksia jäsenvaltioiden tietosuoja- ja viestintälainsäädäntöjen välille[32]. Euroopan Unionissa eroavaisuuksiin on

[27] Hon, w Kuan - Hörnle, Julia - Millard, Christopher, 2013, s.243-244.
[28] A29WP, Opinion 8/2010 on applicable law.
[29] Kaho, Julå, Kara ja Iike, 2014, s 7.
[30] sama.
[31] Hon, w Kuan - Hörnle, Julia - Millard, Christopher, 2013, s.220.
[32] European Commission: Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final Report 2010, s.16. ks. myös s.27-28.

havahduttu ja tavoitteena on yhtenäistää kansallista tietosuojalainsäädäntöä mittavalla tietosuojalainsäädäntöuudistuksella. Uudistuksen tavoitteena on säätää uusi tietosuoja-asetus, joka toteutuessaan harmonisoi ja yhdenmukaistaa EU:n sisäistä tietosuojasääntelyä.[33]

Lainsäädännön kansalliset eroavaisuudet on yksi tekijä, joka vaikuttaa yrityksen sijoittaumispäätöstä koskevaan harkintaan, koska sillä on selviä taloudellisia vaikutuksia. Laissa säädetyn tietosuojatason saavuttaminen ja ylläpitäminen aiheuttaa kahdentyyppisiä kustannuksia. Ensinnäkin tietosuojasääntely luo selvitys- ja koulutuskustannuksia ja toiseksi kustannuksia aiheutuu tietosuojan tason toteuttamisesta ja ylläpitämisestä. Suomen lain erityispiirteet ja poikkeamat kansainvälisesti tavanomaisesta sääntelystä aiheuttaa lisäkustannuksia molemmissa kategorioissa. Merkittävät lisävaatimukset ja -rajoitukset verrattuna kilpaileviin sijoittautumisvaltioihin nostavat erityisesti tietosuojan ylläpito- ja toteutuskustannuksia ja niiden voi olettaa vaikuttavan negatiivisesti yrityksen sijoittautumisharkintaan.[34]

Kansalliset erityispiirteet saattavat johtua muun muassa historiallisista syistä, Euroopan Unionin lainsäädännön tulkinnasta ja implementoinnista tai viranomaisen valvontakäytännöistä[35]. Huonoimmillaan erityispiirteet aiheuttavat epätarkoituksenmukaisia lisäkustannuksia, jotka vähentävät Suomen houkuttelevuutta verkkopalvelua tarjoavien yritysten sijaintivaltiona. Tietosuoja-asetuksen voimaantulo on toteutuessaan tehokas tapa yhtenäistää kansallista lainsäädäntöä ja poistaa tietosuojalainsäädännön kansallisia erityispiirteitä.[36] Toisaalta uudistuksen toteutumattomuus voisi olla Suomen paikka hyödyntää kansalliset erityispiirteensä ja muuttua houkuttelevammaksi sijaintimaaksi verkkotietopalveluyrityksille. Tietosuojalainsäädäntöä tulisi tällöin tarkastella myös yritysten liiketoimintaedellytysten luomisen kautta. Lisäksi yrityksille asetettavia hallinnollisia velvoitteita ja rajoitteita tulisi karsia siten, että ne ovat oikeassa suhteessa tavoiteltavaan tiedon suojaamistasoon nähden.

---

[33] Kaho, Julå, Kara ja Iike, 2014, s 7-8.European Commission: Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final Report 2010, s.16. ks. myös s.39-40.
[34] Kaho, Julå, Kara ja Iike, 2014, 2014, s 8.
[35] Kaho, Julå, Kara ja Iike, 2014, 2014, s 8.
Ks. henkilötietolaki 10 § esimerkkinä kansallisesta erityispiirteestä.
[36] Kaho, Julå, Kara ja Iike, 2014, 2014, s 8.

Henkilötietolaissa (523/1999) asetetaan hallinnollisia velvollisuuksia rekisterinpitäjälle tai sille, joka rekisterinpitäjän lukuun käyttää ja käsittelee henkilörekistereitä tai niissä olevia tietoja[37]. Lainsäädännössä suoraan asetettujen velvollisuuksien lisäksi palveluiden tilaajan ja tarjoajan välisistä tietosuojaan liittyvistä vastuista sovitaan usein sopimuksella. Verkkotietopalveluja tarjoava yritys toimii yleensä tiedon käsittelijänä toisen lukuun[38]. Tietosuojalainsäädännössä puhutaan tällöin henkilötietojen käsittelijästä. Nykyisen lainsäädännön mukaan palveluntarjoajan velvoitteet ovat välillisiä ja sillä on vain rajoitettu vastuu tiedon käsittelystä. Vastuusta toimeksiantajaan nähden sovitaan sopimuksella. Tätä rakennetta tukee myös suomalainen viranomaiskäytäntö, joka korostaa rekisterinpitäjän vastuuta[39].[40] Verkkotietopalveluyrityksen kannalta merkittävää on, että tulevassa tietosuojauudistuksessa kaavaillaan vastuita myös palveluntarjoajalle ja sanktiot mahdollisista tietosuojarikkomuksista saattavat nousta hyvinkin suuriksi.

Tietosuoja-asetusehdotus lisää huomattavasti henkilötietojen käsittelijän vastuita ja velvollisuuksia. Uudistuksessa ehdotetaan sekä aivan uusia vastuita että laajennetaan nykyisiä rekisterinpitäjän vastuita koskemaan myös tiedon käsittelijää. Vastuiden kasvattaminen vaikuttaa merkittävästi palveluntarjoajien liiketoimintariskeihin ja toiminnan kustannuksiin, mikä todennäköisesti tulee näkymään myös palvelun hintojen nousuna. Henkilötietojen käsittelijän vastuita ehdotetaan esityksessä laajennettavan erityisesti käsittelyn dokumentoinnin ja käsittelyketjun hallinnoinnin osalta. Käsittelyn läpinäkyvyyden toteutumiseksi käsittelijän on kerättävä ja säilytettävä yksityiskohtaiset tiedot käsittelystä, jotta nämä ovat ehdotuksen mukaisesti pyydettäessä henkilön saatavilla[41].

[37] Yksi esimerkki tällaisesta hallinnollisesta velvoitteesta rekisteriselosteiden laatiminen ks. henkilötietolaki 10 §.
[38] Article 29 Working Party: Opinion 05/2012 on Cloud Computing, Adopted 1.6.2012, s.7-8. Ks. myös Hon, w Kuan - Hörnle, Julia - Millard, Christopher: Which Law(s) Apply to Personal Data in Clouds? Teoksessa Cloud Computing Law (toim. Millard, Christopher), Oxford University Press 2013, s.210.
[39] Ks. Hon, w Kuan - Hörnle, Julia - Millard, Christopher: Which Law(s) Apply to Personal Data in Clouds? Teoksessa Cloud Computing Law (toim. Millard, Christopher), Oxford University Press 2013, s.201.
[40] Kaho, Julå, Kara ja Iike, 2014, 2014, s 10.
[41] Tietosuoja-asetusehdotus, artikla 15 (Regulation (EU) No XXX/2016
of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)).

Lainsäädännön yhtenäisyys korostaa sääntelyä valvovan viranomaisen painoarvoa säännösten tulkitsijana ja noudattamisen valvojana. Valtioiden tietosuojalainsäädännön erojen vähentyessä lisääntyy myös viranomaisen toimivaltuuksien merkitys. Verkkopalveluita tarjoavien yritysten kohdalla merkitystä on tällöin erityisesti sillä, onko ja millä edellytyksillä viranomaisella oikeutta vaatia pääsyä tietosisältöön. Tällainen oikeus voi olla joko tiedusteluperusteista tai tähdätä esimerkiksi vakavan rikoksen estämiseen tai selvittämiseen. Tiedonsaantivaatimus voi siten perustua muun muassa tiedon käyttötapaan tai tiedon haltijan toimintaan tai suoraan tiedon kohteeseen.[42]

Suomalaisilla viranomaisilla ei nykyisen lainsäädännön mukaan ole oikeutta päästä tietosisältöihin tiedusteluperusteella. Tiukasti rajoitetut viranomaisoikeudet tukevat Suomen mainetta korkean tietosuojan maana, johon sijoittuvien verkkopalveluiden piirissä olevat tiedot säilyvät luottamuksellisina.[43] Tiedusteluperusteisia oikeuksia on tällä hetkellä esimerkiksi Ruotsissa ja Ranskassa, ja paine samankaltaisten oikeuksien saamiseen on olemassa myös täällä. Parhaillaan on vireillä puolustus- ja sisäministeriön yhteinen hanke vastaavan tiedustelulainsäädännön luomiseksi myös Suomeen.

3 Tietosuoja- ja tietoturvanäkökohtia

3.1 Nykyinen tietosuojalainsäädäntö

Viestinnän luottamuksellisuus on suojattu Suomessa perustuslain (731/1999) nojalla. Perustuslain 10 §:n mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Viestinnän luottamuksellisuutta ja viestintäverkkojen käyttäjien yksityisyyttä turvaavista sähköisen viestinnän välittäjien vastuista säädetään tietoyhteiskuntakaaressa (917/2014). Samassa laissa ovat myös säädökset viestintäverkkojen ja -palvelujen laatuvaatimuksista, jotka kohdistuvat teleyrityksiin.

Perustuslain 10 §:n mukaan lailla voidaan säätää välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien

[42] Kaho, Julå, Kara ja like, 2014, 2014, s 13-14.
[43] Kaho, Julå, Kara ja like, 2014, 2014, s 14.

rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana. Tällaisista rajoituksista on säädetty tietoyhteiskuntakaaressa, poliisilaissa (493/1995) ja pakkokeinolaissa (806/2011).

Kotimaisen lainsäädännön lisäksi myös kansainväliset sopimukset kuten Euroopan ihmisoikeussopimus (Yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi) sekä Euroopan unionin perusoikeuskirja (2000/C 364/01) suojaavat viestinnän luottamuksellisuutta. Viestin yksityisyyden kunnioittaminen on osa perusoikeuskirjan 7 artiklaa ja henkilötietojen suojaan liittyviä velvoitteita käsitellään puolestaan artiklassa 8. Lisäksi tarkempia säännöksiä viestinnän luottamuksellisuudesta on annettu sähköisen viestinnän tietosuojadirektiivissä (2002/58/EY) 5 artiklassa, jonka mukaan jäsenvaltioilla on velvollisuus varmistaa sähköisen viestinnän ja siihen liittyvien liikennetietojen luottamuksellisuus.

Näistä kansainvälisesti velvoittavista säännöksistä voidaan kuitenkin kansallisesti poiketa lailla, jos 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. Kansainväliseen viestintään saattaa siten kohdistua kauttakulkumaiden mahdollisesti kansainvälisistä säännöistä poikkeavaa kansallista lainsäädäntöä. Näin on esimerkiksi Ruotsissa, jossa on tietyin edellytyksin lainsäädännössä vahvistettu kansainvälisen viestinnän seuranta ja kuuntelu[44].

3.2 Verkkotietopalveluyrityksen vastuut henkilötietolain mukaan

Luottamuksellisen viestinnän suojaa koskevien tietosuojasäännösten lisäksi verkkotietopalveluja koskevat usein henkilötietojen suojaamista koskevat säännökset, sillä palveluissa tavallisesti käsitellään ja siirretään henkilötiedoiksi luokiteltavia arkaluonteisiakin tietoja. Keskeisin henkilötietoja suojaava laki Suomessa on henkilötietodirektiiviin perustuva henkilötietolaki.

[44] Ks tarkemmin luku 3.4.

Henkilötietolain tarkoituksena[45] on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä. Vastaavasti henkilötietodirektiivissä todetaan[46], että henkilötietojen käsittelyssä luonnollisille henkilöille turvataan heidän perusoikeutensa ja -vapautensa sekä heidän oikeutensa yksityisyyteen. Lisäksi henkilötietolain tarkoituksena mainitaan hyvän tietojenkäsittelytavan kehittämisen ja noudattamisen edistäminen. Henkilötietojen käsittely on sallittu vain henkilön suostumuksella tai erikseen laissa säädetyissä tilanteissa. Henkilötietolain noudattamatta jättäminen on sanktioitu rikoslaissa henkilötietorikoksena[47].

Henkilötietolain perusperiaate on, että rekisterinpitäjä vastaa henkilötietojen käsittelystä. Henkilötietolain 3 §:n 4. kohdan mukaan rekisterinpitäjä tarkoittaa yhtä tai useampaa henkilöä, yhteisöä, laitosta tai säätiötä, jonka käyttöä varten henkilörekisteri perustetaan ja jolla on oikeus määrätä henkilörekisterin käytöstä tai jonka tehtäväksi rekisterinpito on lailla säädetty. Kaikki henkilötietoihin kohdistuvat toimenpiteet myös säilyttäminen ovat henkilötietojen käsittelyä. Siten tietojen säilyttäminen, käsitteleminen ja siirtäminen verkkotietopalvelussa on tietojen käsittelyä, johon sovelletaan henkilötietolakia.[48]

Verkkotietopalveluissa tapahtuvassa henkilötietojen käsittelyssä tilaaja on rekisterinpitäjänä ensisijaisessa vastuussa tietojen käsittelystä. Palvelun tarjoajalle on

---

[45] Henkilötietolaki 1§.

[46] Henkilötietodirektiivi 1 artikla, 1 kohta.

[47] Tietosuojaan olennaisesti liittyvästä henkilörekisteririkoksesta säädetään rikoslain 38:9 §:ssä. Joka tahallaan tai törkeästä huolimattomuudesta:
1) käsittelee henkilötietoja vastoin henkilötietolain käyttötarkoitussidonnaisuutta, käsittelyn yleisiä edellytyksiä, henkilötietojen tarpeellisuutta tai virheettömyyttä, arkaluonteisia tietoja, henkilötunnusta tai henkilötietojen käsittelyä erityisiä tarkoituksia varten koskevia säännöksiä taikka rikkoo henkilötietojen käsittelyä koskevia erityissäännöksiä,
2) antamalla rekisteröidylle väärän tai harhaanjohtavan tiedon estää tai yrittää estää rekisteröityä käyttämästä hänelle kuuluvaa tarkastusoikeutta tai
3) siirtää henkilötietoja Euroopan unionin tai Euroopan talousalueen ulkopuolisiin valtioihin henkilötietolain 5 luvun vastaisesti
ja siten loukkaa rekisteröidyn yksityisyyden suojaa tai aiheuttaa hänelle muuta vahinkoa tai olennaista haittaa, on tuomittava henkilörekisteririkoksesta sakkoon tai vankeuteen enintään yhdeksi vuodeksi.

[48] Henkilötietolakia sovelletaan sellaiseen henkilötietojen käsittelyyn, jossa rekisterinpitäjän toimipaikka on Suomen alueella tai muutoin Suomen oikeudenkäytön piirissä.
Henkilötietolakia sovelletaan myös silloin, kun rekisterinpitäjällä ei ole toimipaikkaa Euroopan unionin jäsenvaltioiden alueella, mutta rekisterinpitäjä käyttää henkilötietojen käsittelyssä Suomessa sijaitsevia laitteita muuhunkin tarkoitukseen kuin vain tietojen siirtoon tämän alueen kautta. Rekisterinpitäjän on tällöin nimettävä Suomessa oleva edustaja.

kuitenkin henkilötietolaissa asetettu velvollisuus huolehtia palvelua tuottaessaan henkilötietojen suojasta tilaajan ohella. Henkilötietolain 5 § huolellisuusvelvoitteen mukaan rekisterinpitäjälle asetettu velvoite käsitellä henkilötietoja laillisesti, noudattaa huolellisuutta ja hyvää tietojenkäsittelytapaa sekä toimia muutoinkin niin, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Vastaava velvoite on myös sillä, joka itsenäisenä elinkeinon- tai toiminnanharjoittajana toimii rekisterinpitäjän lukuun.

Verkkotietopalvelun tarjoajan on henkilötietolain 32 §:n 2 momentin mukaan ennen tietojen käsittelyyn ryhtymistä annettava rekisterinpitäjälle asianmukaiset selvitykset ja sitoumukset sekä muutoin riittävät takeet henkilötietojen suojaamisesta. Henkilötiedot on suojattava teknisin ja organisatorisin toimin asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.

Jotta henkilötietolain tietosuoja- ja tietoturvavaatimukset toteutuisivat asianmukaisella tavalla, on tilaajan käytännössä sovittava niistä verkkotietopalvelun ostosopimuksessa. Palveluntarjoajalla on puolestaan velvollisuus huolehtia, että tietosuoja ja tietoturva toteutuvat sen tarjoamissa palveluissa. Tilaajalla on oikeus saada selvitys siitä, millaisilla menettelyillä on estetty asiattomien pääsy henkilötietoihin sekä muu laiton henkilötietojen käsittely. Näin se voi rekisterinpitäjänä arvioida, riittävätkö tietoturvatoimenpiteet henkilötietojen suojaamiseen.[49]

Henkilötietolain 5 luvun mukaisesti henkilötietojen käsittely on alueellisesti rajattua. Henkilötietoja voidaan siirtää lain 22 §:n mukaan Euroopan unionin jäsenvaltioiden alueen tai Euroopan talousalueen ulkopuolelle vain, jos kyseisessä maassa taataan tietosuojan riittävä taso. Tietosuojan tason riittävyyteen vaikuttavat tietojen luonne, suunnitellun käsittelyn tarkoitus ja kestoaika, alkuperämaa ja lopullinen kohde, asianomaisessa maassa vallitsevat yleiset ja alakohtaiset oikeussäännöt sekä käytännesäännöt ja noudatettavat turvatoimet. Arvioinnissa on huomioitava kaikki olosuhteet, jotka liittyvät tiettyyn siirtoon tai siirtojen ryhmään, ja tietosuojan tason on säilyttävä riittävällä tasolla kaikissa olosuhteissa. Käytännössä tämän arvioinnin

[49] Tietosuoja pilvipalveluiden hankintasopimuksissa julkisessa hallinnossa, Voutilainen, Tomi – Galkin, Denis. Defensor Legis 2013/3, 5.6.2013, s. 376.

suorittavat rekisterinpitäjä ja tietosuojavaltuutettu, jolle ilmoitus henkilötietojen siirrosta on henkilötietolain 36,2§:n mukaan tehtävä.[50]

Henkilötietolain 22 a §:n mukaan henkilötietoja voidaan siirtää, jos komissio on päätöksellään todennut siirtomaan tietosuojan riittäväksi. Jos komissio on antanut tällaisen tiedon jostakin valtiosta, ei rekisterinpitäjällä ole siirrosta ilmoitusvelvollisuutta tietosuojavaltuutetulle. Verkkotietopalvelun tarjoaja voi kuitenkin joutua tekemään toimintailmoituksen tietosuojavaltuutetulle tietojenkäsittelytoiminnastaan. Henkilötietojen käsittely esimerkiksi pilvipalvelussa edellyttää tietoa siitä, missä maassa tietoja säilytetään, millaisen päätöksen komissio on antanut sijaintimaan tietosuojatasosta ja onko tarvittava toimintailmoitus tehty.[51]

Henkilötietolain 23 §:ssä on lueteltu poikkeusperusteet, joilla tietoja voidaan siirtää, vaikka siirtomaan tietosuojan taso on katsottu riittämättömäksi. Lähtökohtaisesti tämä on mahdollista, kun siirtoon on rekisteröidyn yksiselitteinen suostumus. Lisäksi siirto voidaan tehdä rekisteröidyn toimeksiannosta tai sopimuksen toimeenpanemiseksi. Myös rekisteröidyn elintärkeä etu ja yleinen etu sallivat siirtokiellosta poikkeamisen. Näiden yleisten poikkeusperusteiden lisäksi siirto on mahdollista tehdä sopimusmenettelyin. Henkilötietolain 23 §:n poikkeusperustelistan 7 kohdan mukaan siirto voidaan tehdä, jos rekisterinpitäjä antaa sopimuslausekkein tai muulla tavoin riittävät takeet henkilöiden yksityisyyden ja oikeuksien suojasta, eikä komissio ole henkilötietodirektiivin[52] mukaisesti todennut takeita riittämättömiksi. Vastaavasti siirto on sallittu, jos se tapahtuu komission hyväksymiä mallisopimuslausekkeita[53] käyttäen.

Yhdysvaltojen ja Euroopan Unionin välille solmittiin vuonna 2000 Safe Harbor -sopimus[54], joka mahdollisti henkilötietojen siirron Yhdysvaltoihin siitä huolimatta, että Yhdysvalloissa ei katsottu olevan riittävää tietosuojan tasoa. Sopimuksen tavoitteena

[50] HE 96/1998 vp. s.58, Voutilainen s.379.
[51] Voutilainen s.379.
[52] Ks. Henkilötietodirektiivi 3 artikla ja 26 artiklan 3 kohta.
[53] Ks. Henkilötietodirektiivin 26 artikla 4 kohta, Voutilainen s.380-381.
[54] Ks. Komission päätös, tehty 26 päivänä heinäkuuta 2000, Euroopan parliamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä, 2000/520/EY.

oli varmistaa, että yhdysvaltalaisten yritysten tietosuojakäytännöt ovat vähintään Euroopan Unionin lainsäädännön tasoiset.[55]

Safe Harbor -järjestely toteutettiin käytännössä siten, että Yhdysvaltain kauppaministeriön (US Department of Commerce) julkaisi verkkosivustollaan listan, johon Yhdysvaltalaiset yritykset pystyivät ilmoittautumaan ja näin sitoutumaan Safe Harbor -järjestelyssä sovittujen periaatteiden noudattamiseen. Osana järjestelyä yritykset muun muassa velvoitettiin ilmoittamaan, mihin tarkoitukseen henkilötietoja kerätään ja käsitellään ja siirretäänkö niitä kolmansille tahoille. Järjestelyn tavoitteena oli taata henkilöille vähintään henkilötietodirektiivin mukaiset tietosuojaoikeudet. Safe Harbor -järjestelyyn sitoutuneita yrityksiä vastaan voitiin nostaa kanne sillä perusteella, että se on rikkonut toiminnassaan järjestelyn periaatteita.[56]

Safe Harbor on vuosien ajan mahdollistanut sen, että yhdysvaltalaiset yritykset ovat voineet tarjota esimerkiksi henkilötietojen käsittelyyn liittyviä pilvipalveluja Eurooppaan. Järjestelyä ei voida kuitenkaan jatkossa enää hyödyntää, sillä EU:n tuomioistuin on päätöksessään[57] todennut Safe Harbor -sopimuksen mitättömäksi. Tuomioistuimen mukaan Safe Harbor ei takaa riittävää yksityisyyden suojaa EU-jäsenvaltioiden kansalaisille, sillä järjestelystä huolimatta Yhdysvaltain viranomaisilla on laaja pääsyoikeus heidän tietoihinsa. Päätöksessä todetaan myös, ettei Safe Harbor -järjestely takaa henkilöille riittäviä keinoja tarkastaa heistä kerättyjä henkilötietoja, tai vaatia näiden tietojen korjaamista tai poistamista[58].

Päätöksen jälkeen Euroopan Komissio aloitti eurooppalaisten tietosuojaviranomaisten ja WP 29 tietosuojatyöryhmän (eurooppalainen tietosuojavaltuutettujen muodostama elin) kanssa analysoinnin päätöksen vaikutuksista voimassa oleviin tietojensiirtosopimuksiin, joissa Safe Harbor -järjestelyyn on turvauduttu. Yritysten osalta kysymys on oikeusvarmuudesta. Oikeustoimia tehdessään yritysten on voitava luottaa lainsäädännön pysyvyyteen siltä osin, että niiden voimassa olevan lainsäädännön mukaan tekemät toimet eivät yhtäkkiä muutu lainvastaisiksi.

[55] Voutilainen 2013, s. 381.
[56] Pitkänen 2013, s.185.
[57] C- 362/14, 6.lokakuuta 2015.
[58] Court of Justice of the European Union press release No 117/15.

Kannanotossaan päätöksen vaikutuksista WP 29 tietosuojatyöryhmä toteaa oikeusvarmuusperiaatteen vastaisesti, että ennen kuin Yhdysvaltojen viranomaisten kanssa saadaan sovittua uudesta järjestelystä koskien tietojen turvallista siirtoa Euroopan ja Yhdysvaltojen välillä, tiedonsiirto ei ole mahdollista muutoin laissa erikseen myönnetyllä poikkeusperusteella. Työryhmä lausuu kannanotossaan yksiselitteisesti, että päätöksen jälkeen tapahtuva tietojen siirto Safe Harbor -järjestelyyn nojaten on lainvastaista.[59]

Komission tavoitteena on sopia uusi järjestely, joka täyttää EU-tuomioistuimen asettamat siirtoehdot[60]. Tämä EU:n ja Yhdysvaltojen.välinen Privacy Shield –järjestely vastaa toimintatavoiltaan Safe Harboria, mutta siinä tulee olemaan tietosuojan osalta jonkinasteisia tiukennuksia verrattuna Safe Harboriin[61].

Kun Safe Harbor ei ole enää käytettävissä, henkilötietojen siirto Yhdysvaltoihin on mahdollista edellä mainittujen poikkeusperusteiden toteutuessa. Käytännössä tämä tarkoittaa sitä, että yrityksen on sovittava tietosuojasta joko sopimusmenettelyin tai sitten rekisteröidyn on annettava nimenomainen suostumus henkilötietojensa siirtoon. Yrityksille tämä tulee aiheuttamaan huomattavia hallinnollisia kustannuksia, sillä jokainen yrityksen toimittajiensa kanssa solmima, Safe Harbor -järjestelyyn nojannut sopimus on kartoitettava ja neuvoteltava tietosuojan osalta uudelleen.

Suomen kannalta positiivinen seuraus päätökselle saattaa olla se, että Suomen houkuttavuus verkkotietopalveluyrityksen sijaintivaltiona kasvaa suhteessa Yhdysvaltoihin, sillä henkilötietojen siirron hankaloituminen ja suoranaiset kustannukset puoltavat yritysten sijoittautumista EU-alueelle. Erityisesti tiedon säilytystä tarjoavien yhdysvaltalaisyritysten on löydettävä ratkaisuja, jotka mahdollistavat palvelujen tarjoamisen Euroopassa ilman, että tietoja joudutaan siirtämään EU:n ulkopuolelle. Yksi vaihtoehto on investoida Euroopassa sijaitseviin datakeskuksiin jonkun paikallisen toimijan kanssa yhteistyössä, jolloin esimerkiksi

[59] Statement of the Article 29 Working Party, Brussels, 16 October 2015.
[60] Kom (2015) 566 lopullinen, s.15.
[61] European Commission, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016

NSA:n (Yhdysvaltain kansallinen turvallisuusviranomainen) pääsy tietoon voidaan estää EU-lainsäädännön edellyttämällä tavalla[62].

3.3 Lainsäädännön asettamat tietoturvavaatimukset

3.3.1 Tietoturvaan vaikuttaminen lainsäädännön keinoin

Tietosuojakysymysten lisäksi myös tietoturvan tasolla on vaikutusta siihen, miten suotuisa sijaintikohde valtio on verkkotietopalveluyrityksille. Lainsäädännöllä on mahdollista taata tietoturvallisuuden toteutuminen kolmella eri tavalla. Ensinnäkin voidaan rikoslain keinoin varmistaa, että tietoturvallisuuteen kohdistuvien hyökkäysten tekeminen ei ole rikollisen näkökulmasta kannattavaa. Tietomurtojen ja hyökkäysten kattava ja aukoton kriminalisointi sekä toisaalta teoista määrättävissä olevien rangaistusten riittävä ankaruus suhteessa teosta saatavaan hyötyyn todennäköisesti vähentävät tai jopa estävät mahdollisia tietohyökkäyksiä. Lisäksi edellytyksenä tällaiselle ennaltaehkäisevyydelle on tietenkin tutkimus- ja valvomisresurssien riittävyys ja tehokkuus sekä ennen kaikkea rikosten ehkäisyyn ja selvitykseen käytössä oleva keinovalikoima.

Kriminalisoinnin ja rangaistusten avulla toteutettavan suojan lisäksi tietoturvan tasoon voidaan vaikuttaa säätämällä yrityksille tietoturvavelvoitteita. Yritysten näkökulmasta tällainen lainsäädäntö parantaa tietoturvan tasoa ja asiakasyritysten sekä loppukäyttäjien luottamusta palveluiden laatuun. Lisäksi tietoturvan tason parantuminen pienentää ja ehkäisee tietoturvariskejä ja mahdollisista tietoturvarikkomuksista aiheutuvia vahinkoja.

Toinen puoli tässä lähestymistavassa yritysten kannalta on kustannusten hallinta. Tietoturvavelvoitteiden ja niistä syntyvien kustannusten tulee olla oikeassa suhteessa saavutettavaan hyötyyn nähden. Kuten luvussa kaksi todetaan, kustannukset ovat keskeinen tai jopa ratkaiseva tekijä yritysten punnitessa mahdollista sijaintiaan.

Vaikka tietoturvan taso olisi kuinka aukoton tahansa, yrityksen voi olla silti kannattamatonta sijoittautua maahan, jos tietoturvan kustannukset nousevat suhteettoman suuriksi suhteessa tietoturvan tuomiin hyötyihin, kuten asiakasmäärien

[62] Esimerkki tästä on Microsoftin Deutsche Telekomin kanssa Saksaan perustama datakeskus, josta uutisoitiin muutamia viikkoja Safe Harbor-päätöksen jälkeen.

kasvuun. Eräässä mielessä voidaan ajatella, että täydellisen tietoturvallinenkaan valtio ei voi silloin olla tiedon turvasatama ainakaan, jos käsitteellä tiedon turvasatama tarkoitetaan valtiota, johon tiedonsiirtoon ja muuhun käsittelyyn keskittyvät yritykset haluavat sijoittautua. Koska nimenomaan tämä näkökulma on otettu käsitemäärittelyn lähtökohdaksi tässä tutkimuksessa, on tämänhetkistä ja valmisteilla olevaa säätelyä tarkasteltaessa huomioitava myös tietoturvavelvoitteiden aiheuttamat kustannusvaikutukset.

Kolmas tapa suojata tietoturvan toteutuminen lainsäädännön keinoin on varmistaa se yleisellä tasolla tehostamalla tietoturvan valvontaa ja mahdollisiin tietoturvauhkiin puuttumista. Tätä sääntelykeinoa tarkastellaan lähemmin luvussa 5.3, joka käsittelee kyberturvallisuutta koskevaa nykyistä sääntely-ympäristöä ja valmisteilla olevia EU-tason lakihankkeita.

Kyberrikokset ovat yleensä massarikollisuutta, jonka alueelliset vaikutukset ovat vähäiset[63]. Niiden torjunta vaatii tiivistä ja nopeaa kansallista sekä valtioiden välistä yhteistyötä, sillä uhrit, tekijät ja rikoksentekovälineet sijaitsevat tyypillisesti eri maissa ja vähintään saman valtion eri maantieteellisillä alueilla. Välttämättä edes tekijät eivät tunne toisiaan tekojen tapahtuessa verkkomaailmassa.[64] Tämä aiheuttaa myös tietoturvarikosten ennaltaehkäisylle haasteita, sillä sitä ei ole mahdollista toteuttaa vain kansallisista lähtökohdista.

3.3.2 Tietoturvaloukkauksia koskeva sääntely

Tietoturvaan kohdistuvista tieto- ja viestintärikoksista säädetään rikoslain 38 luvussa. Luvun rikoksista erityisesti viestintäsalaisuuden loukkaus 38:3 § ja törkeä viestintäsalaisuuden loukkaus 38:4§ liittyvät verkkotietopalveluyritysten toimintaan. Viestintäsalaisuuden loukkaukseksi katsotaan toiselle osoitetun kirjeen tai muun suljetun viestin avaaminen tai tiedon hankkiminen suojaus murtaen sähköisesti tai muulla vastaavalla teknisellä keinolla tallennetusta, ulkopuoliselta suojatusta viestistä tai tiedon hankkiminen televerkossa välitettävänä olevan puhelun, sähkeen, tekstin-, kuvan- tai datasiirron taikka muun vastaavan televiestin sisällöstä tai tällaisen viestin lähettämisestä tai vastaanottamisesta. Rangaistus viestintäsalaisuuden

[63] Leppänen, Virta, 2014 s.5.
[64] Grabosky, 2009, s. 172.

loukkauksesta on sakkoa tai enintään yksi vuosi vankeutta. Myös yritys on rangaistava.

Viestintäsalaisuuden loukkausta on pidettävä rikoslain mukaan törkeänä, jos
1) rikoksentekijä käyttää rikoksen tekemisessä hyväksi asemaansa teleyrityksen palveluksessa tai muuta erityistä luottamusasemaansa tai
2) rikoksentekijä käyttää rikoksen tekemistä varten suunniteltua tai muunnettua tietojenkäsittelyohjelmaa tai teknistä erikoislaitetta tai
3) rikos muuten tehdään erityisen suunnitelmallisesti tai
4) rikoksen kohteena oleva viesti on sisällöltään erityisen luottamuksellinen taikka
5) teko huomattavasti loukkaa yksityisyyden suojaa ja viestintäsalaisuuden loukkaus on myös kokonaisuutena arvostellen törkeä. Rangaistus törkeästä viestintäsalaisuuden loukkauksesta on enintään kolme vuotta vankeutta. Myös törkeän viestintäalaisuuden loukkauksen yritys on rangaistava.

Verkkotietopalveluyritysten tietoturvaan liittyy oleellisesti myös rikoslain tietomurtoa 38:8§ ja törkeää tietomurtoa 38:9§ koskevat pykälät. Tietomurroksi katsotaan toiselle kuuluvaa käyttäjätunnusta käyttäen tai turvajärjestelyn muuten murtaen oikeudeton tunkeutuminen tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan. Tietomurrosta on tuomittava sakkoa tai enintään kaksi vuotta vankeutta.

Tietomurrosta tuomitaan myös se, joka tietojärjestelmään tai sen osaan tunkeutumatta
1) teknisen erikoislaitteen avulla tai
2) muuten teknisin keinoin turvajärjestelyn ohittaen, tietojärjestelmän haavoittuvuutta hyväksi käyttäen tai muuten ilmeisen vilpillisin keinoin oikeudettomasti ottaa selon tietojärjestelmässä olevasta tiedosta tai datasta.
Myös tietomurron yritys on rangaistava.

Törkeän tietomurron tunnusmerkit täyttyvät jos tietomurto tehdään osana järjestäytyneen rikollisryhmän toimintaa tai erityisen suunnitelmallisesti ja tietomurto on myös kokonaisuutena arvostellen törkeä. Rikoksentekijä on tuomittava törkeästä tietomurrosta sakkoon tai vankeuteen enintään kolmeksi vuodeksi. Vastaavasti kuin tietomurron osalta myös törkeän tietomurron yritys on rangaistava.

Verkkotietopalveluyrityksen tietoturvaan liittyy myös rikoslain 38:8b §, jossa säädetään suojauksen purkujärjestelmärikoksesta. Suojauksen purkujärjestelmärikokseen syyllistyy rikoslain mukaan se, joka tietoyhteiskuntakaaren 269 §:n 2 momentissa säädetyn kiellon vastaisesti ansiotarkoituksessa tai siten, että teko on omiaan aiheuttamaan huomattavaa haittaa tai vahinkoa suojatun palvelun tarjoajalle, valmistaa, tuo maahan, pitää kaupan, vuokraa tai levittää suojauksen purkujärjestelmää, mainostaa sitä taikka asentaa tai huoltaa sitä. Suojauksen purkujärjestelmärikoksesta on tuomittava sakkoa tai vankeutta enintään yksi vuosi.

3.3.3 Tietoturvavelvollisuuksia koskeva sääntely

Viestinnän välittäjän ja lisäarvopalvelun tarjoajan velvollisuudesta huolehtia tietoturvasta säädetään tietoyhteiskuntakaaren 247 §:ssä. Samat tietoturvavelvollisuudet koskevat myös yritystä, joka on velvollinen säilyttämään teletunnistetietoja[65]. Viestejä välitettäessä on huolehdittava palvelujen, viestien, välitystietojen ja sijaintitietojen tietoturvasta. Poikkeuksena yhteisötilaajan on viestien välittäjänä huolehdittava ainoastaan käyttäjiensä viestien, välitystietojen ja sijaintitietojen käsittelyn tietoturvasta. Lisäarvopalvelun tarjoajan velvollisuutena on huolehtia, että sen tarjoamat palvelut ovat tietoturvallisia.

Tietoturvatoimenpiteet on suhteutettava siihen, miten vakava uhka on kyseessä, toimenpiteistä aiheutuviin kustannuksiin sekä siihen, millaisia teknisiä mahdollisuuksia uhan torjumiseksi on käytettävissä. Viestintävirasto voi tarkentaa tietoturvamääräyksiä tietoyhteiskuntakaaressa säädetystä.

Kun verkkotietopalveluyrityksen asiakkaana on valtiotoimija, yrityksen tietoturvavelvoitteet seuraavat lainsäädännössä valtiolle asetetuista velvoitteista. Valtionhallinnon tietoturvallisuudesta annetun asetuksen (681/2010) mukaan valtionhallinnon viranomaisten on täytettävä vähintään perustietoturvatason vaatimukset. Näitä vaatimuksia ovat tietoturvariskien kartoittaminen, tietoturva-asiantuntemuksen varmistaminen, tiedonhallinnan tehtävien ja vastuiden määrittely, tietojen saannin ja käytettävyyden turvaaminen erilaisissa tilanteissa, pääsynhallinnan, käyttöoikeuksien hallinnan ja valvonnan järjestäminen,

[65] Tietoyhteiskuntakaari 158§.

tietojenkäsittelijöiden luotettavuuden arviointi sekä tietoturvaohjeistus ja -koulutus. Verkkotietopalveluyrityksellä on oltava käytössään samat prosessit tietoturvallisuuden järjestämiseksi kuin viranomaisilla, jotta ne olisivat kelvollisia tuottamaan palveluja.

Perustasoa korkeammin luokiteltujen tietojen käsittelyyn sisältyy lisäksi erityisvelvoitteita, kuten kielto siirtää tietoja Suomen ulkopuolelle. Tällaiset vaatimukset edellyttävät verkkotietopalvelun tarjoajalta sitä, että datakeskus sijaitsee fyysisesti Suomessa eikä palvelussa säilytettävään tietoon ole pääsyä ulkomailta. Tietoturva-asetuksen 9.1 §:n mukaisiin perustason korkeampiin suojaustasoihin III–IV kuuluvat esimerkiksi viranomaisen henkilörekistereissä olevat muut kuin erikseen yleiseen käyttöön säädetyt henkilötiedot.[66]

3.3.4 Tietoturvan valvontaan ja tietoturvaloukkausten ehkäisyyn keskittyvä sääntely

Tietoturvan valvontaan ja ehkäisyyn liittyvä sääntely kuuluu Suomessa sisäministeriön vastuualaan. Sisäministeriö vastaa esimerkiksi siitä, että poliisilla on riittävät edellytykset estää, paljastaa ja selvittää tietoverkkorikoksia. Sisäministeriö myös kehittää Suomen kyberlainsäädäntöä ja on osaltaan toimeenpanemassa Suomen kyberturvallisuusstrategiaa jonka valtioneuvosto on hyväksynyt tammikuussa 2013.[67]

Viestintäviraston alaisuudessa toimii kansallinen tietoturvaviranomainen Kyberturvallisuuskeskus, jonka tehtävänä on tietoturvaloukkausten ehkäisy ja selvittäminen sekä merkittävistä tietoturvauhkista tiedottaminen. Kyberturvallisuusstrategian mukaisesti kyberturvallisuuskeskus tuottaa ja ylläpitää yhdistettyä kyberturvallisuuden tilannekuvaa, jota keskuksen asiakkaat voivat hyödyntää, kun ne järjestävät ja priorisoivat omaa varautumistaan.[68]

Käytännössä tietoturvan taso ja tietoturvan ylläpitämiseksi valittu ratkaisu on jokaisen yrityksen valittavissa toimintansa ja tarpeidensa mukaan. Keskitettyä ohjausta tähän ei ole, vaan tietoturvaloukkausten ehkäisy perustuu vapaaehtoisuuteen. Tietoturvahyökkäysten ehkäisyn ja havaitsemisen tukena on Tietoyhteiskuntakaaren 272 §, joka mahdollistaa sähköisiä viestintäpalveluja hyödyntäville yrityksille niiden

[66] Ks. ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010, s. 59.
[67] https://www.intermin.fi/fi/turvallisuus/rikostorjunta/kyberturvallisuus
[68] Suomalaisen tiedustelulainsäädännön suuntaviivoja, s.36.

verkkoon tulevien ja niistä lähtevien viestien sisällön analysoinnin haittaa aiheuttavien häiriöiden havaitsemiseksi, estämiseksi, selvittämiseksi ja esitutkintaan saattamiseksi.

3.4 Nykytilan arviointia

Tällä hetkellä Suomessa voimassa oleva tietosuojalainsäädäntö tarjoaa kattavan suojan verkkotietopalveluyritysten käsittelemälle tiedolle. Käytännössä yrityksillä on kuitenkin oltava liiketaloudellinen kannustin kuten maine, asiakaskunnan kasvu tai toiminnan jatkuminen toteuttaa ja ylläpitää tietosuojaa, jotta riittävä tietosuojan taso todella toteutuisi. Tätä tukevat lainsäädännössä määritellyt sanktiot sekä tietenkin saavutettavat taloudelliset hyödyt.

Tietoturvan osalta tilanne ei ole aivan yhtä hyvällä tasolla. Lainsäädännöllisiä velvoitteita yrityksille huolehtia tietoturvasta ei ole juuri asetettu, vaan tietoturvasta huolehtiminen ja kulloisetkin tietoturvatasot ovat yritysten omassa päätäntävallassa. Tämä on käytännössä johtanut siihen, että kaikissa yrityksissä ei tietoturvasta ole huolehdittu riittävästi, koska siitä ei ole säädetty pakottavasti. Suuri määrä yrityksissä käytössä olevista järjestelmistä on todennäköisesti sellaisia, ettei niissä ole varauduttu verkkohyökkäyksiin[69].

Jotta tietoturvallisuutta voidaan oikeasti parantaa, tulee olla käytössä olla mahdollisimman tehokkaat keinot ehkäistä tietoturvaloukkauksia. Tässä oleellista on tiedonkulku sekä viranomaisten välillä että viranomaisilta yrityksille ja kansalaisille. Hyökkäyksiltä voidaan tehokkaasti suojautua vain, jos niistä saadaan tieto mahdollisimman aikaisessa vaiheessa. Yksi keino saada tietoa ja ehkäistä tietoturvarikoksia on tietoturvahyökkäysten kohteiden velvoittaminen kertomaan tapahtuneista hyökkäyksistä ja niistä käytetyistä tekniikoista. Tämä voi olla vaikeaa erityisesti verkkotietopalveluyritysten näkökulmasta, joille maine tietoturvallisina palveluntarjoajina on usein elintärkeää asiakaskunnan luottamuksen säilyttämisen kannalta.

Asiakkaiden kasvava tietoisuus tietosuojasta ja sääntelyn merkityksestä kannustaa yrityksiä sekä ylläpitämään toiminnassaan että tavoittelemaan korkeaa

[69] Ks. esim Manner, Tiilikainen, 2014.

tietosuojatasoa. Vastaavasti asiakkaiden kasvavat tietoturvavaatimukset toivottavasti saavat lainsäädännön puutteellisuudesta huolimatta myös yritykset huolehtimaan järjestelmiensä tietoturvasta.

Suomella on hyvät mahdollisuudet profiloitua korkean tietosuojan ja tietoturvan maana, mikä tuo verkkotietopalveluyrityksille taloudellisesti hyödynnettävää lisäarvoa[70]. Mielikuvaan Suomesta tiedon turvasatamana voidaan vaikuttaa lainsäädäntö- ja viranomaistoimin. Tämä tarkoittaa, että Suomi voi lainsäädännön keinoin saavuttaa aseman korkean tietosuojan ja -turvan maana, jossa sääntely-ympäristö tarjoaa liiketoiminnan harjoittamiselle tarkoituksenmukaiset lähtökohdat.

Tavoitetta tulla tiedon turvasatamaksi on mahdollista tukea lakien soveltamisalan suunnitelmallisella mitoittamisella, yksiselitteisillä ja läpinäkyvillä säännöksillä sekä viranomaisen soveltamiskäytäntöjen ennakoitavuudella. Samalla on panostettava erityisesti tietoturvan toteutumiseksi tietoverkkohyökkäysten ja muiden tietoturvarikosten ennaltaehkäisyyn. Uutta tiedustelulainsäädäntöä luodessa on ehdottomasti ymmärrettävä tällaisen lainsäädännön mahdollinen vaikutus Suomi-kuvaan korkean tietosuojan maana. Uusia tietosuojaan vaikuttavia lakeja onkin harkittava erityisellä huolella myös Suomen kilpailukyvyn säilymisen kannalta.

[70] Ks. Information Technology and Innovation Foundation (ITIF) report, elokuu 2013. NSA-paljastuksilla oli merkittävä vaikutus Yhdysvalloissa toimivien pilvipalveluyritysten kilpailukykyyn ja tulokseen.

4 Tiedustelulainsäädäntö

4.1 Suomen verkkotiedustelulainsäädäntö

Suomessa ei ole tällä hetkellä voimassa varsinaista verkkotiedustelulainsäädäntöä eli lainsäädäntöä, jolla sallittaisiin viranomaisille tiedustelun harjoittaminen verkossa tapahtuvasta viestinnästä tai muusta siirrettävästä tiedosta. Näin ollen myöskään Suomen turvallisuusviranomaisilla ei ole lainsäädännön asettamia valtaoikeuksia kansalaisten strategiseen seurantaan. Ainoa massamittaista seurantaa sivuava lainsäädäntö on sähköistä viestintää välittäville yrityksille asetettu velvollisuus teletunnistetietojen säilyttämisestä. Tämä velvollisuus on implementoitu Suomeen EU:n sähköisen viestinnän tunnistetietojen säilyttämistä koskevasta direktiivistä 2006/24/EY[71] ensin Sähköisen viestinnän tietosuojalakiin 16.6.2004/516 ja sittemmin Tietoyhteiskuntakaareen 917/2014, joka kokoaa kaikki erilliset viestintää koskevat lait yhdeksi kokonaisuudeksi.

4.2 Teletietojen tallennusvelvollisuus

Teletietojen tallennusvelvollisuudesta säädetään tietoyhteiskuntakaaren 157 pykälässä, jonka mukaan teletoimintaa harjoittavalla yrityksellä on velvollisuus säilyttää teletunnistetiedot välittämästään viestinnästä tietyn laissa säädetyn ajan. Teletunnistetiedoilla tarkoitetaan tietoyhteiskuntakaaren määritelmän mukaan oikeus- tai luonnolliseen henkilöön yhdistettävissä olevaa tietoa, jota käsitellään viestin välittämiseksi sekä tietoa radioaseman tunnisteesta, radiolähettimen lajista tai käyttäjästä ja tietoa radiolähetyksen alkamisajankohdasta, kestosta tai lähetyspaikasta. Viranomainen ei voi kuitenkaan vaatia tietojen saamista haltuunsa ilman, että tuomioistuin myöntää luvan perustellun epäilyn perusteella tiettyjen pakkokeinolaissa (22.7.806/2011)[72] nimettyjen rikosten selvittämiseksi ja syyteharkintaan saattamiseksi.

---

[71] Euroopan parliamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006,yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta.

[72] Pakkokeinolain (22.7.806/2011) 10 luvun 6 §:n 2 momentissa luetellut rikokset.

Pakkokeinolain mukaisella televalvonnalla tarkoitetaan tunnistamistietojen hankkimista viestistä, joka on lähetetty yleiseen viestintäverkkoon tai siihen liitettyyn viestintäverkkoon kytketystä teleosoitteesta tai telepäätelaitteesta taikka vastaanotettu tällaiseen osoitteeseen tai laitteeseen sekä teleosoitteen tai telepäätelaitteen sijaintitiedon hankkimista taikka teleosoitteen tai telepäätelaitteen käytön tilapäistä estämistä.

Esitutkintaviranomaiselle voidaan antaa lupa kohdistaa televalvontaa rikoksesta epäillyn hallussa olevaan tai hänen oletettavasti muuten käyttämäänsä teleosoitteeseen tai telepäätelaitteeseen, jos epäiltyä on syytä epäillä:
1) rikoksesta, josta säädetty ankarin rangaistus on vähintään neljä vuotta vankeutta;
2) teleosoitetta tai telepäätelaitetta käyttäen tehdystä rikoksesta, josta säädetty ankarin rangaistus on vähintään kaksi vuotta vankeutta;
3) teleosoitetta tai telepäätelaitetta käyttäen tehdystä, automaattiseen tietojenkäsittelyjärjestelmään kohdistuneesta luvattomasta käytöstä, vahingonteosta, viestintäsalaisuuden loukkauksesta tai tietomurrosta;
4) seksikaupan kohteena olevan henkilön hyväksikäytöstä, lapsen houkuttelemisesta seksuaalisiin tarkoituksiin tai parituksesta;
5) huumausainerikoksesta;
6) terroristisessa tarkoituksessa tehtävän rikoksen valmistelusta, kouluttautumisesta terrorismirikoksen tekemistä varten tai terroristiryhmän rahoittamisesta;
7) törkeästä tulliselvitysrikoksesta;
8) törkeästä laittoman saaliin kätkemisestä;
9) panttivangin ottamisen valmistelusta; taikka
10) törkeän ryöstön valmistelusta.

Tietoyhteiskuntakaaren 157 §:n mukainen teletunnistetietojen säilytysvelvollisuus koskee tietoja, jotka liittyvät:
1) säilytysvelvollisen yrityksen tarjoamaan matkaviestinverkon puhelinpalveluun tai tekstiviestipalveluun mukaan lukien puhelut, joissa yhteys on saatu muodostettua, mutta puheluun ei vastattu tai puhelu on estynyt verkonhallintatoimenpiteestä johtuen;
2) säilytysvelvollisen yrityksen tarjoamaan internetpuhelinpalveluun, jolla tarkoitetaan palveluyrityksen tarjoamaa loppuasiakkaille asti internetyhteyskäytäntöön perustuvaa puhelun mahdollistavaa palvelua;

3) säilytysvelvollisen yrityksen tarjoamaan internetyhteyspalveluun.

Puheluihin liittyvä tietojen säilytysvelvollisuus koskee tilaajan ja rekisteröidyn käyttäjän nimeä ja osoitetta, liittymän tunnistetta sekä tietoa, jonka avulla voidaan yksilöidä viestintäpalvelun käyttäjä ja yksilöidä viestintätyypin, viestinnän vastaanottajan sekä viestinnän ajankohdan ja keston mukaan viestintätapahtumat mukaan lukien soitonsiirrot. Lisäksi matkaviestinverkkopalveluissa säilytysvelvollisuus koskee tietoa, jonka avulla voidaan yksilöidä viestintään käytetty laite sekä laitteen ja siinä käytetyn liittymän sijainti viestintätapahtuman alkaessa. Internetyhteyspalvelussa säilytysvelvollisuus koskee tilaajan ja rekisteröidyn käyttäjän nimeä ja osoitetta, liittymän tunnistetta ja asennusosoitetta sekä tietoa, jonka avulla voidaan yksilöidä viestintäpalvelun käyttäjä, viestintään käytetty laite sekä palvelun käytön ajankohta ja kesto.

Säilytettävät tiedot tulee Tietoyhteiskuntakaaren mukaan rajata vain siihen, mikä on palvelun tekninen toteutus huomioon ottaen välttämätöntä edellä mainittujen seikkojen yksilöimiseksi. Tietoyhteiskuntakaaressa todetaan erikseen, ettei säilytysvelvollisuus koske viestin sisältöä tai verkkosivustojen selaamisesta kertyviä välitystietoja.

Säilytysvelvollisuuden edellytyksenä on, että tiedot ovat saatavilla ja säilytysvelvollisen yrityksen yleisesti saatavilla olevien viestintäpalvelujen tarjoamisen yhteydessä Tietoyhteiskuntakaaren tai Henkilötietolain perusteella tuottamia tai käsittelemiä. Valtioneuvoston asetuksella voidaan antaa tarkempia tietoja säilytettävistä tiedoista. Tietojen teknisistä yksityiskohdista määrätään Viestintäviraston määräyksessä.

Tietoyhteiskuntakaaren 158 §:n mukaan säilytysvelvollisen yrityksen tulee ennen säilytysvelvollisuuden toteuttamista neuvotella sisäministeriön kanssa tietojen säilyttämistä koskevista viranomaisten tarpeista. Säilytysvelvollinen yritys päättää, miten tietojen säilytys teknisesti toteutetaan. Tiedot on kuitenkin säilytettävä kustannustehokkaasti. Tietojen säilytyksessä on huomioitava myös säilytysvelvollisen yrityksen liiketoiminnan tarpeet ja järjestelmien tekniset ominaispiirteet sekä maksuvelvollisen viranomaisen tarpeet. Tarkoituksena on pyrkiä siihen, ettei samoja tietoja säilytetä monessa yrityksessä.

Säilytysvelvollisen yrityksen velvollisuutena on huolehtia tietoturvasta Tietoyhteiskuntakaaren mukaisesti[73]. Säilytysvelvollisen yrityksen tulee nimetä joko tietojen käsittelyyn oikeutetut henkilöt tai ne tehtävät, joissa tietoja saa käsitellä. Säilytysvelvollisen yrityksen tulee myös huolehtia siitä, että tietojen säilyttämisestä ja sen tarkoituksesta on tietoa tilaajan saatavilla.

Tietoyhteiskuntakaaren 158 §:n mukaan säilytettävät tiedot on voitava toimittaa viranomaiselle ilman tarpeetonta viivästystä. Säilytysvelvollisen yrityksen tulee tarvittaessa olla yhteistyössä verkkoyrityksen kanssa siten, että myös ne saatavilla olevat teletunnistetiedot säilytetään, joita verkkoyritys käsittelee säilytysvelvollisen yrityksen palvelun toteuttamiseksi. Valtioneuvoston asetuksella voidaan tarkentaa Tietoyhteiskuntakaaren määräyksiä teletunnistetietojen säilyttämisvelvollisuuden toteuttamisesta. Lisäksi viestintävirasto voi antaa määräyksiä tietojen säilyttämisen teknisestä toteutuksesta ja tietoturvasta.

Teletunnistustietojen tallentamista ja käyttöä viranomaistarkoituksiin valvotaan Tietoyhteiskuntakaaren 159 §:ssä säädetyllä tilastointivelvollisuudella. Sisäministeriön on toimitettava eduskunnan oikeusasiamiehelle vuosittain tilastot teletunnistetietojen hyödyntämisestä. Tilastojen tulee tietoyhteiskuntakaaren mukaan sisältää:
1) tapaukset, joissa säilytettyjä tietoja toimitettiin viranomaiselle;
2) tapaukset, joissa säilytettyjä tietoja koskevaa viranomaisen tietopyyntöä ei voitu täyttää;
3) tiedot siitä, kuinka kauan kului säilytettävien tietojen tallentamisesta viranomaisen tietopyyntöön.
Sisäministeriön on lisäksi huomioitava nämä tilastot televalvonnan ja telekuuntelun käytöstä eduskunnan oikeusasiamiehelle antamissaan kertomuksissa, jotka ministeriö laatii poliisilain (872/2011), pakkokeinolain tai muun lain perusteella.

Tietoyhteiskuntakaaren myötä tietosuoja uudistui muun muassa siten, että luottamuksellisen viestinnän soveltamisala laajentui kaikkiin viestinnän välittäjiin eli myös sosiaaliseen median ja vastaaviin. Samalla uudistuksessa tunnistamistiedon käsite korvattiin välitystiedon käsitteellä. Tämä on merkittävä tietosuojaan kohdistuva uudistus sikäli, että tunnistamistieto on osa henkilötietojen kokonaisuutta, jota valvoo

[73] Ks. velvollisuuksista tarkemmin tietoyhteiskuntakaari 247§.

tietosuojavaltuutettu. Välitystietojen käsittely ja suojaaminen on puolestaan viestintäviraston valvonnassa.[74]

Uudistuksena aikaisempaan, Sähköisen viestinnän tietosuojalaissa olleeseen teletunnistetietojen säilytysvelvollisuuteen Tietoyhteiskuntakaari myös mahdollistaa yhden kokonaisrekisterin rakentamisen teletunnistetiedoista. Lain 158 §:n mukaan sisäministeriöllä on oikeus hankkia ulkopuoliselta palveluntarjoajalta järjestelmä, johon säilytysvelvollisuuden piiriin kuuluvat tiedot voidaan siirtää. Säilytysvelvollisella yrityksellä on oikeus tallentaa järjestelmään myös ne tiedot, joiden käsittely omaa tarvetta varten ei ole vielä päättynyt.

Muutos aikaisempaan lainsäädäntöön on oleellinen kahdesta näkökulmasta. Ensinnäkin kerätystä rekisteristä voidaan selvittää kaikkien suomalaisten kommunikaatiohistoria. Tämä saattaa aiheuttaa vakavan tietovuotoriskin, mikäli rekisteriin onnistutaan murtautumaan jonkin kolmannen osapuolen toimesta. Tietojen säilytys toisistaan erillisten teleoperaattoreiden järjestelmistä sekä hajauttaa että pienentää tietoturvariskiä verrattuna yhteen yhtenäiseen, kaikki tiedot kokoavaan rekisteriin. Toinen rekisterin aiheuttama tietoturvaongelma on se, että keskittäminen mahdollistaa kommunikaatiotietojen louhimisen järjestelmästä samaan tapaan kuin NSA:n suorittamassa vakoilussa. Aikaisemmassa hajautetussa järjestelmässä tämä ei ollut mahdollista.[75]

Kyseessä ei siten ole vain tekninen muutos kommunikaatiotietojen säilyttämiselle, vaan potentiaalinen tietoturvaongelma. Järjestelmä tarjoaa mahdollisuuden kansalaisten hyvin kattavaan seurantaan ja profilointiin.[76] Verkkotietopalveluyrityksen näkökulmasta kyseessä on merkittävästi asiakkaiden luottamuksen muodostumiseen liittyvä asia.

[74] Neuvonen s.155.
[75] Ville Oksanen 2014, Suomi ja verkkovalvonta s.15.
[76] Sama.

4.3 EU:n tuomioistuimen tallennusvelvollisuutta koskeva tuomio

Käytännössä teleliikennetietojen laajan tallennusvelvollisuuden seurauksena EU:ssa on kerätty kansalaisten välisestä viestinnästä vastaavat tiedot kuin laajasti kritisoidussa NSA:n PRISM-ohjelmassa[77].[78] Tällä hetkellä tallennusvelvollisuuden kohtalo on kuitenkin kokonaisuudessaan epäselvä. EU:n tuomioistuin on todennut 8.4.2014 antamassaan päätöksessä yhdistetyissä asioissa Digital Rights Ireland Ltd (C-293/12) ja Seitlinger ym.(C-594/12), että tallennusvelvollisuuden asettava direktiivi on vastoin EU-oikeutta ja siten pätemätön.

Tuomioistuimen päätös merkitsee sitä, että jatkossa tallennusvelvollisuuden asettavalla direktiivillä ei ole oikeusvaikutuksia. Päätös ei kuitenkaan edellytä jäsenmaita poistamaan tallennusvelvollisuutta lainsäädännöstään, sillä sähköisen viestinnän tietosuojadirektiivi 2002/58/EY luo tallennusvelvollisuudelle edelleen oikeudellisen puitekehyksen. Tuomioistuimen päätös kuitenkin velvoittaa siihen, että tallennusvelvollisuutta koskeva järjestelmä on selkeä ja tarkkarajainen.

Tuomioistuin toteaa tuomiossaan, että unionin lainsäätäjä on tallennusvelvollisuutta koskevan direktiivin säätäessään ylittänyt ne rajat, joita suhteellisuusperiaatteen noudattaminen olisi EU:n perusoikeuskirjan 7 ja 8 artiklan sekä 52 artiklan 1 kohdan kannalta edellyttänyt.

Tietoyhteiskuntakaarta säädettäessä perustuslakivaliokunta antoi lausunnon säädösehdotuksen teletunnistetietojen säilytysvelvollisuutta koskevasta 19 luvusta.[79] Lausunnossaan perustuslakivaliokunta ottaa kantaa myös Unionin tuomioistuimen tuomioon. Perustuslakivaliokunnan mukaan tuomio ei estä säätämästä direktiivin kattamasta asiasta kansallisessa lainsäädännössä. Kansallinen lainsäädäntö ei voi kuitenkaan saada sisältöään pätemättömästä direktiivistä eikä se sinällään voi perustua oikeusvaikutuksensa menettäneeseen direktiiviin. Perustusvaliokunnan mukaan on kuitenkin selvää, että myös kansallista lainsäädäntöä säädettäessä on

[77] Yhdysvaltojen PRISM-vakoiluohjelma antoi NSA:lle ja FBI:lle pääsyn Microsoftin, Yahoon, Applen, Googlen, Facebookin, Skypen ja Youtuben tiedostoihin.
[78] Vesa Viljanen, Yksityisyydensuojan parantaminen tietoverkoissa, 2013.
[79] Perustuslakivaliokunnan lausunto PeVL 18/2014 vp - HE 221/2013 vp.

huomioitava Suomen perusoikeussäännösten lisäksi myös Unionin tuomioistuimen päätöksessä käsitellyt EU:n peruskirjan 7 artiklan ja 8 artiklan määräykset yksityiselämän ja henkilötietojen suojasta. Tuomioistuimen esittämät huomiot muodostavat valiokunnan valtiosääntöisen arvioinnin perustan. Perustuslakivaliokunta toteaa lausunnossaan, että kansallisen sääntelyn on täytettävä tuomiossa mainitut edellytykset, vaikka tuomio ei suoranaisesti koskekaan kansallista täytäntöönpanolainsäädäntöä.[80]

Tuomion johdosta perustuslakivaliokunta joutuu arvioimaan uudelleen sähköisessä viestinnässä saatavien tunnistamistietojen säilyttämistä ja käyttöä koskevaa käytäntöään, joka kohdistuu perustuslain 10 §:ssä turvattuihin yksityiselämän ja henkilötietojen suojan sekä luottamuksellisen viestin salaisuuden suojaan. Tällaista käytäntöä on esimerkiksi viestin tunnistamistietojen katsominen luottamuksellisen viestin salaisuutta suojaavan perusoikeuden ydinalueen ulkopuolelle[81]. Mahdollisuus koota ja yhdistellä tunnistamistietoja on kuitenkin siinä määrin merkittävää puuttumista yksityisyyden suojaan, ettei tällainen yksinkertainen jaottelu suojan reuna- ja ydinalueeseen ole välttämättä enää mahdollista.[82]

Unionin tuomioistuin nostaa tuomiossaan esille direktivin oikeasuhtaisuutta pohtiessaan kolmenlaisia ongelmia. Ensinnäkin direktiivin soveltamisala on liian laaja, sillä se kattaa rajoituksetta kaikki henkilöt, sähköisen viestinnän välineet ja viestintätiedot. Toiseksi direktiivissä ei säädetä objektiivisista perusteista, joiden nojalla tietojen vastaanottajien piiriä ja tietojen käyttöä voitaisiin rajoittaa. Direktiivistä puuttuvat myös aineelliset ja menettelylliset edellytykset, joilla toimivaltaiset kansalliset viranomaiset voivat saada ja käyttää tietoja. Kolmanneksi tietojen säilytysaikoja ei ole sidottu tietojen hyödyllisyyteen tai kyseessä oleviin henkilöihin. Säilyttämisen kesto ei myöskään perustu objektiivisin perustein täysin välttämättömään säilytykseen.

Huomionarvoista on, että tuomioistuimen mainitsemat puutteet direktiivissä vastaavat luvussa 2.1 käsiteltyjä edellytyksiä ihmisoikeuksien noudattamisesta viestinnän valvonnassa. Direktiivistä puuttuvat selvät ja täsmälliset säännöt, joilla perusoikeuksiin puuttumisen laajuus voitaisiin rajata. Tämän lisäksi tuomioistuin kiinnitti huomiota

[80] Sama.
[81] Ks. esim. PeVL 33/2013 vp, s. 3/I, PeVL 6/2012 vp , s. 3-4, PeVL 29/2008 vp , s. 2/II ja PeVL 3/2008 vp , s. 2/I.
[82] Perustuslakivaliokunnan lausunto PeVL 18/2014 vp - HE 221/2013 vp.

siihen, että direktiivistä puuttui riittävä suoja tietojen väärinkäyttöä vastaan eikä siinä edes edellytetty tietojen säilyttämistä EU-alueella.

Perustuslakivaliokunnan mukaan Unionin tuomioistuimen tuomiosta ei ole saatavilla suoraa sääntöä siihen millaista kansallisen lainsäädännön tulee olla, jotta se täyttää yksityiselämän ja henkilötietojen suojaan liittyvät oikeasuhtaisuusvaatimukset, sillä tuomio perustuu kokonaisarvioon kyseessä olevasta direktiivistä. Valiokunnan mukaan oikeasuhtaisuusvaatimuksen vastaisena on kuitenkin lähtökohtaisesti pidettävä sääntelyä, joka johtaa laajamittaiseen, erittelemättömään, pitkäaikaiseen ja rajoittamattomaan tietojen säilyttämiseen yhdistettynä rajoittamattomaan pääsyyn näihin tietoihin. Kansallisessa lainsäädännössä tietojen säilytyksen ja käytön rajoituksista on säädettävä direktiiviä täsmällisemmin.[83]

Lausuntonaan perustuslakivaliokunta esitti, että tietoyhteiskuntakaaren tallennusvelvollisuudesta voidaan säätää tavallisen lain säätämisjärjestyksessä vain, jos valiokunnan valtiosääntöoikeudelliset huomautukset otetaan huomioon. Ensinnäkin sääntelyä on täsmennettävä oleellisesti. Tietojen säilytysaika (enintään 12 kuukautta) ja käyttötarkoitus (liityntä pakkokeinolain 10 luvun 6 §:n 2 momentissa tarkoitettuihin rikoksiin) on mainittava sääntelyssä selkeästi. Vastaavasti kuin säilytysvelvollisuuden myös tallennusmahdollisuuden edellytyksenä tulee olla että tiedot ovat saatavilla ja säilytysvelvollisen yrityksen yleisesti saatavilla olevien viestintäpalvelujen tarjoamisen yhteydessä Tietoyhteiskuntakaaren tai Henkilötietolain (523/1999) perusteella tuottamia tai käsittelemiä[84].

Valiokunnan lausunnon mukaan tallennettavien tietojen listan on oltava tyhjentävä. Tallentaminen voidaan sallia vain, jos se on nimenomaisesti palvelun teknisen toteutuksen vuoksi välttämätöntä käyttäjän tunnistamiseksi. Teleyrityksen ei voida edellyttää luovuttavan tietoja käyttäjästä yhtään laajemmin kuin se on käyttäjän tunnistamiseksi välttämätöntä.

Valiokunta korostaa lausunnossaan, että verkkosivustojen selaamistietojen tallentaminen viranomaistarpeita varten on merkittävä tieto käyttäjän yksityisyyden

[83] Perustuslakivaliokunnan lausunto PeVL 18/2014 vp - HE 221/2013 vp.
[84] Perustuslakivaliokunnan lausunto PeVL 18/2014 vp - HE 221/2013 vp, HE 221/2013 vp.

suojan näkökulmasta. Koska tallentaminen on vapaaehtoista ja teleyrityksissä on käytössä erilaisia teknologioita valiokunta olettaa lausunnossaan, että kaikki teleyritykset eivät käytä lain sallimaa tallennusmahdollisuutta. Perustuslakivaliokunta toteaakin lausunnossaan pitävänsä tärkeänä, että selaamistietoja viranomaistarpeita varten säilyttävät teleyritykset huolehtivat tilaajien saavan tiedon tietojensa tallentamisesta. Voimassa olevassa Tietoyhteiskuntakaaren 157 §:ssä selaamistietojen tallentaminen suljetaan kokonaan säilytysvelvollisuuden ulkopuolelle. Säännöksessä todetaan yksiselitteisesti, ettei säilytysvelvollisuus koske viestin sisältöä eikä verkkosivustojen selaamisesta kertyviä välitystietoja.

4.4 Katsaus Ruotsin verkkotiedustelusääntelyyn

4.4.1 Sääntely yleisesti

Ruotsin puolustushallinnon harjoittamaa yleistä tiedustelutoimintaa sääntelevät sotilastiedustelusta annettu yleislaki ja sitä täydentävä asetus sekä tiedustelua koskevat erityislait[85]. Puolustusvoimien (Försvarsmakten) lisäksi sotilastiedustelua harjoittavat puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA), puolustusvoimien materiaalilaitos (Försvaretsmaterielverk, FMV) ja kokonaismaanpuolustuksen tutkimusinstituutti (Totalförsvarets forskningsinstitut, FOI). Kaikki nämä organisaatiot toimivat puolustusministeriön alaisina.[86]

Puolustustiedustelulain mukaan tiedustelua voidaan harjoittaa vain Ruotsin ulko-, turvallisuus- ja puolustuspolitiikan tueksi ja Ruotsiin kohdistuvien ulkoisten uhkien kartoittamiseksi ja se saa koskea vain ulkomaisia olosuhteita. Tiedustelutoiminnalla myötävaikutetaan myös Ruotsin osallistumiseen kansainväliseen turvallisuusyhteistyöhön. Tiedustelutoiminnan yleisestä kohdentamisesta päättää aina hallitus. Yleisen kohdentamisen puitteissa hallituksen erikseen nimeämät viranomaiset voivat antaa kohdistusta tarkentavia määräyksiä.[87]

[85] 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.
[86] Tiedonhankintalakityöryhmän mietintö, s.37.
[87] Lag om försvarsunderrättelseverksamhet (2000:130) 1§.

Tiedustelun tarkoitus on hankkia, työstää ja analysoida tietoja, jotka hankitaan teknisesti tai henkilötiedustelulla sekä avoimista että muista lähteistä. Kerätyt tiedot raportoidaan asianomaisille viranomaistahoille. Tiedustelutoimintaa harjoittavat viranomaiset voivat hallituksen tarkempien määräysten mukaan tehdä yhteistyötä tiedustelutoiminnan alalla muiden maiden ja kansainvälisten organisaatioiden kanssa.[88]

Tiedustelu ei voi ottaa hoitaakseen sellaisia tehtäviä, jotka lain tai muiden säädösten mukaan kuuluvat poliisin, turvallisuuspoliisin tai muiden lainvalvontaviranomaisten rikostorjunta- tai estämistoimivaltaan. Tällä tarkoitetaan puolustustiedustelutoiminnasta annetun lain esitöiden[89] mukaan sitä, ettei tiedustelussa saada muuta lainsäädäntöä kiertämällä käyttää sellaisia esitutkinta- tai pakkokeinotoimivaltuuksia, joiden käyttöalasta ja käytön edellytyksistä säädetään oikeudenkäymiskaaressa ja esimerkiksi poliisilaissa. Tiedustelulla voidaan kuitenkin antaa tukea muille viranomaisille rikosten torjumiseksi, mikäli lainsäädännössä ei ole tälle esteitä[90].

Puolustustiedustelusta annetun lain esitöiden mukaan[91] turvallisuuspoliisin työ on nykyisin monilta osin tiedustelupalvelunomaista ja suuntautuu myös ulkomailla harjoitettavaa Ruotsin turvallisuutta vaarantavaa toimintaa koskevien tietojen hankintaan. Tähän tehtäväkokonaisuuteen liittyen turvallisuuspoliisin on voitava hyödyntää myös tiedustelusta vastaavien viranomaisten tiedonhankintakapasiteettia.[92]

Tiedustelua harjoittavilla viranomaisilla on puolustustiedustelutoiminnasta annetun asetuksen mukaan velvollisuus raportoida puolustusministeriölle muun muassa tiedustelutoiminnan yleisestä suuntautumisesta, suurista ja tärkeistä tapahtumista, kansainvälisessä yhteistyössä nousseista erityisistä kysymyksistä sekä erityisillä tiedonhankintakeinoilla tehtävästä tiedustelusta. Erityisillä tiedonhankintakeinoilla viitataan lain esitöiden mukaan pääasiallisesti henkilö ja signaalitiedusteluun[93].

---

[88] Lag om försvarsunderrättelseverksamhet (2000:130) 3§.
[89] Regeringens proposition 1999/2000:25.
[90] Lag om försvarsunderrättelseverksamhet (2000:130) 4§.
[91] Regeringens proposition 2006/07:63: ”En anpassad försvarsunderrättelseverksamhet”.
[92] Tiedonhankintalakityöryhmän mietintö, s.37-38.
[93] Regeringens proposition 2006/07:63: ”En anpassad försvarsunderrättelseverksamhet”.

Tiedusteluviranomaisten tulee myös tehdä vuosittain menneen vuoden tiedustelutoiminnasta julkinen yleiskatsaus[94]. Puolustustiedustelutoiminnan harjoittamista valvoo valtion tiedustelutarkastus (statens inspektion för försvarsunderrättelseverksamheten, SIUN)[95]. SIUN tehtävänä on valvoa muun muassa lain noudattamista, tiedustelun kohdentamista ja tiedonhankinnassa käytettyjä menetelmiä[96].

4.4.2 Signaalitiedustelu

Ruotsin harjoittamasta tiedustelusta on kirjoitettu lehdissä usein[97]. Tällöin kyseessä on yleensä signaalitiedustelu, jota harjoittaa Ruotsin puolustusministeriön alainen siviiliorganisaatio puolustusvoimien radiolaitos (Försvarets radioanstalt, FRA). FRA ei ole osa puolustusvoimia, vaan sen henkilökunta koostuu siviileistä. FRA:n toimenkuvaan kuuluu tiedustelutietojen hankkiminen saatujen toimeksiantojen mukaisesti ja hankittujen tietojen välittäminen toimeksiantajien käyttöön. Tätä signaalitiedustelua säädellään kahdella erityislailla ja -asetuksella[98].[99]

Aiemmin FRA:lla oli oikeus seurata vain radioliikennettä, mutta 8.3.2007 valtiopäiville annettiin lakimuutoesitys, jossa kuunteluoikeutta esitettiin laajennettaksi myös tietoverkkoihin. Esityksestä syntyneen julkisen keskustelun vuoksi lain valmistelua siirrettiin vuodella. Toisaalta lain sanottiin johtavan totalitarismiin ja valvontayhteiskuntaan ja toisaalta sitä pidettiin välttämättömänä työkaluna terrorismin ja kansainvälisten verkkouhkien torjunnassa.

---

[94] Förordning (2000:131) om försvarsunderrättelseverksamhet 8 §.

[95] Ks. Förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten.

[96] Förordning (2009:969) med instruktion för Statens inspektion för försvarsunderrättelseverksamheten 4§.

[97] Petteri Järvinen, NSA Näin meitä Seurataan, 2014, s.140.

[98] 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.

[99] Petteri Järvinen, NSA Näin meitä Seurataan, 2014, s.140, Tiedonhankintalakityöryhmän mietintö, s.38.

Ruotsin parlamentti hyväksyi lopulta 18.6.2008 täpärästi niin sanotun FRA-lain eli Ruotsin signaalitiedustelulain (2008:717). Tämän jälkeen lakiin tehtiin vielä joitakin kansalaisten tietosuojaa parantavia tiukennuksia ja lopullisessa muodossaan laki astui voimaan 1.12.2009[100].

Signaalitiedustelulaissa signaalitiedustelulla tarkoitetaan elektronisessa muodossa olevien signaalien hakemista. Tämä tekniikkaneutraali määritelmä sisältää kaikki signaalitiedustelun menetelmät, kuten esimerkiksi kaapeli- ja radiosignaalitiedustelun sekä manuaalisen ja automaattisen tiedonkeräämisen. Signaalitiedustelussa on neljä osiota: tiedustelun kohdennus, tietojen keräys, käsittely ja raportointi.[101]

Signaalitiedustelua voidaan harjoittaa vain, jos sekä yleisessä puolustustiedustelulaissa että signaalitiedustelua koskevassa erityislaissa olevat ehdot täyttyvät. Yleisenä edellytyksenä on, että kyseessä on Ruotsin ulko-, turvallisuus ja puolustuspolitiikkaa tukeva, ulkomaisia olosuhteita koskeva tiedustelutehtävä, jossa kartoitetaan Ruotsiin kohdistuvia ulkoisia uhkia. Nämä ulkoiset uhat ja tilanteet, joiden kartoittamiseksi signaalitiedustelua saadaan käyttää, luetellaan signaalitiedustelulaissa[102].

Jos toiminnan kannalta on välttämätöntä, tietoja voidaan hankkia myös signaaliympäristössä, teknisessä kehityksessä ja signaalisuojassa tapahtuvien muutosten seuraamiseksi sekä tiedonhankinnassa käytettävän tekniikan ja menetelmien kehittämiseksi. Signaalitiedustelu koskee vain Ruotsin rajat ylittävää viestintää. Signaalia ei saa kerätä, jos signaalin vastaanottaja ja lähettäjä ovat Ruotsissa.[103]

---

[100] Laki herätti yleistä keskustelua myös Suomessa ja sen vaikutuksista jätettiin kirjallinen kysymys KK 558/200 hallitukselle. Huhtikuussa 2008 TeliaSonera Finland Oyj siirsi liikenne- ja viestintäministeriön pyynnöstä Suomen sisäisen viestiliikenteen sähköpostipalvelimet Ruotsista Suomeen. Tätä ennen osa Suomen sisäisestä sähköpostiliikenteestä kierrätettiin Ruotsin kautta.

[101] Tiedonhankintalakityöryhmän mietintö, s.38.

[102] Signaalitiedustelulain 1 §:n mukaan tällaisia tilanteita ovat: 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.

[103] Signaalitiedustelulaki 1-2 §.

FRA voi aloittaa signaalitiedustelun vain valtioneuvoston, valtioneuvoston kanslian, puolustusvoimien, keskusrikospoliisin tai suojelupoliisin toimeksiannosta. Tällaista toimeksiantoa ei voida kohdistaa yksinomaan tiettyyn luonnolliseen henkilöön.[104]

Signaalitiedustelulle on haettava aina lupa erityistuomioistuimena toimivalta puolustustiedustelutuomioistuimelta. Lupahakemuksen tulee sisältää kuvaus tiedustelutehtävästä, tieto siitä, mihin kaapelin kuituihin tiedonhankinta halutaan kohdistaa, käytettävät hakuehdot, luvan kesto ja yleiset olosuhteet, joihin signaalitiedusteluviranomainen haluaa vedota. Signaalitiedustelulaissa annetaan tarkat edellytykset sille, milloin tuomioistuin voi myöntää luvan, ja mitä luvasta tulee käydä ilmi. Luvan saadakseen tiedustelutoiminnan tulee olla lainmukaista ja rajoittaa mahdollisimman vähän yksityisyyttä. Vastaavasti tavoiteltavan tiedon tulee olla suhteessa arvokkaampaa kuin rajoitukset yksityisyyteen. Luvasta tulee käydä ilmi tiedonhakutehtävä, mitä kaapeleiden kuituja lupa koskee, mitä hakuehtoja tai hakuehtokategorioita[105] saa käyttää, luvan kesto ja muut ehdot, joita tarvitaan yksittäisen henkilön yksityisyyden suojaan puuttumisen rajoittamiseksi.

Yksityisyyden suojan toteutumiseksi signaalitiedustelulaissa on rajoitettu yksittäiseen luonnolliseen henkilöön viittaavien hakuehtojen käyttöä. Tällaisen hakuehdon käyttö on mahdollista vain, jos se on erityisen tärkeää tiedustelutoiminnalle. FRA:n tulee aina antaa selvitys signaalitiedustelua valvovalle valtion tiedustelutarkastukselle yksityiseen ihmiseen viittaavan hakuehdon käytöstä. Henkilölle itselleen tulee ilmoittaa niin pian kuin mahdollista ja viimeistään kuukausi tiedustelutehtävän päättymisestä, milloin ja missä tarkoituksessa tiedustelu on toteutettu, elleivät salassapitomääräykset tätä estä.[106]

Signaalitiedustelu edellyttää tietoliikenneoperaattoreilta avustavia toimenpiteitä. Tietoliikenneoperaattoreilla on velvollisuus viedä Ruotsin rajat ylittävä tietoliikenne määritettyyn yhteyspisteeseen tai -pisteisiin. Lisäksi operaattoreilla on velvollisuus

[104] Signaalitiedustelulaki 4 §.
[105] Hakuehdoilla tarkoitetaan lain esitöiden mukaan 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. (Regeringens proposition 2006/07:63, s. 76–77.)
[106] Signaalitiedustelulaki 11 a - 11 b §.

luovuttaa viranomaiselle sellaiset tiedot, jotka helpottavat signaalien haltuunottoa. Operaattoreiden tulee toimia salassapitosäännöksiä vaarantamatta.[107]

Operaattoreiden yhteyspisteisiin viemään tietoliikenteeseen pääsee vain valvontaviranomaisena toimiva valtion tiedustelutarkastus. Se erottelee ja luovuttaa FRA:lle pääsyn vain tuomioistuimen luvassa yksilöityihin kaapelikuituihin, joihin FRA kohdistaa hakunsa.[108] FRA raportoi keräämänsä tiedot asianomaisille viranomaisille[109].

Yksityisyyden suojan toteutumista valvoo FRA:n tietosuojaneuvosto (Integritetsskyddsråd). Neuvosto raportoi havainnoistaan FRA:n johdolle sekä tarpeen mukaan valtion tiedustelutarkastukselle. Neuvoston ohella signaalitiedustelua valvovat tietosuojavaltuutettu (Datainspektion), eduskunnan oikeusasiamies ja oikeuskansleri. Valtion tiedustelutarkastuksen suorittama valvonta kohdistuu erityisesti signaalitiedustelun hakuehtojen käyttöön, tietojen hävittämiseen ja raportointiin. Luvan vastainen tiedustelutoimenpide voidaan määrätä lopetettavaksi ja tiedot tuhottaviksi. Luonnollisen henkilön pyynnöstä tiedustelutarkastus selvittää, onko henkilön viestejä seurattu ja onko seuranta noudattanut lakia. Signaalitiedustelua käyttämällä kerättyjen henkilötietojen käsittelystä on säädetty erillinen laki[110].[111]

FRA:n harjoittamalla signaalitiedustelulla on merkitystä myös Suomessa toimiville verkkotietopalveluyrityksille. Signaalitiedustelulain mukaan FRA:lla on oikeus seurata ja kuunnella kaikkea Ruotsin läpi kulkevaa viestiliikennettä. Merkittävä osa suomalaisten ulkomaille suuntautuvasta viestinnästä (puhelut, tekstiviestit, sähköpostit, Internet-selaus jne.) kulkee Ruotsin kautta, mikä tarkoittaa, että FRA voi

[107] Lag (2003:389) om elektronisk kommunikation 19 a §.
[108] Signaalitiedustelulaki 12 §. Pykälää muutettiin lailla 2009:967, jota koskee hallituksen esitys Prop 2008/09:21 Förstärkt integritetsskydd vid signalspaning. Aiemmin FRA keräsi tiedot yhtyeyspisteessä. Muutoksen perusteena oli signaalitiedustelun uskottavuuden lisääminen. Signaalitiedusteluviranomaisella voi olla pääsy vain niihin kaapeleiden kuituihin, joita luvat koskevat.
[109] Signaalitiedustelulaki 8§.
[110] Lag (2007:259) om behandling av personuppgifter i Försvarets radioanstalts försvarsunderrättelse- och utvecklingsverksamhet.
[111] Signaalitiedustelulaki 11 §, Tiedonhankintalakityöryhmän mietintö, s.39-40.

valvoa käytännössä kaikkea suomalaisten televiestintää, jos viestinnän toinen osapuoli on Suomen rajojen ulkopuolella.[112]

Myös Ruotsi on sitoutunut kansainvälisiin ihmisoikeussopimuksiin, jotka sisältävät oikeuden yksityisyyteen ja viestisalaisuuteen. Koska signaalitiedustelulaki on säädetty nimenomaan torjumaan Ruotsin valtioon kohdistuvia ulkoisia uhkia, kansainväliset säännökset kuitenkin sallivat kyseessä olevan sääntelyn ja sen aiheuttamat vaikutukset suomalaiseen yksityisyyden suojaan.[113]

[112] www.yksityisyydensuoja.fi/lainsäädäntö, Petteri Järvinen, NSA Näin meitä Seurataan, 2014, s.140.
[113] KK 558/2008 vastaus.

5 Uhkia ja mahdollisuuksia

5.1 Verkkotiedustelulakihanke

Elokuussa 2015 pidetyssä strategiakokouksessaan Suomen hallitus on päättänyt aloittaa siviili- ja sotilastiedustelulainsäädännön valmistelutyön.[114] Lainsäädäntöhankkeen taustalla on edellisen hallituksen käynnistämä hanke, jonka päätöksenä julkaistiin tiedustelutoimintaa pohtiva työryhmämietintö.

Hallitusohjelman mukaan kasvavat riskit ja uudet uhat edellyttävät koko yhteiskunnalta uudenlaista valmiutta ja varautumista. Tällaisina uusina, laajalle alueelle vaikuttavina uhkina hallituksen esityksessä mainitaan erityisesti hybridivaikuttaminen, kyberhyökkäykset ja terrorismin torjunta. Hallituksen tavoitteena on vahvistaa kokonaisturvallisuusajattelua kansallisesti, EU:ssa ja kansainvälisessä yhteistyössä. Hallitus esittää ohjelmassaan säädösperustaa ulkomaantiedustelulle ja tietoliikennetiedustelulle painottaen kuitenkin samalla perus- ja ihmisoikeuksien toteutumista.[115]

Hallitusohjelmaan perustuen hallitus päätti strategiakokouksessaan, että sisäministeriön ja puolustusministeriön toimesta selvitetään, mitä vaihtoehtoisia tiedonhankintakeinoja on olemassa, ja käynnistetään lainsäädäntövalmistelu koskien siviili- ja sotilastiedustelua. Oikeusministeriön tehtävänä on ryhtyä toimenpiteisiin perustuslain tarkistamiseksi Suomen kansainvälisten ihmisoikeusvelvoitteiden määräämissä rajoissa siten, että kansallisen turvallisuuden suojaamiseksi välttämättömistä rajoituksista luottamuksellisen viestin salaisuuden suojaan voidaan säätää lailla tarpeellisina pidettävien edellytysten täyttyessä.[116]

Näiden lainsäädäntöhankkeiden toteuttamistavasta on sovittu liikenne- ja viestintäministeriön, oikeusministeriön, puolustusministeriön ja sisäministeriön välillä.

[114] Mediatiedote 21.8.2015.
[115] Hallitusohjelma 2015 s.35.
[116] Mediatiedote 21.8.2015.

Hankkeet käynnistyvät käytännössä kolmen lainsäädäntöä valmistelevan työryhmän asettamisella, joista kutakin johtaa oma ministeriönsä. Oikeusministeriön vastuulla on perustuslain mahdollista muuttamista koskeva hanke. Varsinaista tietoliikennetiedustelua koskevat lakihankkeet ovat sisäministeriön ja puolustusministeriön vastuulla.

Tietoliikennetiedustelu jakautuu siviilitiedusteluun ja sotilastiedusteluun. Näistä siviilitiedustelun tarkoituksena on torjua kansallista turvallisuutta vaarantavia vakavia siviililuontoisia uhkia, mikä liittyy sisäministeriön hallinnonalan tarpeisiin. Sotilastiedustelu puolestaan on osa puolustusvoimien tehtäviin liittyvän tilannekuvan muodostuksessa ja ylläpitämisessä, mikä liittyy puolustusministeriön hallinnonalan tarpeisiin.[117] Hallinnonalansa mukaisesti sisäministeriö johtaa siviilitiedustelua koskevaa lakihanketta, puolustusministeriö sotilastiedustelua koskevaa lakihanketta. Erillisiä hankkeita on tarkoitus valmistella tiiviissä yhteistyössä ja valmistelulle on varattu aikaa noin puolitoista vuotta.[118]

Näissä vireillä olevissa lainsäädäntöhankkeissa on tarkoitus huomioida viime hallituskaudella puolustusministeriön asettaman tiedonhankintalakityöryhmän mietintö ja sen liiteaineisto. Vuoden 2014 toiminut turvallisuusviranomaisten tiedonhankintaa koskevaa lainsäädäntöä kehittävä työryhmä arvioi Suomen kansallisen lainsäädännön nykytilaa ja kehitystarpeita tämänhetkisessä ja muuttuvassa turvallisuusympäristössä.[119]

Erityisesti työryhmän työ kohdistui turvallisuusviranomaisten tiedonhankintaa koskevien toimintaedellytysten ja toimivaltuudet selvittämiseen sekä kehitystarpeiden arviointiin. Kehitteillä olevan tiedustelulainsäädännön valmistelutyön kannalta oleellista on työryhmän päätelmä, että tiedustelutarkoituksessa toteutettavasta tietoliikennetiedustelusta ei näytä olevan mahdollista säätää perustuslakia muuttamatta. Ainoa lievä poikkeus tästä pääsäännöstä on Ruotsin mallin mukainen pelkästään vieraan valtion tietoliikenteeseen kohdistuva tiedustelu.[120]

[117] Puolustusministeriön tiedote 14.1.2015.
[118] Mediatiedote 21.8.2015.
[119] Sama.
[120] Sama.

Työryhmä ehdottaa mietinnössään harkittavaksi, että hallitus käynnistäisi tarvittavat toimenpiteet tiedustelua koskevan säädösperustan luomiseksi käynnistämällä yhden tai useampia lainsäädäntöhankkeita. Keskeiset osat tiedustelukeinojen kokonaisuutta ovat ulkomaantiedustelu ja tietoliikennetiedustelu. Mietinnöstä annetun tiedotteen mukaan työryhmässä vallitsi yhteisymmärrys tiedustelulainsäädännön tarpeesta ylipäänsä ja ulkomaan tiedustelusta. Tiedustelua ehdotetaan mietinnössä sekä oikeudellisesti että parlamentaarisesti valvottavaksi.[121]

Tiedustelulainsäädännöllä tavoitellaan helpotusta erityisesti puolustusministeriön tiedonhankintaan. Tarkoituksena on säätää puolustusvoimille oikeus kerätä tietoa kolmella eri tavoin: henkilö-, tietoliikenne- ja tietojärjestelmätiedustelulla.

Tiedustelulla pyritään saamaan kansallisen turvallisuuden kannalta välttämätöntä tiedustelutietoa vakavista kansainvälisistä uhista. Ulkomaan tiedustelussa tietoa ehdotetaan hankittavaksi sekä ulkomaisista tietojärjestelmistä että henkilökohtaisella kanssakäymisellä ja havainnoimalla henkilöä tai muuta kohdetta. Tietoliikennetiedustelu puolestaan on työryhmän mukaan Suomen rajat ylittävissä tietoliikennekaapeleissa liikkuvaan tietoliikenteeseen kohdistuvaa tiedustelua, jolla hankitaan tietoa Suomen kansallista turvallisuutta vaarantavista uhista.[122] Tällaista tietoa on esimerkiksi sähköpostiliikenne ja sosiaalisen median viestit. Tietojärjestelmiin kohdistuvan tiedustelun riskinä on, että se näyttäytyy muiden valtioiden näkökulmasta laittomana urkintana.

Tietosuojan osalta mietinnössä todetaan, että tietoliikennetiedustelua koskevan lainsäädännön valmistelua harkittaessa on erityisesti otettava huomioon perus- ja ihmisoikeutena turvattu luottamuksellisen viestin salaisuuden suoja. Tällä on vaikutusta myös verkkotietopalveluyritysten liiketoimintaan. Tiedustelulainsäädännön vaikutuksia arvioitaessa tulee mietinnön mukaan ottaa huomioon myös vaikutukset yhteiskunnan digitalisoitumiseen ja yritysten toimintaedellytyksiin. Työryhmä pitää lähtökohtanaan sitä, ettei yrityksille esitetä velvollisuutta luovuttaa salausavaimia tai asentaa ohjelmistoihin ja laitteistoihin takaportteja.[123]

[121] Puolustusministeriön tiedote 14.01.2015.
[122] Suomalaisen tiedustelulainsäädännön suuntaviivoja.
[123] Suomalaisen tiedustelulainsäädännön suuntaviivoja.

Mietinnössä suositetaan, että tietoliikennetiedustelun tekninen suorittaminen keskitetään yhdelle viranomaiselle ja toimeksiantajina toimisivat muut tahot. Tällaisiksi tahoiksi mietinnössä mainitaan uhkien torjunnasta vastaavat viranomaiset sekä niiden kautta Suomen ulko-, turvallisuus- ja puolustuspoliittisesta päätöksenteosta vastaavat tahot. Tätä ratkaisua puoltavat yhdenmukaisiin menettelytapoihin ja laillisuusvalvontaan liittyvät seikat.

Mietinnössä ehdotetaan myös harkittavaksi, säädetäänkö tietoliikennetiedustelusta erillislakina, koska lainsäädäntö on tarpeellinen kahdelle eri hallinnonalalle. Vastaavasti on toimittu esimerkiksi Ruotsissa[124]. Verkkotietopalveluyrityksiä koskien mietinnössä esitetään, että myös elinkeinoelämän edustus on mukana lainsäädännön valmistelussa. Tällöin myös sidosryhmien tarpeet tulevat huomioiduksi.[125]

Tiedustelulainsäädännön valmistelutyö on aiheuttanut huolta yksilön tietosuojan toteutumisesta sekä erityisesti siitä, valvooko joku puolueeton taho verkkovalvontaa suorittavia viranomaisia ja mikä elin mahdollisia tiedustelulupia tulee myöntämään, jos tiedustelu säädetään luvanvaraiseksi. Poliisihallitus on tältä osin esittänyt, että tiedustelulupa myönnettäisiin Helsingin käräjäoikeudessa, jonne myös tällä hetkellä on keskitetty salaisten tiedonhankintakeinojen erityisharkintaa. Poissuljettua ei myöskään ole, että tätä tarkoitusta varten perustettaisiin erityistuomioistuin.

5.2 EU:n tietosuojalainsäädännön uudistus

EU:ssa on parhaillaan vireillä mittava tietosuojalainsäädäntöuudistus, jonka tarkoituksena on luoda uusi tietosuoja-asetus ja mahdollisesti myös tietosuojadirektiivi. Lainsäädäntöhanke on ollut vireillä jo vuodesta 2012, jolloin Euroopan komissio teki esityksen tietosuojaa koskevan lainsäädännön kokonaisuudistuksesta. Vuonna 2013 julkaistiin Euroopan parlamentin LIBE-valiokunnan mietintö tietosuoja-asetuksesta, jonka Euroopan parlamentti hyväksyi keväällä 2014. Kesäkuussa 2015 lainsäädäntöhanke sai sysäyksen eteenpäin, kun Euroopan unionin oikeus- ja

[124] Ks. tästä enemmän luku 3.4.
[125] Suomalaisen tiedustelulainsäädännön suuntaviivoja.

sisäasioiden neuvosto hyväksyi kokouksessaan ehdotuksen yleiseksi tietosuoja-asetukseksi[126].

Lainsäädäntöhanke on nyt siinä vaiheessa, että komissio, parlamentti ja neuvosto ovat saaneet päätökseen kolmikantaneuvottelut asetuksen tekstistä ja asetuksen lopullinen sisältö hyväksyttiin Euroopan parlamentin kansalaisvapauksien sekä oikeus- ja sisäasioiden valiokunnan (LIBE) ylimääräisessä kokouksessa 17. joulukuuta 2015. Neuvosto ja Parlamentti hyväksyvät päätöksellään vielä viimeistellyt asetustekstit, ja lopullinen asetus tulee voimaan todennäköisesti kahden vuoden siirtymäajan jälkeen keväällä 2018.

Toteutuessaan asetus korvaa nykyisen vuonna 1995 annetun henkilötietodirektiivin[127]. Asetusehdotukseen sisältyy samoja tietosuojateemoja kuin nykyisessä henkilötietodirektiivissä muun muassa henkilötietojen käsittelyn periaatteet, käsittelyn lainmukaisuus, rekisteröidyn suostumuksen edellytykset ja arkaluonteisten tietojen käsittely, joita asetuksen on tarkoitus päivittää ja nykyaikaistaa.[128] Mikäli asetus hyväksytään, se tulee voimaan kahden vuoden siirtymäajan jälkeen eli aikaisintaan vuonna 2018.

Tietosuoja-asetuksella on kaksi keskeistä tavoitetta. Ensinnäkin ehdotuksella on tarkoitus luoda EU-alueelle yhtenäinen tietosuojakehys, joka harmonisoi nykyisen tietosuojalainsäädännön[129]. Tämä osaltaan vahvistaa merkittävästi henkilötietojen suojaa jäsenvaltioissa. Toteutuessaan asetus on jäsenvaltioissa suoraan

[126] Neuvosto 9565/15, Yleisnäkemys ehdotukseksi Euroopan parliamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta.

[127] Euroopan parliamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

[128] Regulation (EU) No XXX/2016
of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

[129] Ks. esim Komission tiedonanto Euroopan parliamentille ja neuvostolle - Tietosuojadirektiivin tehokkaampaa soveltamista koskevan työohjelman seurannasta KOM/2007/0087 lopullinen. Henkilötietodirektiivin implementoinnissa jäsenvaltioiden välillä on eroja kahdesta syystä. Joko jäsenvaltiot eivät ole implementoineet direktiiviä kansalliseen lainsäädäntöönsä direktiivin vaatimusten mukaisesti tai direktiivissä on tarkoituksella jätetty kansallista liikkumavaraa. Esimerkiksi tietosuojaperiaatteiden soveltamisalaa voidaan kansallisesti rajoittaa tietyissä olosuhteissa kuten direktiivin 13 artiklassa tärkeän yleisen edun suojaamiseksi.

sovellettavaa lainsäädäntöä. Toiseksi ehdotuksella tavoitellaan suotuisia vaikutuksia EU:n digitaalisten sisämarkkinoiden kehittymiselle. Vahva tietosuojalainsäädäntö tuo todennäköisesti luottamusta online-palveluihin ja kasvattaen niiden markkinoita. Alueellisesti tietosuoja-asetusta sovelletaan kaikkiin EU-alueella sijaitseviin rekisterinpitäjiin sekä tietyin edellytyksin kaikkiin EU-alueen ulkopuolisiin rekisterinpitäjiin niiden käsitellessä EU-alueella asuvien henkilötietoja[130].

Asetuksen keskeinen tavoite on vahvistaa rekisteröityjen eli henkilötietojen käsittelyn kohteiden tietosuojaa. Rekisteröidyn oikeuksia ovat asetuksen mukaan oikeus saada tietoa omien henkilötietojensa käsittelystä, oikeus saada virheelliset tiedot oikaistuksi, oikeus tulla unohdetuksi sekä oikeus saada tiedot poistetuksi ja kieltää tietojen käsittely. Rekisterinpitäjille ja käsittelijöille puolestaan asetus tuo velvollisuuden antaa avoimia ja helposti saatavia tietoja rekisteröidyille heidän tietojensa käsittelystä.[131]

Yksi lähtökohta uuden tietosuoja-asetuksen säätämisessä on ollut riskipohjainen lähestyminen tietosuojaan. Tämä tarkoittaa sitä, että sääntelyn painavuus sidotaan riskien suuruuteen. Vähäriskisten toimien ylisääntelyä koetetaan välttää samalla, kun varmistetaan erityisen tarkasti rekisteröidyn tietosuojan toteutuminen silloin, kun toiminnassa on korkea riski tietojen väärinkäytöstä. Punninnassa otetaan huomioon esimerkiksi tietojen laatu ja se, miten arkaluonteisia tiedot ovat eli tietojen luonne, käsittelytarkoitus ja tietojen käsittelyn laajuus. Tällä on vaikutusta rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuuksiin. Toimien on vastattava käsittelyn kulloistakin tietosuojariskiä.[132]

Uudistuksen keskeisiä periaatteita on tilivelvollisuus eli rekisterinpitäjän ja käsittelijän velvollisuus kyetä todentamaan, että tietosuojasäädöksiä noudatetaan henkilötietojen käsittelyssä koko käsittelyprosessin ajan. Jos asetus tulee voimaan esitetyssä muodossa, yrityksille ei enää riitä, että ne noudattavat lainsäädännössä asetettuja velvoitteita, vaan tietosuojavelvoitteiden noudattaminen on kyettävä myös pyydettäessä todistamaan. Rekisterinpitäjiltä ja käsittelijöiltä tämä edellyttää tietojen

[130]Regulation (EU) No XXX/2016
of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[131] Sama.
[132] Sama.

yksityiskohtaista dokumentointia sekä tietosuojan toteuttamisen huolellista riskipohjaista suunnittelua ja ennakointia. Tähän liittyen uutena vaatimuksena ehdotuksessa vaaditaan, että rekisterinpitäjien ja käsittelijöiden on asetettava tietosuojavastaava, jos rekisteröityjen järjestelmällinen seuranta tai arkaluonteisten tietojen käsittely on niiden ydintoimintoja[133]. Lisäksi yritysten on tietyin edellytyksin toteutettava tietosuojaa koskeva vaikutusarviointi eli riskiarviointi. Erityisesti verkkotietopalveluyritysten kannalta merkittävä uudistus on toimittajaketjun hallintaan ja ketjussa tapahtuvaan tiedon siirtoon liittyvät velvoitteet, joiden noudattamattomuus on asetuksessa myös sanktioitu.

Rekisteröidyn kannalta uudistus vahvistaa erityisesti oikeutta tulla unohdetuksi eli mahdollisuutta saada halutessaan tietonsa pois rekisteristä. Samalla uudistuksessa korostetaan ikärajoin sitä, että lapsen antama suostumus on eri kuin aikuisen suostumus.[134] Jatkossa rekisteröity on oikeutettu saamaan kaikki itseään koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Rekisteröidyllä on myös ehdotuksen mukaan oikeus siirtää henkilötietonsa ja kaikki muutkin luovuttamansa tiedot toiseen järjestelmään halutessaan silloin, kun tietojen käsittely perustuu suostumukseen tai sopimukseen.[135]

Kansallisten tietosuojaviranomaisen toimivaltaa, tehtäviä ja valtuuksia säännellään ehdotuksessa tietosuoja-asetuksen tasolla. Kansalliset tietosuojaviranomaiset ovat toimivaltaisia, kun henkilötietojen käsittely tapahtuu jäsenvaltion rajojen sisäpuolella. Kun henkilötietojen käsittely ylittää jäsenvaltion rajat, toimivaltainen tietosuojaviranomainen määräytyy lähtökohtaisesti rekisterinpitäjän päätoimipaikan mukaan.[136]

---

[133] Section 4, Regulation (EU) No XXX/2016 of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[134] Regulation (EU) No XXX/2016 of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); Neuvonen, s.89-91; Ks. LIBE-raportti 2012/0011 (COD) (Albrecht).
[135] Article 18, Regulation (EU) No XXX/2016 of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
[136] Chapter VI, Regulation (EU) No XXX/2016

Kansallisten tietosuojaviranomaisten välisen yhteistyön toteuttamiseksi asetusehdotuksessa esitetään luotavaksi yhden luukun periaatteella toimiva ns. yhdenmukaisuusmekanismi. Keskeinen toimija tässä on perustettava Euroopan tietosuojaneuvosto (EDPB), joka voi tarvittaessa antaa sitovia päätöksiä tietosuoja-asetuksen soveltamisesta. Yhdenmukaisuusmekanismin avulla varmistetaan, että ratkaisukäytäntö ja tietosuoja-asetuksen soveltaminen on kaikissa jäsenmaissa yhdenmukaista.

Yhtenä uudistuksena asetusehdotuksessa esitetään ilmoitusvelvollisuutta kaikista vähäistä suuremmista tietosuojan loukkaustapauksista. Samalla rangaistuksia loukkauksista ehdotetaan tiukennettavaksi. Valvontaviranomaisilla on ehdotuksen mukaan valtuudet määrätä hallinnollisia seuraamuksia asetuksessa listatuista teoista. Kunkin tapauksen olosuhteet huomioiden valvontaviranomainen voisi määrätä sakkoja teon vakavuuden mukaan portaittain. Enimmillään sakko on ehdotuksen mukaan jopa 20 miljoonaa euroa tai vaihtoehtoisesti 4 % yrityksen maailmanlaajuisesta liikevaihdosta edeltävältä vuodelta, jos tämä on euromääräistä summaa suurempi.[137]

5.3 Kyberturvallisuus

Euroopan unionin tasolla tietoturva on tunnistettu jo pitkään yhdeksi sisämarkkinoiden kasvun keskeiseksi tekijäksi. Jo vuonna 2004 Euroopan yhteisö perusti asetuksella[138] Euroopan verkko- ja turvallisuusviraston (ENISA), jonka tehtävänä on sekä varmistaa verkko- ja tietoturvan toteutuminen että kehittää EU:n verkko- ja tietoturvakulttuuria. Marraskuusta 2009 voimassa ollut sähköisen viestinnän sääntelyjärjestelmä asettaa turvallisuusvelvoitteita sähköisten viestintäpalvelujen tarjoajille[139]. Vastaavasti tietosuojan osalta voimassa oleva sääntelykehys[140] velvoittaa rekisterinpitäjät

---

of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
Neuvonen, s.89-91, Ks. LIBE-raportti 2012/0011 (COD) (Albrecht).

[137] Article 79, Regulation (EU) No XXX/2016
of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation); Neuvoston mietintö 9565/15.

[138] EY No 460/2004, jota on myöhemmin uudistettu asetuksella EU No 526/2013.

[139] Puitedirektiivin 13 a ja 13 b.

[140] Direktiivi 2002/58/EY.

ottamaan käyttöön turvatoimenpiteet henkilötietojen suojaamiseksi. Toteutuessaan edeltävässä luvussa käsitelty komission ehdotus yleiseksi tietosuoja-asetukseksi velvoittaa rekisterinpitäjät raportoimaan henkilötietojen loukkauksista kansallisille viranomaisille.

Verkkorikollisuuden torjuntaa EU:ssa ohjaa Europolin osana oleva verkkorikostorjuntakeskus. Lisäksi EU:n toimielimillä, virastoilla ja muilla elimillä on yhteinen tietotekniikan kriisiryhmä CERT-EU.

Tällä hetkellä tietoturvaa EU:ssa säännellään direktiivillä tietojärjestelmiin kohdistuvista hyökkäyksistä[141], jonka tavoitteena on tietyntyyppisten tekojen kriminalisoinnin yhdenmukaistaminen unionissa sekä parantaa viranomaisten välistä yhteistyötä ja tekojen tilastointia. Osaltaan direktiivi varmistaa sen, että tietojärjestelmiin kohdistuvista rikoksista on säädetty riittävät rangaistukset koko EU-alueella. Direktiivi on pantu täytäntöön Suomessa kansallisesti säädöksillä 368-372/2015.

Tietojärjestelmiin kohdistuvia hyökkäyksiä koskevassa direktiivissä ei kuitenkaan käsitellä verkko- ja tietoturvariskien ennaltaehkäisyä, verkko- ja tietoturvapoikkeamiin reagoimista eikä niiden vaikutusten minimoimista. Näitä tavoitteita varten komissio on antanut ehdotuksen direktiiviksi toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa[142] eli niin kutsutun NIS-direktiivin.

Tällä hetkellä NIS-direktiivin käsittely on siinä vaiheessa, että neuvosto ja Euroopan parlamentti ovat päässeet yhteisymmärrykseen ehdotetun NIS-direktiivin pääperiaatteista neljännessä kolmikantakokouksessaan 29. kesäkuuta 2015. Neuvotteluja direktiivin lopullisesta sisällöstä jatkettiin syksyllä 2015 ja direktiiviehdotus odottaa lopullista hyväksyntää.[143]

Direktiiviehdotuksen tavoitteena on varmistaa verkko- ja tietoturvan korkea taso koko EU-alueella. Tarkoituksena on toimintaedellytysten yhdenmukaistaminen yhtenäisten sääntöjen avulla. Käytännössä direktiivillä pyritään parantamaan sekä Internetin että

[141] Direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksiä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta.
[142] KOM 2013(48).
[143] http://www.consilium.europa.eu/fi/policies/cyber-security/

yksityisten verkkojen ja tietoturvan parantamiseen. Ehdotettuja keinoja tämän tavoitteen saavuttamiseksi on ensinnäkin jäsenvaltioiden velvoittaminen sekä nostamaan varautumistasoaan että parantamaan keskinäistä yhteistyötään. Kaikkien jäsenvaltioiden tulee ehdotuksen mukaan perustaa ryhmiä tietotekniikkakriisejä varten (CERT), hyväksyttävä kansallinen verkko- ja tietoturvastrategia ja yhteistyösuunnitelmat sekä nimetä kansallinen, toimivaltainen verkko- ja tietoturvasta vastaava viranomainen. Tällaisella viranomaisella tulee direktiiviehdotuksen mukaan olla riittävät resurssit estää ja käsitellä tietoturvariskejä ja poikkeamia sekä tarvittaessa myös vastata niihin.[144]

Toiseksi direktiiviehdotuksessa edellytetään kansallisten toimivaltaisten viranomaisten yhteistyötä. Tällaisen verkoston tarkoituksena on varmistaa koordinoitu tiedonvaihto, varhaisvaroitusten jakaminen sekä verkko- ja tietoturvauhkien sekä poikkeamien havaitseminen ja torjuminen EU-tasolla Euroopan verkko- ja tietoturvan yhteistyösuunnitelman mukaisesti.[145]

Kolmanneksi direktiiviehdotuksessa edellytetään, että yhteiskunnalle elintärkeitä rakenteita tarjoavat operaattorit ja keskeisten tietoyhteiskuntapalvelujen tarjoajat sekä julkishallinnot toimivat osaltaan turvariskien hallitsemiseksi ja myös raportoivat kaikista vakavista turvapoikkeamista toimivaltaisille kansallisille viranomaisille. Tällä pyritään varmistamaan sähköisen viestinnän puitedirektiivin mallin mukainen riskinhallintakulttuurin kehittyminen ja tiedonjako yksityisten ja julkisten toimijoiden välillä.[146]

Verkko- ja tietojärjestelmien vaarantavista poikkeamista, jotka vaikuttavat merkittävästi palveluiden jatkuvuuteen ja turvallisuuteen tulee ehdotuksen mukaan ilmoittaa kaikilla kriittisillä sektoreilla muun muassa rahoituspalveluiden, liikenteen ja energian alalla. Lisäksi tietotekniikkapalveluja tarjoavien yritysten kuten sovelluskauppojen, sähköisen kaupankäynnin alustojen, pilvipalvelualustojen, hakukoneiden ja verkkoyhteisöpalvelujen tulee ilmoittaa tällaisista poikkeamista. Vastaava velvollisuus on julkishallinnoilla.[147]

[144] KOM (2013) 48, http://www.consilium.europa.eu/fi/policies/cyber-security/.
[145] KOM (2013) 48.
[146] Sama.
[147] KOM (2013) 48, http://www.consilium.europa.eu/fi/policies/cyber-security/.

5.4 Uudistusten vaikutusten arviointi

On erittäin suuri vaara, että verkkotiedustelu loukkaa yksityisyyttä ja tiettyjä muita ihmisoikeuksia. Euroopan ihmisoikeussopimuksen ja EU:n perusoikeuskirjan turvaamaan tietosuojaan ja yksityisyydensuojaan kajotaan erityisesti verkkotiedustelulla, jossa kerätään talteen koko liikenne, seulotaan kohdehenkilöt tai suoritetaan tietokoneen kohdennettua tarkkailua. Tällaisissa tarkkailumenetelmissä perusoikeuksiin puututaan käytännössä sellaisessa laajuudessa, joka on vastoin kansainvälisiä sopimuksia.[148]

Toisaalta ongelmat yksityisyydensuojan kannalta eivät ole ainoita haittoja, joita strateginen valvonta mahdollisesti voi tuoda mukanaan. Sääntelemätön ja kontrolloimaton valvonta saattaa aiheuttaa yhteiskunnalle monia tarkasti yksilöimättömiä, hajanaisia, pitkän aikavälin haittoja. Ongelmallista on esimerkiksi, jos yrityksille asetetaan samanaikaisesti ristiriitaisia velvoitteita kuten velvoite luovuttaa ja suojata tietoa.[149]

Verkkotiedustelusta voidaan säätää joko niin, että se koskee suurta joukkoa tai niin, että tiedustelun kohdistuminen on rajoitettu tiukasti. Näistä ensimmäinen vaihtoehto todennäköisesti rikkoo yksityisyydensuojaa ja muita ihmisoikeuksia enemmän kuin jälkimmäinen vaihtoehto. [150] Kohdentamatonta tiedonkeräystä viestinnästä kutsutaan myös massavalvonnaksi. Tällaista käsitettä käytetään erityisesti toiminnasta, joka on salaista ja eikä viestinnän valvonta perustu erilliseen lainsäädäntöön ja lainsäädäntö muutoin on tulkinnaltaan epäselvää, jolloin yksityisyydensuojan rikkominen on hyvin todennäköistä.[151]

Jotta verkkotiedustelusääntely täyttää Euroopan ihmisoikeussopimuksen määräykset, on tiedustelusta säädettävä yksiselitteisesti lailla. Tämä ei kuitenkaan välttämättä vielä poista julkista huolta yksityisyydensuojan rikkomisesta, vaan lisäksi tarvitaan vahvoja valvontamekanismeja ihmisoikeuksien toteutumisen valvomiseksi.

[148] Scheinin, 2014, s.35.
[149] CDL-AD(2015)006-e, s.39.
[150] Sama.
[151] Nikkanen 2014, s. 139-140.

Yritysten toiminnan suunnittelun kannalta on tärkeää, että lainsäädäntö on sekä selkeää että ennakoitavissa. Epävarmuus lainsäädännön tulkinnasta ja muuttumisesta muodostaa esteen yritysten investointipäätösten tekemiselle. Tässä mielessä täsmällinen tiedustelulainsäädäntö voi olla jopa kansallinen kilpailuetu. Toisaalta on selvää, että liika puuttuminen tietosuojaan tulee todennäköisesti heikentämään Suomen houkuttelevuutta verkkotietopalveluyritysten sijaintimaana. Tällaista sääntelyä on esimerkiksi yritysten velvoittaminen rakentamaan takaportteja tai luovuttamaan salausavaimia asiakkailleen tarjottaviin ohjelmistoihin tai laitteistoihin. Ainakaan toistaiseksi viranomaisen oikeutta takaportteihin tai salausavaimiin ei ole julkisesti ehdotettu tietoliikennetiedustelulainsäädäntöä valmisteltaessa.[152]

Tämä osaltaan varmasti vähentää myös verkkotietopalveluyritysten huolta tulevasta tiedustelulainsäädännöstä. Tuotteiden ja palveluiden tietoturvan heikentäminen viranomaisten vaatimuksesta heikentää asiakkaiden luottamusta niitä tarjoaviin yrityksiin. Takaportit ja salausavaimet kun ovat keinoja kiertää esimerkiksi puhelimen tai sähköpostin salaukset ja suojaukset. Tällainen velvoite mahdollistaa käytännössä viranomaisen pääsyn kenen tahansa puhelimeen tai muuhun tietotekniseen laitteeseen tai esimerkiksi sähköpostissa tai muussa sovelluksessa tai pilvipalvelussa säilytettävään tietoon. Elinkeinoelämän selkeä tavoite on Suomen profiloituminen ennen kaikkea tietoturvallisten tuotteiden ja palveluiden toteuttajana kuin viranomaisvalvonnan mallimaana.

Käytännössä tietoliikennetiedustelun toteuttaminen edellyttää Ruotsin mallin mukaisesti, että tietoliikennepalvelua tarjoavat yritykset kuten teleyritykset tai tietoliikennekaapeleita omistavat yritykset velvoitetaan avaamaan liityntäpisteet tietoliikennetiedusteluviranomaisille. Tietoliikenteen jatkuvasti kasvavat määrät ja tiedon salaaminen eri tekniikoin vähentävät tällaisen tiedustelutoteutuksen tehokkuutta.[153]

[152] Suomalaisen tiedustelulainsäädännön suuntaviivoja, s.72.
[153] Suomalaisen tiedustelulainsäädännön suuntaviivoja s.72.

Salaustekniikoiden kehittyminen johtaa siihen, että salatun viestin avaaminen ei enää onnistu ilman salausavainta. Tulevaisuudessa reaaliaikaisen tiedon saaminen tietoliikennetiedustelun avulla voi olla vaikeaa tai jopa mahdotonta.[154] Oletettava johtopäätös tästä on, että esitetty tiedustelun toteutustapa ei tule välttämättä tulevaisuudessa riittämään, vaan todennäköistä on, että vahvempia tiedustelutapoja tullaan vaatimaan.

Toisaalta salaus ei estä esimerkiksi tunnistamistietojen keräämistä, mikä saattaa olla kansallisen turvallisuuden kannalta myös tärkeää tietoa, vaikka varsinainen viesti jäisikin avaamatta. Vastaavasti salauksesta huolimatta pystytään havaitsemaan tietoverkkohyökkäyksiä ja vastaavia uhkia.[155]

Uudesta tiedustelulainsäädännöstä ehkä poiketen EU:n tietosuoja-asetuksella saattaa olla verkkotietopalveluyritysten toimintaan myös selkeästi positiivisia vaikutuksia. Keskeisin yritysten kannalta myönteinen seuraus tietosuoja-asetuksesta on lainsäädännön yhtenäistyminen. Tietosuoja-asetuksen myötä poistuvat tilanteet, joissa tiedon käsittelyyn joudutaan soveltamaan useita toisistaan poikkeavia säännöksiä samanaikaisesti. Tämä poistaa tulkinnallisten epäselvyyksien lisäksi myös yritysten hallinnollisia kuluja, kun soveltamisepäselvyydet ja moninkertaiset valtiokohtaiset tiedonsuojaamis- ja koulutuskulut poistuvat.

Voimassa oleva henkilötietodirektiivi on vuodelta 1995, jolloin tietojärjestelmissä liikuteltavat ja käsiteltävät tietomäärät ja teknologiaympäristö olivat hyvin toisenlaisia kuin nykyään. Direktiivi on implementoitu kansallisesti jokaisessa jäsenvaltiossa erikseen, minkä vuoksi rekisterinpitäjiin ja henkilötietojen käsittelyyn liittyvät käytännön toimintatavat saattavat vaihdella huomattavastikin valtioittain. Yksi esimerkki tällaisesta vaihtelusta ovat tilanteet, joissa rekisterinpitäjä on ilmoitusvelvollinen paikalliselle tietosuojaviranomaiselle, missä on suuria eroja eri jäsenmaiden lainsäädäntöjen välillä. Erityisesti monikansallisille yrityksille toisistaan poikkeavien

[154] Sama.
[155] Sama.

henkilötietojen käsittelyä koskevien säännösten noudattaminen on monimutkaista ja aiheuttaa turhia kustannuksia.[156]

Uusi tietosuoja-asetus tulee osittain poistamaan tämän kaltaisia lainsäädännön eroavaisuuksista johtuvia ongelmia, sillä toteutuessaan se on suoraan jäsenvaltioissa soveltuvaa oikeutta. Henkilötietojen käsittelyä koskevien vaatimusten ja rikkomuksista määrättävien sanktioiden yhdenmukaistuminen EU-alueella tulee todennäköisesti lisäämään kansalaisten luottamusta henkilötietoja käsitteleviin yrityksiin ja muihin toimijoihin. Sen lisäksi, että uudistuksella vahvistetaan kuluttajien luottamusta verkkoympäristöön, sen on esitetty myös vähentävän yritysten hallintokustannuksia. Parhaimmillaan tietosuoja-asetus voi tuoda talouskasvua, työllisyyttä ja innovaatioita. Tietosuojaa ja yksityiselämää turvaavien tavoitteiden lisäksi uudistuksella tavoitellaan myös elinkeinoelämää hyödyttäviä päämääriä.[157]

Vastaavasti kuin tietosuoja-asetuksella NIS-direktiivillä on verkkotietopalveluita tarjoaville yrityksille positiivisia vaikutuksia sen vuoksi, että direktiivi tulee yhdenmukaistamaan tietoturvasääntelyä valtioiden välillä. Lisäksi NIS-direktiivi toteutuessaan ennaltaehkäisee verkko- ja tietoturvariskejä sekä parantaa verkko- ja tietoturvapoikkeamiin reagoimista ja niiden vaikutusten minimoimista, mikä tulee lisäämään yritysten toimintaympäristön tietoturvallisuutta, vähentämään tietoturvauhista aiheutuvia kustannuksia ja parantamaan asiakkaiden luottamusta palveluita kohtaan.

Yritysten näkökulmasta uudet EU-tasoiset lainsäädöshankkeet ovat pääasiassa positiivinen asia lainsäädännön ja sovellettavien säännösten selkeytyessä. Sen sijaan Suomen asemaan tiedon turvasatamana tietosuoja- ja tietoturvalainsäädännön yhdenmukaistumisella saattaa olla myös negatiivisia seurauksia. Eräässä mielessä Suomi menettää mahdollisen kilpailuvalttinsa suhteessa muihin EU-jäsenmaihin, kun se ei pysty enää samalla tavalla muokkaamaan tietosuoja- ja tietoturvalainsäädäntöään verkkotietopalveluyritysten kannalta houkuttelevammaksi suhteessa vaikkapa naapurivaltioihin. EU-tasoisten lainsäädäntöhankkeiden toteutuessa Suomen ainoaksi selväksi lainsäädännölliseksi poikkeukseksi muodostuu viranomaisten toimivaltuuksien laajuus tiedonhankintaan eli viranomaisten oikeudet

[156] Pitkänen, Tiilikka, Warma 2013, s.26.
[157] Euroopan komission lehdistötiedote 25.1.2012, Pitkänen, Tiilikka, Warma 2013, s.26 ja 29.

harjoittaa verkkotiedustelua tai näiden oikeuksien puute. Tässä mielessä kansallisella verkkotiedustelulakivalmistelulla tulee olemaan keskeinen merkitys verkkotietopalveluyritysten sijaintipäätöksille.

6 Johtopäätöksiä

Nykyisellään Suomessa voimassa oleva tietosuoja- ja tietoturvalainsäädäntö on verkkotietopalveluyritysten toiminnan kannalta suhteellisen hyvällä tasolla ja mahdollistaa yrityksille liiketoiminnan turvallisen harjoittamisen. Suurelta osalta tietosuojan ja tietoturvan toteutuminen on kuitenkin kiinni yritysten omista tavoitteista ja toimista, ja lainsäädäntö antaa usein käytännössä vain puitteet toiminnalle. Jotta tietosuoja ja tietoturva toteutuvat elinkeinoelämässä tehokkaalla tavalla, on yrityksillä oltava taloudellinen kannustin niiden varmistamiseen. Lainsäädännöllä voidaan vaikuttaa sekä tämän kannustimen luomiseen että toimintaympäristön yleiseen turvallisuuteen, jolla osaltaan varmistetaan myös asiakkaiden luottamus verkkotietopalveluihin yleisesti.

Verkkotietopalveluyritysten toiminnan luonteeseen kuuluu valtioiden rajojen ylittyminen. Tieto kulkee nopeasti valtiosta toiseen mannertenvälisiä kaapeleita pitkin ja esimerkiksi pilvipalveluissa tiedon fyysisen sijainnin merkitys hämärtyy. Tiedonsiirto- ja tiedonkäsittelytekniikan jatkuvasti kehittyessä on tärkeää, että lainsäädäntö ei ole tiukan valtiokohtaista, vaan tietosuoja- ja tietoturvakysymyksiä ajatellaan laajasti.

Tällä hetkellä EU-tasolla valmistelussa olevat lainsäädäntöhankkeet koskien tietosuoja-asetusta ja NIS-direktiiviä tukevat EU-alueen yhteistä tietosuoja- ja tietoturvapolitiikkaa. Toteutuessaan uudistukset harmonisoivat alueen lainsäädäntöä hyvin voimakkaasti, mikä voi parhaimmillaan nostaa EU-valtioiden kilpailukykyä digitaalisilla markkinoilla. Yhtenäinen tietosuoja- ja tietoturvalainsäädäntö helpottaa yritysten rajat ylittävää liiketoimintaa ja madaltaa kynnystä sijoittautua EU-alueelle.

Tietosuoja-asetusehdotukseen sisältyvät velvoitteet kyetä todentamaan tietosuojan toteutuminen koko käsittelyprosessin ajan sekä rikkomuksiin liittyvät voimakkaat sanktiot vaikuttavat verkkotietopalveluyritysten sijoittautumiseen ja toimintaan sekä negatiivisesti että positiivisesti. Toisaalta tietosuoja EU-alueella tulee varmasti parantumaan käsittelyn läpinäkyvyyden ja voimakkaiden sanktioiden myötä, mikä lisää

asiakkaiden luottamusta siihen, että heidän tietonsa ovat turvassa ja niitä käsitellään asianmukaisesti laissa edellytetyllä tavalla.

Asiakkaiden luottamus todennäköisesti lisää halukkuutta ostaa palveluja, jolloin yritysten liikevaihto kasvaa. Tästä huolimatta kasvavat hallinnolliset kustannukset ja sanktiot saattavat vaikuttaa myös negatiivisesti yritysten sijoittautumispäätöksiin tai saattavat vaikuttaa siihen, millaisia palveluita voidaan tarjota. Näin on esimerkiksi kustannusten ja sanktioiden ollessa toiminnasta saatavaan rahalliseen hyötyyn tai liikevaihdon mahdolliseen kasvuun nähden suhteettoman suuria. Tietosuoja-asetukseen kaavaillut sakot tietosuojarikkomuksesta rekisterinpitäjälle tai tietoja käsittelevälle yritykselle ovat suuruudeltaan sitä luokkaa, että niillä voi olla verkkotietopalveluyritysten sijoittautumiseen myös negatiivinen vaikutus.

Nykyisellään kansallinen lainsäädäntö antaa viranomaisille mahdollisuuksia reagoida tietoturvauhkiin ja -hyökkäyksiin, jotka on kriminalisoitu rikoslaissa. Lisäksi viranomaisilla on jo nyt oikeus kohdistaa viestintään esimerkiksi televalvontaa. Uuden EU-tasoisen, osin myös suoraan kansallisesti sovellettavissa olevan lainsäädännön myötä on tärkeä huolehtia siitä, ettei kansalliseen lainsäädäntöön jää päällekkäisiä tai ristiriitaisia sanktiomekanismeja. Vastaavasti uuden kansallisen tiedustelulainsäädännön valmistelussa on huomioitava, että samaan toimintaan ei kohdistu useita yhtäaikaisia valvontakeinoja, jolloin myös perusoikeuksien toteutumisen valvominen käy vaikeaksi.

Suomella on maine hyvän tietoturvan maana, jossa toimitaan rehellisesti. Verkkohyökkäyksiin varautuminen on kuitenkin yrityskohtaista ja yleinen tietoturvan taso esimerkiksi verkkotietopalveluiden kohdalla on kiinni siitä, miten alan yksittäiset toimijat suojaavat järjestelmänsä. Tiukkoja tietoturvavelvoitteita muun tiedon kuin viranomaistiedon käsittelylle laissa on vähän. Myös uhkien ja rikkomusten raportoinnissa ja tilastoinnissa on kehitettävää. Nykytilanteessa vaarana on, että rikkomukset eivät tule ilmi, jolloin niiden ehkäiseminen myös jatkossa on vaikeaa.

Tällä hetkellä EU-lainsäädännössä voimassa oleva tietojärjestelmiin kohdistuvia hyökkäyksiä koskeva direktiivi[158], joka on edesauttanut jäsenmaiden viranomaisten

[158] Direktiivi 2013/40/EU tietojärjestelmiin kohdistuvista hyökkäyksiä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta.

välisen yhteistyön kehittymistä kyberturvallisuuden alalla ja alaan liittyvien rikosten EU:n laajuista tilastointia. Direktiivin kansallisella implementoinnilla kyberturvallisuuteen kohdistuvista rikoksista on säädetty yhtenäiset rangaistukset koko EU-alueella.

Verkko- ja tietoturvariskien ennaltaehkäisy, verkko- ja tietoturvapoikkeamiin reagoiminen ja vaikutusten minimoiminen eivät kuulu tietojärjestelmiin kohdistuvia hyökkäyksiä koskevan direktiivin tavoitteisiin. Näiden tavoitteiden saavuttaminen edellyttää pitkään vireillä olleen eli NIS-direktiivin[159] voimaantuloa. Toteutuessaan NIS-direktiivi nostaa tietoturvan tasoa koko EU-alueella, mikä auttaa myös verkkotietopalveluyritysten toimintaa. Direktiiviehdotus kohdistuu kuitenkin alueelle, joka on perinteisesti katsottu olevan jokaisen valtion oman kansallisen sääntelyn piirissä eli kansallisen turvallisuuden varmistamiseen, mistä syystä direktiivin lopullisen sisällön saavuttaminen vie todennäköisesti vielä aikaa.

Ehkä oleellisin verkkotietopalveluyritysten sijoittumiseen ja toimintaan vaikuttava lainsäädäntöuudistus kansallisesti ajatellen on vireillä oleva tiedustelulainsäädännön luominen Suomeen. Tämän hankkeen vaikutuksia voi vain arvailla, kun tulevan lainsäädännön sisältö on vielä avoin. Tiukasti perusoikeuksiin puuttuva tiedustelulainsäädäntö voi pahimmillaan lamauttaa koko verkkotietopalveluyritysten toiminnan ja voimakkaasti jarruttaa alalla toimivien yritysten sijoittumisen Suomeen. Toisaalta harkiten elinkeinoelämän kanssa säädetyn lain vaikutukset verkkotietopalveluyritysten toimintaan voivat jäädä hyvinkin vähäisiksi tai jopa olemattomiksi. Näin on ainakin, jos päätetään, että perustuslakiin eikä perusoikeuksiin puututa tai että mahdollinen puuttuminen on hyvin rajattua ja tarkoin valvottua.

Yksityisyyden ja turvallisuuden välillä on saavutettavissa tasapaino vain, jos tiedustelulainsäädännön valmistelussa turvataan yksityisyydensuojan toteutuminen. Tämä edellyttää, että lainsäädäntö noudattaa kansainvälisiä ihmisoikeussopimuksia yksityisyyden ja viestinnän suojan noudattamisesta viestinnän valvonnassa. Lainsäädännön on määriteltävä selkeät ja läpinäkyvät säännökset siitä, mikä on oikeasuhtaista ja tarpeellista viestinnän valvontaa. Summittainen ja laaja-alainen massavalvonta ei tue sananvapauden ja viestinnän salaisuuden periaatteiden toteutumista. Tiedustelun harjoittamisen tulee olla luvanvaraista ja sitä tulee valvoa

[159] KOM 2013(48).

tuomioistuimen tai muun riippumattoman tahon toimesta. Tällä varmistetaan tiedustelun läpinäkyvyys ja vastuullinen harjoittaminen.

Erityisesti verkkotietopalveluja tarjoavien yritysten toiminnan ja sijoittautumisen kannalta on tärkeää, että valtiolla ei ole suoraa pääsyä yritysten järjestelmiin tai tietoverkkoihin. Verkkotietopalveluyrityksillä tulee säilyä tekninen ja operatiivinen kontrolli omista järjestelmistään.

Valtion on myös oltava avoin tiedustelutoimien käytöstä ja kohdistumisesta, jotta kansalaisten, yritysten ja sijoittajien luottamus tiedustelun oikeasuhtaisuuteen ja siten tietosuojan riittävään toteutumiseen säilyy. Salassa harjoitettu tiedustelu, josta ei raportoida näyttää herkästi epätoivottavalta urkinnalta tai massavalvonnalta, joka ei kunnioita valtioiden välisiä suhteita saati ihmisoikeuksia.

Suomella on hyvät mahdollisuudet tulla tiedon turvasatamaksi, mitä edesauttavat Suomen sijainti, teknologian osaaminen, sotilaallinen liittoutumattomuus ja hyvät runkoverkkoyhteydet muille mantereille. Suomen toimista keskeisenä tiedonsiirron solmukohtana voidaan lisäksi tukea lainsäädännöllisin keinoin monella tavalla. Yritysten kannalta tietosuojaan ja tietoturvaan kohdistuvassa sääntelyssä on tärkeää kustannustehokkuus, sääntelyn ennakoitavuus ja asiakkaiden luottamuksen turvaaminen, mikä mahdollistaa verkkotietopalveluyrityksen toiminnan Suomessa.

7 Kokoavia näkökohtia

Suomen kilpailukyvyn parantaminen ja kansainvälisten investoijien ja yritysten houkutteleminen Suomeen on mahdollista vain, jos Suomen maine tietoturvallisena valtiona kyetään säilyttämään. Tähän tavoitteeseen pääseminen edellyttää, että politiikka on yhtenäistä ja johdonmukaista. Suomesta voi tulla tiedon turvasatama eli valtio, johon verkkotietopalveluyritykset ensisijaisesti haluavat sijoittautua, vain jos tavoite huomioidaan kaikessa poliittisessa päätöksenteossa ja erityisesti lainsäädäntötyössä. Huonosti valmisteltuna ja toteutettuna jo yksi yksittäinen laki, saattaa romuttaa koko käsitteen. Tämä johdonmukaisuus lainsäädännössä tulee säilyä erityisesti, kun uutta EU-lainsäädäntöä säädetään.

Jos tavoitteena on tehdä Suomesta tiedon turvasatama, on poliitikkojen haasteena muistaa tavoite jokaisessa lainsäädäntöhankkeessa ja varmistaa tavoitteen toteutuminen jokaisen yksittäisen lain kohdalla. Tämä ei kuitenkaan yksin riitä, vaan edellyttää lainsäädäntöhankkeiden vaikuttavuuksien jatkuvaa tutkimista ja analysoimista. Poliitikkojen lisäksi myös tutkijat saavat siis haasteen seurata lainsäädännön kehittymistä ja osallistua myös aktiivisesti lainsäädäntöhankkeiden kommentointiin.

Digitaalisen kasvuympäristön kehittäminen on hallituksen selkeä tavoite, johon halutaan aktiivisesti panostaa tällä hallituskaudella. Digitalisaatio on myös nostettu yhdeksi hallituksen viidestä kärkihankkeesta, jonka tutkimukseen ja kehittämiseen tullaan hallituskaudella kohdentamaan valtion rahoitusta. Yksi digitalisaation edellytyksistä on tietoturvallisen Suomen kehittäminen eli ajatus tiedon turvasatamasta. Tämän tavoitteen toteutuminen edellyttää jatkuvaa tämän tutkimuksen kaltaista analyysia, sillä lainsäädäntö elää koko ajan ja tilanteet muuttuvat erityisesti teknologian kehityksen myötä.

Lopulta voidaan ajatella, että verkkotietopalveluyritysten sijoittautumisen määräävät puhtaasti kaupalliset edellytykset. Tekniikan voidaan olettaa olevan kaikkialla samanlaista. Käytännössä lainsäädännöllä on luotava riittävän tehokkaat taloudelliset kannustimet yrityksille sijoittautua Suomeen ja samalla pitää huoli siitä, ettei tietosuojaa ja tietoturvaa vahvistettaessa säädetä sanktioita ja velvoitteita, jotka muuttavat taloudellisen toiminnan kannattamattomaksi.

Erityisesti verkkotietopalveluyritysten toiminnan kannalta on merkittävää, millaisia tietosuojaan puuttuvia lakeja säädetään. Suomeen on turha investoida tai edes säilyttää olemassa olevaa toimintaa, jos lainsäädännöllä viedään kuluttajien luottamus palvelun tietosuojaan. Kaikkein suurin merkitys on tällöin sellaisilla lainsäädäntöhankkeilla, jotka edellyttävät puuttumista perustuslaissa säädettyihin kansalaisten perusoikeuksiin kuten oikeuteen luottamuksellisen viestin suojaan. Käytännössä lainsäädännössä on löydettävä tasapaino tietosuojan ja turvallisuuden välillä. Kysymykseen, voiko Suomesta tulla tiedon turvasatama vaikuttaa moni yksittäinen laki nyt ja tulevaisuudessa ja suuri vaikutus tulee olemaan sillä, mitä säädetään EU-tasolla ja mitkä poliittiset tavoitteet ohjaavat päättäjiä. Runollisesti voi todeta, että tiedon turvasatama on karikkoisen reitin päässä.

Lähdeluettelo

Virallisaineisto

Article 29 Working Party: Opinion 8/2010 on applicable law, Adopted 16.12.2010.

Article 29 Working Party: Opinion 05/2012 on Cloud Computing, Adopted 1.6.2012.

CDL-AD(2015)006-e. Update of the 2007 Report on the Democratic Oversight of the Security Services and Report on Democratic Oversight of Signals Intelligence Agencies adopted by the Venice Commission at its 102nd Plenary Session (Venice, 20-21 March 2015).

COM(2015) 566 final, COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14, (Schrems), Brussels, 6.11.2015.

Eduskunta, Verkkotiedustelu, https://www.eduskunta.fi/FI/tietoaeduskunnasta/kirjasto/aineistot/kotimainen_oikeus/LATI/Sivut/Verkkotiedustelu.aspx

European Commission: Comparative study on different approaches to new privacy challenges, in particular in the light of technological developments, Final Report 2010.

European Commission, Restoring trust in transatlantic data flows through strong safeguards: European Commission presents EU-U.S. Privacy Shield, Brussels, 29 February 2016

Euroopan komissio, Tietosuojasääntöjen kattava uudistus parantaisi käyttäjien mahdollisuuksia valvoa tietojaan ja vähentäisi yritysten kustannuksia, Brysseli 25.1.2012.

Kaho, Julå, Kara ja Iike, 2014, Dataintensiivisen teollisuuden sijoittautumisen edellytykset, Liikenne- ja viestintäministeriö.

KOM(2012) 529 lopullinen, Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle, Pilvipalveluiden potentiaali käyttöön Euroopassa,

KOM 2013(48), Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON DIREKTIIVI toimenpiteistä yhteisen korkeatasoisen verkko- ja tietoturvan varmistamiseksi koko unionissa.

Kysymys KK 558/200 hallitukselle.

Neuvosto 9565/15.

Nordic Council of Ministers: Nordic Public Sector Cloud Computing - a discussion paper, 2012, http://www.norden.org/fi/julkaisut/julkaisut/2011-566.

Perustuslakivaliokunnan lausunto PeVL 18/2014 vp - HE 221/2013 vp.

Ratkaisujen suomi, pääministeri Juha Sipilän strateginen ohjelma 2015.

Regeringens proposition 1999/2000:25.

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

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

Siviili- ja sotilastiedustelua koskevan lainsäädännön valmistelu käyntiin, Sisäministeriön mediatiedote 21.8.2015.

Suomalaisen tiedustelulainsäädännön suuntaviivoja, 2015, Tiedonhankintalakityöryhmän mietintö, Puolustusministeriö.

Statement of the Article 29 Working Party, Brussels, 16 October 2015

Tiedonhankintalakityöryhmä luovutti mietintönsä puolustusministeri Carl Haglundille, Puolustusministeriön tiedote 14.01.2015.

Parempaa kyberturvallisuutta kaikkialla Euroopassa, http://www.consilium.europa.eu/fi/policies/cyber-security/.

Kirjallisuus ja muu tutkimusaineisto

Grabosky, Peter, 2009, The Internet, Technology and Organised Crime. Teoksessa Plywaczewski, Emil W. (toim.) Current Problems of the Penal Law and Cri-Minology, s. 155 - 179. Faculty of law, University of Bialystok. Poland.

Hon, w Kuan, Hörnle, Julia, Millard, Christopher, 2013, Which Law(s) Apply to Personal Data in Clouds? Teoksessa Cloud Computing Law (toim. Millard, Christopher), s.231-244, Oxford University Press

International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/

Järvinen, Petteri, 2014, NSA Näin meitä seurataan.

Kyberturvallisuus ja tietoverkkorikokset, https://www.intermin.fi/fi/turvallisuus/rikostorjunta/kyberturvallisuus.

Leppänen, Anna, Virta, Sirpa, 2014, Kohti systeemiälykästä kyberturvallisuuden hallintaa - kyberrikollisuus ja sen torjunta, s.5-13, Futura 2/2014.

Manner, Jukka, Tiilikainen, Seppo, 2014 Suomen automaatioverkkojen haavoittuvuus s. 23-31, Futura 2/2014.

Neuvonen, Riku, Yksityisyyden suoja Suomessa, 2014, Lakimiesliiton Kustannus.

Nikkanen, Hanna, 2014, Massavalvonta ja puolivarjoisat tilat, s.135-155, Verkko suljettu, Internet ja avoimuuden rajat, Mikael Brunila ja Kimmo Kallio (toim.), Into Kustannus.

Oksanen, Ville, 2014, Suomi ja verkkovalvonta, s.14-22, Futura 2/2014.

Pitkänen, Olli, Tiilikka, Päivi, Warma, Eija, 2013, Henkilötietojen suoja.

Scheinin, Martin, 2015, Massavalvonnan kyseenalaiset hyödyt, s.35, Tietosuoja-lehti, 2/2015.

Unionin tuomioistuin totesi teletunnistamistietojen säilyttämisestä annetun direktiivin pätemättömäksi, Castren & Snellman julkaisu 23.4.2014.

Viljanen, Vesa, 2013, Yksityisyydensuojan parantaminen tietoverkoissa.

Voutilainen, Tomi, Galkin, Denis, 2013, Tietosuoja pilvipalveluiden hankintasopimuksissa julkisessa hallinnossa, Defensor Legis 2013/3.

Yksityisyydensuoja, lainsäädäntö, www.yksityisyydensuoja.fi/lainsäädäntö.