EU:N YLEINEN TIETOSUOJA-ASETUS: TIETOTURVALLISUUDESTA HENKILÖTIETOJEN KÄSITTELYSSÄ

Tanja Kalliojärvi
Maisteritutkielma
Oikeusinformatiikka
Oikeustieteiden tiedekunta
Lapin yliopisto
2016

Lapin yliopisto, oikeustieteiden tiedekunta
Työn nimi: EU:n yleinen tietosuoja-asetus: tietoturvallisuudesta henkilötietojen käsittelyssä
Tekijä: Tanja Kalliojärvi
Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka
Työn laji: Tutkielma_X_Laudaturtyö__ Lisensiaatintyö__
Sivumäärä: XVII + 82 + 3 liitettä
Vuosi: Kevät 2016

Tiivistelmä:

Euroopan komissio antoi tammikuussa 2012 ehdotuksen tietosuojasääntelyn uudistamisesta EU:ssa. Tutkielma käsittelee erityisesti komission tietosuoja-asetusehdotuksen 30–32 §:ä, jotka säätelevät rekisterinpitäjälle ja henkilötietojen käsittelijälle asetettuja tietoturvallisuusvelvoitteista. Lobbausaktiviteetit ja yli 4000 muutosehdotusta tietosuoja-asetusehdotukseen osoittavat, että useat organisaatiot pitävät muutosta tietosuojalainsäädännössä merkittävänä. Tutkielmassa tarkastellaan, minkälaista diskurssia tietosuoja-asetusehdotuksesta on käyty asetuksen valmisteluvaiheessa.

Voimassa oleva henkilötietodirektiivi ei aseta rekisterinpitäjille velvollisuutta ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista. Uudistuksen kautta tähän on tulossa muutos, sillä rekisterinpitäjille asetetaan tietosuoja-asetuksessa velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaisille ja asianomaisille yksilöille. Komission ehdotuksessa edellytettiin, että rekisterinpitäjä tekee kaikissa tietoturvaloukkaustapauksissa ilmoituksen valvontaviranomaiselle 24 tunnin kuluessa sen ilmitulosta. Useat rekisterinpitäjät totesivat kannanotoissaan, että näin lyhyt määräaika aiheuttaisi todennäköisesti haittaa tietoturvaloukkausten korjaamiselle. Ehdotusta kritisoitiin myös siitä, että myös vähäisistä tietoturvaloukkauksista oli ehdotuksen mukaan ilmoitettava valvontaviranomaiselle. Joulukuussa 2015 neuvoston, Euroopan parlamentin ja komission kolmikantaneuvotteluissa päästiin sopimukseen tietosuoja-asetuksesta. Kompromissitekstissä ilmoituksen tekemisen määräaika on 72 tuntia. Tietosuoja-asetuksessa ilmoitus ei tule koskemaan vähäisiä tietoturvaloukkauksia. Tämä asetuksen valmistelun aikana tehty rajaus johtaa kysymykseen siitä, kuinka objektiivisesti rekisterinpitäjät pystyvät tekemään arvion tietoturvaloukkauksen luonteesta ja vaikutuksista. Oikeusvertailevassa osuudessa esitellään, millaisia vaikutuksia vastaavantyyppisistä velvoitteista säätäminen on aiheuttanut Yhdysvalloissa.

Tietosuoja-asetuksessa lujitetaan tietoturvallisuutta asettamalla valvontaviranomaisille oikeus ja velvollisuus asettaa rekisterinpitäjälle hallinnollinen sakko, jos velvoitteiden toteutuksessa on puutteita. Asetustasolla on määritelty sakkojen enimmäismäärä, mutta valvontaviranomaiselle on jätetty asetuksessa tapauskohtaista harkintavaltaa.

Avainsanat: **Tietosuoja, henkilötietojen suoja, tietoturvallisuus**

Tutkimusmenetelmä: **Oikeusdogmaattinen**

Muita tietoja:
Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön _x_
Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi _x_
Suostun tutkielman luovuttamiseen Lapin maakuntakirjastossa käytettäväksi _x_
(vain Lappia koskevat)

SISÄLLYSLUETTELO

LÄHTEET

LYHENTEET

1 JOHDANTO ... 1
1.1 Henkilötietojen käsittelyn muuttunut ympäristö ... 1
1.2 Henkilötietodirektiivistä yleiseen tietosuoja-asetukseen ... 2
1.3 Rekisterinpitäjän uudet velvollisuudet ... 4
1.4 Tutkielman rakenteesta ... 7
2 TUTKIMUSAIHEEN ESITTELY ... 9
2.1 Tutkimuksen kohde ja metodi ... 9
2.2 Tutkimusalasta ... 11
3 KESKEISET KÄSITTEET ... 14
4 TIETOSUOJAN PERIAATTEET, STANDARDOINTI JA MUU ITSESÄÄNTELY ... 23
4.1 Tietosuojan periaatteet ... 23
4.2 Standardointi ja muu itsesääntely ... 25
5 TIETOTURVAN JA TIETOSUOJAN KANSALLINEN SÄÄNTELY ... 27
5.1 Yleisesti tietoturvallisuuden sääntelystä ... 27
5.2 Perustuslaki ... 27
5.3 Henkilötietolaki ... 28
5.3.1 Taustaa ... 28
5.3.2 KHO 2009:82, EUT C-73/07, EIT 21.7.2015 ... 31
5.3.3 Tietosuojavaltuutetun päätös (Dnro 1186/452/2010) ... 33
6 TIETOSUOJAN YLIKANSALLINEN SÄÄNTELY ... 34
6.1 OECD:n tietosuojaohjeet ... 34
6.2 Euroopan neuvoston tietosuojasopimus ... 35
6.3 Euroopan ihmisoikeussopimus ... 36
6.3.1 Taustaa ... 36
6.3.2 EIT 17.7.2008, I v. Suomi ... 37
6.4 Euroopan perusoikeuskirja ... 38
6.5 Henkilötietodirektiivi (95/46/EY) ... 40
7 TIETOSUOJA-ASETUS JA TIETOTURVALLISUUS ... 43
7.1 Tietosuoja-asetuksen valmistelusta ... 43
7.2 Tietosuojakysely ja esimerkkejä eurooppalaisista käytännöistä ... 45
7.3 Käsittelyn turvallisuus ... 47
7.4 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle ... 48
7.5 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle ... 50

7.6 Käsittely Suomen eduskunnassa – valiokuntien lausuntoja 52
7.7 Vahtikoirajärjestöjen ja muiden intressiryhmien kannanottoja 53
7.8 Hallinnolliset seuraamukset 56
7.9 WP 29:n kannanotto 03/2014 henkilötietojen tietoturvaloukkauksiin 59
8 ULKOMAISESTA TIETOSUOJALAINSÄÄDÄNNÖSTÄ 61
8.1 Ruotsi 61
8.2 Norja 64
8.3 Yhdysvallat 68
9 HENKILÖTIETOJEN SIIRTO EU:N ULKOPUOLELLE 76
9.1.1 Yleiset edellytykset 76
9.1.2 Maximilliam Schrems v. Data Protection Commissioner 76
10 JOHTOPÄÄTÖKSET 80

LIITE 1. Euroopan komission ehdotus asetukseksi henkilötietojen suojasta COM(2012) 11 Final.

LIITE 2. OSA-neuvoston yleisnäkemys asetukseksi henkilötietojen suojasta 15.6.2015.

LIITE 3. Rakenne epävirallisen suomennoksen pohjalta (kolmikantaneuvotteluiden ehdotus 15.12.2015).

LÄHTEET

Kirjallisuus

Aarnio, Aulis. Luentoja lainopillisen tutkimuksen teorioista. Helsinki: Unigrafia Oy Yliopistopaino 2011.

Aarnio, Aulis. Laintulkinnan teoria. Yleisen oikeustieteen oppikirja. Juva: Werner Söderström Oy 1989.

Aarnio, Aulis. Oikeussäännösten systematisointi ja tulkinta: Ajatuksia teoreettisesta ja käytännöllisestä lainopista. Teoksessa: Häyhä, Juha (toim.) Minun metodini. Porvoo: Werner Söderström lakitieto Oy 1997. s. 35–56.

Aarnio Aulis. Lainoppi. Teoksessa: Mattila, Heikki E.S. (toim.). Encyclopaedia iuridica Fennica VII: suomalainen oikeus-tietosanakirja. Oikeuden yleistieteet. Helsinki: Suomalainen lakimiesyhdistys 1999. s. 331–338.

Andreasson, Ari, Koivisto, Juha ja Ylipartanen, Arto. Tietosuojakäsikirja johdolle. Tallinna: Tietosanoma Oy 2015.

Andreasson, Ari, Koivisto, Juha ja Ylipartanen, Arto. Tietosuojavastaavan käsikirja 1. 2. laitos. Drukatava, Riika: Tietosanoma Oy 2014a.

Andreasson, Ari, Koivisto Juha ja Ylipartanen Arto. Tietosuojavastaavan käsikirja 2. Tallinna: Tietosanoma Oy 2014b.

Andreasson, Ari ja Koivisto, Juha. Tietoturvaa toteuttamassa. Tallinna: Tietosanoma Oy 2013.

Blanchette Jean-François. Burdens of Proof: Cryptographic Culture and Evidence Law in the Age of Electronic Documents. Cambridge, MA: The MIT Press 2012.*Blume, Peter* (toim.). Nordic Data Protection Law. Helsinki: Kauppakaari 2001.

Bygrave, Lee. Data privacy law : an international perspective. Oxford: Oxford University Press 2014.

Bygrave, Lee. Data Protection Law: Approaching Its Rationale, Logic and Limits. The Hague: Kluwer Law International 2002.

Bygrave, Lee A: Privacy and data protection in an international perspective. Stockholm Institute for Scandinavian Law 2010.

Fritsch, Clara. Data Processing in Employment Relations; Impacts of the European General Data Protection Regulation Focusing on the Data Protection Officer at the Worksite. Teoksessa: Gutwirth, Serge, Leenes, Ronald & de Hert, Paul (editors). Reforming European data protection law. Dordrecht: Springer 2015. s. 147–167.

Helopuro, Sanna, Perttula, Juha ja Ristola, Juhapekka. Sähköisen viestinnän tietosuoja. 2. painos. Helsinki: Talentum Media Oy 2009.

Hirvelä, Päivi ja Heikkilä, Satu. Ihmisoikeudet–käsikirja EIT:n oikeuskäytäntöön. Porvoo: Bookwell Oy 2013.

Hoikka, Mikko, Neuvonen, Riku ja Rautiainen, Pauli. Viestintämarkkinaoikeus. Helsinki: Kauppakamari 2016.

Jyränki, Antero ja Husa, Jaakko. Valtiosääntöoikeus. Hämeenlinna: Kariston Kirjapaino Oy 2012.

Järvinen, Petteri. Tietoturva & yksityisyys. Porvoo: Docendo Finland Oy 2002.

Kierkegaard, Sylvia. Data Insecurity: Scams, Blags & Scalawags. Teoksessa: The Secure Information Society: Ethical, Legal and Political Challenges. Krüger, Jörg, Nickolay, Bertram, Gaycken, Sandro (Eds.). London: Springer 2013. s. 117–134.

Kiss, Attila & Szőke, Gergely László. Evolution or Revolution? Steps Forward to a New Generation of Data Protection Regulation. Teoksessa: Gutwirth, Serge, Leenes, Ronald & de Hert, Paul (editors). Reforming European data protection law. Dordrecht: Springer 2015. s. 311–331.

Korhonen, Rauno. Poliisin valvontakeinot ja kansalaisten yksityisyyden suoja. Helsinki: Edita Publishing Oy 2005.

Korhonen, Rauno. Perusrekisterit ja henkilötietojen suoja. Rovaniemi: Lapin yliopistopaino 2003.

Korhonen, Rauno. Sähköinen asiointi ja viestintä julkisella sektorilla. Teoksessa: Niemi, Marja-Leena (toim.) Oikeus tänään | Osa I. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja 2016. s. 274–379.

Kuner, Christopher. Transborder data flows and data privacy law. Oxford: Oxford University Press 2013.

Mahkonen, Sami. Oikeus yksityisyyteen. Porvoo: WSOY 1997.

Miettinen, Juha E. Tietoturvallisuuden johtaminen–näin suojaat yrityksesi toiminnan. Jyväskylä: Gummerus Kirjapaino Oy 1999.

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

Nielsen, Jakob. Usability Engineering. Boston: Academic Press 1993.

Ojanen, Tuomas. EU-oikeuden perusteita. Helsinki: Edita Publishing Oy 2010.

Pitkänen, Olli, Tiilikka, Päivi ja Warma, Eija. Henkilötietojen suoja. Helsinki: Talentum 2013.

Pihlajamäki, Antti. Tietojenkäsittelyrauhan suoja. Suomalainen Lakimiesyhdistys. Jyväskylä: Gummerus Kirjapaino Oy 2004.

Pöysti, Tuomas. Tehokkuus, informaatio ja eurooppalaisen oikeusalue. Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta 1999.

Pöysti, Tuomas. Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet. Teoksessa: Kulla, Heikki (toim.): Viestintäoikeus. Helsinki: WSOY Lakitieto 2002, s. 35–81.

Raitio, Juha. Eurooppaoikeus ja sisämarkkinat. 3. Uudistettu painos. Helsinki: Talentum 2013.

Råman, Jari, Regulating secure software development, Analysing the potential regulatory solutions for the lack of security in software, Acta Universitatis Lapponiensis 102, University of Lapland, Faculty of Law, Rovaniemi 2006a.

Saarenpää, Ahti. Finland. Teoksessa: Blume, Peter: Nordic Data Protection. Helsinki 2001: Kauppakaari Oyj.

Saarenpää, Ahti. Oikeusinformatiikka. Teoksessa: Niemi, Marja-Leena (toim.) Oikeus tänään | Osa I. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja 2016. s. 67–273.

Saarenpää, Ahti. Henkilö- ja persoonallisuusoikeus. Teoksessa: Niemi, Marja-Leena (toim.) Oikeus tänään | Osa II. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja 2015. s. 203–430.

Saarenpää. Ahti. Oikeusinformatiikka. Teoksessa: Mattila, Heikki E. S. (toim.). Encyclopaedia iuridica Fennica VII: suomalainen oikeustietosanakirja. Oikeuden yleistieteet. Helsinki: Suoma-lainen lakimiesyhdistys, 1999. s. 713–726.

Saarenpää, Ahti (toim.)–Pöysti, Tuomas (toim.), Sarja, Mikko, Still Viveca & Balboa-Alcoreza, Ruxandra. Tietoturvallisuus ja laki: näkökohtia tietoturvallisuuden oikeudellisesta sääntelystä–tutkimusraportti. Helsinki: Edita Oy 1997.

Saarenpää. Ahti. Henkilöoikeus. Teoksessa: Helin, Markku (toim). Encyclopaedia iuridica Fennica III: suomalainen oikeustietosanakirja. Perhe-, työ- ja sosiaalioikeus. Helsinki: Suomalainen lakimiesyhdistys, 1996. s. 125–131.

Schartum, Dag Wiese. Norway. Teoksessa Blume, Peter (toim.). Nordic Data Protection Law. Helsinki: Kauppakaari 2001.

Seipel, Peter. Sweden. Teoksessa Blume, Peter (toim.). Nordic Data Protection Law. Helsinki: Kauppakaari 2001.

Siltala, Raimo. Oikeustieteen tieteenteoria. Suomalainen Lakimiesyhdistys: Helsinki 2003.

Skouma, Georgia & Léonards, Laura. On-line Behavioral Tracking: What May Change After the Legal Reform on Personal Data Protection. Teoksessa: Gutwirth, Serge, Leenes, Ronald & de Hert, Paul (editors). Reforming European data protection law. Dordrecht: Springer 2015. s. 35–60.

Solove, Daniel J., Rotenberg, Marc & Schwartz, Paul M. Information privacy law. New York, NY: Aspen Publishers 2006.

Timonen, Pekka. Johdatus lainopin metodiin ja lainopilliseen kirjoittamiseen. Helsinki: Helsingin yliopiston oikeustieteellinen tiedekunta 1998.

Tolonen, Hannu. Oikeuslähdeoppi. Vantaa: WSOY Lakitieto 2003.

Vanto, Jarno J. Henkilötietolaki käytännössä. Sähköinen kirja (ISBN 978-951-0-36933-3). Talentum Media Oy 2011.

Virolainen, Jyrki ja Martikainen, Petri. Tuomion perusteleminen. Helsinki: Talentum 2010.

Voutilainen, Tomi. ICT-oikeus sähköisessä hallinnossa–ICT-oikeudelliset periaatteet ja sähköinen hallintomenettely. Helsinki: Edita Publishing 2009.

Whitman, James Q. The Two Western Cultures of Privacy: Dignity Versus Lobert. Teoksessa: Solove, Daniel J., Rotenberg, Marc & Schwartz, Paul M. Information privacy law. New York, NY: Aspen Publishers 2006.

Ylipartanen, Arto. Tietosuoja terveyden huollossa–Potilaan asema ja oikeudet henkilötietojen käsittelyssä.3. uudistettu painos. Tallinna: Tietosanoma Oy 2010.

Öman, Sören & Lindblom Hans-Olof. Personuppgiftslagen: en kommentar. Stockholm: Norstedts juridik 2011.

Kotimaiset virallislähteet

HaVL 25/2015 vp. Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi)

HaVL 2/2015 vp. Valtioneuvoston kirjelmä eduskunnalle ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi)

HaVL 6/2013 vp. Valtioneuvoston kirjelmä ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi).

HaVL 11/2012 vp. Valtioneuvoston kirjelmä ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi)

HE 232/2014 vp. Hallituksen esitys eduskunnalle laiksi rikoslain eräiden tietoverkkorikoksia koskevien säännösten muuttamisesta ja eräiksi siihen liittyviksi laeiksi

HE 221/2013 vp. Hallituksen esitys eduskunnalle tietoyhteiskuntakaareksi sekä laeiksi maankäyttö- ja rakennuslain 161 §:n ja rikoslain 38 luvun 8 b §:n muuttamisesta.

HE 17/2002 vp. Hallituksen esitys Eduskunnalle laiksi sähköisestä asioinnista viranomaistoiminnassa.

HE 75/2000 vp. Hallituksen esitys Eduskunnalle laiksi yksityisyyden suojasta työelämässä ja eräiksi siihen liittyviksi laeiksi.

HE 184/1999 vp. Hallituksen esitys Eduskunnalle yksityisyyden, rauhan ja kunnian loukkaamista koskevien rangaistussäännösten uudistamiseksi

HE 30/1998 vp. Hallituksen esitys Eduskunnalle laiksi viranomaisten toiminnan julkisuudesta ja siihen liittyviksi laeiksi.

HE 96/1998. Hallituksen esitys Eduskunnalle henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

HE 309/ 1993 vp. Hallituksen esitys Eduskunnalle perustuslakien perusoikeussäännösten muuttamisesta.

OM 4/41/2013. Oikeusministeriön arviointimuistio: Identiteettivarkaus; henkilöllisyyden luomista koskevan hankkeen (identiteettiohjelma) työryhmän loppuraportin arviointia ja ehdotuksia jatkotoimiksi.

PeVL 12/2012 vp. Valtioneuvoston kirjelmä ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi).

PeVL 25/1998 vp. Hallituksen esitys henkilötietolaiksi ja eräiksi siihen liittyviksi laeiksi.

PeVL 8/1995 vp. Hallituksen esitys laiksi poliisin tehtävien suorittamisesta puolustusvoimissa.

PeVL 2/1990 vp. Ulkoasiainvaliokunnalle HE n:o 22 ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyn yleissopimuksen ja siihen liittyvien lisäpöytäkirjojen eräiden määräysten hyväksymisestä.

U 21/2012 vp. Valtioneuvoston kirjelmä ehdotuksesta asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (Yleinen tietosuoja-asetus) sekä direktiiviksi yksilöiden suojelusta toimivaltaisten viranomaisten henkilötietojen käsittelyssä rikosten torjumiseksi, tutkimiseksi, selvittämiseksi tai niistä syyttämiseksi tai rikosoikeudellisten seuraamusten täytäntöönpanemiseksi ja näiden tietojen vapaasta liikkuvuudesta (Tietosuojadirektiivi).

U 21/2012 vp HaV 03.06.2015 emeritusprofessori Ahti Saarenpää. Asiantuntijalausunto. Saatavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2015-AK-5174.pdf (Katsottu 13.12.2015).

Muu kotimainen virallisaineisto

Arkistolaitos. Yhteenveto: Tietosuojavaltuutetun toimiston ja arkistolaitoksen yhteiskyselystä hyvän tiedonhallinnan toteutumisesta viranomaisissa 28.1.2015. Saatavissa: http://www.arkisto.fi/uploads/Palvelut/Julkisen%20hallinnon%20s%C3%A4hk%C3%B6iset%20palvelut/Yhteenveto%20kyselyst%C3%A4%2028%201%2015.pdf (Katsottu 8.11.2015).

Liikenne- ja viestintäministeriö. Tietoturvallisuuslainsäädäntö: Kansainvälinen vertailututkimus. LUOTI-julkaisuja 4/2006. Luottamus ja tietoturva sähköisissä palveluissa –kehittämisohjelma. Saatavissa: http://www.lvm.fi/fileserver/4_2006.pdf (Katsottu 13.9.2015).

Liikenne- ja viestintäministeriö. Maailman luotetuinta digitaalista liiketoimintaa. Työryhmän ehdotus Suomen tietoturvallisuusstrategiaksi. Julkaisuja 4/2016. Saatavissa: http://urn.fi/URN:ISBN:978-952-243-472-2 (Katsottu 3.4.2016).

Oikeusministeriö. EU:n tietosuoja-asetuksen edellyttämät lainmuutokset selvitetään työryhmässä. Saatavissa: http://www.oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2016/02/euntietosuoja-asetuksenedellyttamatlainmuutoksetselvitetaantyoryhmassa.html (Katsottu 18.2.2016).

Oikeusministeriö. EU:n tietosuojauudistuksesta päästiin sopuun. Julkaistu 18.12.2015. Saatavissa: http://www.oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2015/12/euntietosuojauudistuksestapaastiinsopuun.html (Katsottu 21.2.2016).

Suomen Standardointitoimisto SFS ry. Mikä on standardi? Saatavissa: http://www.sfs.fi/usein_kysyttya (Katsottu 3.10.2015).

Tietosuojavaltuutetun toimisto. Henkilötietolain seuraamusjärjestelmä 27.102010. Tietosuojavaltuutetun toimiston opas. Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfprbX39/Henkilotietolain_seuraamusjarjestelma.pdf (Katsottu 3.10.2015).

Valtiontalouden tarkastusvirasto. Käyttäjäystävällisillä tietojärjestelmillä jopa 400 000 lääkärin vastaanottoaikaa lisää. Valtiontalouden tarkastusvirasto. Tiedote 2012. Saatavissa: https://www.vtv.fi/ajankohtaista/tiedotteet/2012/kayttajaystavallisilla_tietojarjestelmilla_jopa_400_000_laakarin_vastaanottoaikaa_lisaa.3546.news (Katsottu 30.7.2015).

Viestintävirasto. Tietosuoja-asetus tulee. Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/05/ttn20150521 1233.html (katsottu 27.5.2015).

Ulkomaiset virallislähteet ja muut asiakirjat

Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015. Saatavissa: https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (Katsottu 3.8.2015).

Commission decisions on the adequacy of the protection of personal data in third countries. Saatavissa: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (Katsottu 22.11.2015).

Committee of Civil Liberties, Justice and Home Affairs. Albrecht, Jan Philipp. Working document 2 on the protection of individuals with regard to processing of personal data and on the free movement of such data (General Data Protection Regulation). 8.10.2012. Saatavissa: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/915/915162/915162en.pdf (Katsottu 10.8.2015).

Committee on Civil Liberties, Justice and Home Affairs. Draft Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)(COM(2012)0011–C7-0025/2012–2012/0011(COD)) Committee on Civil Liberties, Justice and Home Affairs. Rapporteur: Albrecht, Jan Philipp. Saatavissa: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf (Katsottu 12.8.2015).

Datainspektionen, Ruotsin tietosuojavaltuutettu. Tillsyn enligt personuppgiftslagen (1998:204) –Salems kommunstyrelse. Diarienr 263-2011. Saatavissa: https://www.datainspektionen.se/Documents/beslut/2011-09-30-salems-kommun.pdf (Katsottu 4.8.2015).

Datainspektionen, Ruotsin tietosuojavaltuutettu. Säkerhet för personuppgifter. Datainspektionens allmänna råd. Reviderad november 2008. Saatavissa: https://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf (Katsottu 13.9.2015).

Datatilsynet, Norjan tietosuojaviranomainen. Håndtering av personopplysninger på avveier. Saatavissa: https://www.datatilsynet.no/Sikkerhet-internkontroll/ID-tyveri/Personopplysninger-pa-avveier---en-handlingsplan-for-virksomheter/ (Katsottu 16.11.2015).

Datatilsynet, Norjan tietosuojaviranomainen. Høringsuttalelse —EU-kommisjonens forslag til nye personvernregler, s. 6. Saatavissa: https://www.regjeringen.no/contentassets/082f55782d6e4d698f8571667f8ef20c/datatilsynet.pdf (Katsottu 13.9.2015).

Datatilsynet, Norjan tietosuojaviranomainen. Hva er personvern? Saatavissa: https://www.datatilsynet.no/personvern/Hva-er-personvern/ (Katsottu 22.11.2015).

European Comission. Data protection Factsheet. Eurobarometer. Saatavissa: http://ec.europa.eu/justice/dataprotection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf (Katsottu 13.9.2015).

Euroopan komissio. Lehdistötiedote. EU:n tietosuojauudistuksen hyväksyminen vauhdittaa digitaalisten sisämarkkinoiden toteuttamista. Saatavissa: http://europa.eu/rapid/press-release_IP-15-6321_fi.htm (Katsottu 5.1.2016).

Euroopan komissio. Lehdistötiedote. EU:n komissio ja Yhdysvallat sopivat uusista Atlantin yli tapahtuvan tiedonsiirron puitteista: yksityisyyden suojaa koskeva Privacy Shield –sopimus. Saatavissa: http://europa.eu/rapid/press-release_IP-16-216_fi.htm (Katsottu 14.2.2016).

Euroopan komission ehdotus Euroopan parlamentin ja neuvoston asetukseksi: yksilöiden suojelusta henkilötietojenkäsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus). COM(2012) 11 Final, annettu 25.1.2012. Saatavissa: http://register.consilium.europa.eu/doc/srv?f=ST+5853+2012+INIT&l=fi (Katsottu 23.11.2015).

Euroopan komissio. Special Eurobarometer 431: Data Protection -report. June 2015. Saatavissa: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (Katsottu 13.9.2015).

Euroopan unionin tuomioistuin: Lehdistötiedote 117/15. Saatavissa: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fi.pdf (Katsottu 1.11.2015).

Förslag till Datalag Prop. 1973:33. Saatavissa: http://data.riksdagen.se/dokument/FW0333 (Katsottu 31.7.2015).

Justis- og beredskapsdepartementet, Norjan oikeus- ja yleinen turvallisuus -ministeriö. Høring - EU-kommisjonens forslag til nye personvernregler. Saatavissa: https://www.regjeringen.no/no/dokumenter/horing---eu-kommisjonens-forslag-til-nye/id679008/ (Katsottu 13.9.2015).

Komission tiedonanto. COM(2015)566 final. The Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgement by the Court of Justice in Case 362/14 (Scherems). Saatavissa: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf (Katsottu 23.11.2015).

Komission tiedonanto. COM(2013) 846 final. Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52013DC0846&from=FI (Katsottu 7.11.2015).

Komission tiedonanto. KOM(2012) 9 lopullinen. Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys. Saatavissa. http://data.consilium.europa.eu/doc/document/ST-5852-2012-INIT/fi/pdf. Katsottu (21.2.2016).

Komission tiedonanto. KOM/2010/0609 lopull. Kattava lähestymistapa henkilötietojen suojaan Euroopan unionissa. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52010DC0609&from=FI (Katsottu 23.11.2015).

Komission tiedonanto. KOM(2010)245 lopullinen. Euroopan digitaalistrategia. Saatavissa: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:FI:PDF. (Katsottu 21.2.2016).

Komission tiedonanto. KOM(2007)267 lopullinen. Tavoitteena yleinen toimintalinja tietoverkkorikollisuuden torjumiseksi. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52007DC0267&from=FI. (Katsottu 31.3.2016).

Neuvoston, Euroopan parlamentin ja komission kolmikantaneuvotteluiden ehdotus tietosuoja-asetukseksi. Saatavissa suomeksi: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/fi/pdf (22.2.2016).

Oikeus- ja sisäasioiden neuvoston (OSA) yleisnäkemys uudesta tietosuoja-asetuksesta. Yleisnäkemyksen valmistelu. Saatavissa: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/fi/pdf (Katsottu 10.8.2015).

Statement of the Article 29 Working Party. Brussels, 16 October 2015. Saatavissa: http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (Katsottu 23.11.2015).

Sveriges riksdag, Ruotsin valtiopäivät. Sveriges fyra grundlagar. Studiematerial från riksdagen, s. 3. Saatavissa: http://www.riksdagen.se/PageFiles/dokument/bestall/svenska/Sveriges_fyra_grundlagar.pdf (Katsottu 4.10.2015).

WP 187. Opinion 15/2011 on the definition of consent. Saatavissa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (Katsottu 13.7.2015).

WP 01/2011. Working document on the current EU personal data breach framework and recommendations for future policy developments. Saatavissa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2011/wp184_en.pdf (Katsottu 23.11.2015).

WP 169. Lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä. Saatavissa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fi.pdf (Katsottu 23.11.2015).

WP 74. Working Document, Adopted on 3 June 2003: Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers. Saatavissa: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp74_en.pdf (Katsottu 23.11.1015).

Internetlähteet

Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005–2014. Howard, Philip N. & Gulyas, Orsolya. Central European University, Center for Media, Data and Society. Saatavissa: http://cmds.ceu.edu/sites/cmcs.ceu.hu/files/attachment/article/663/databreachesineurope_1.pdf (Katsottu 15.10.2015).

Effi, Electronic Frontier Finland. Saatavissa: https://effi.org/ (Katsottu 3.4.2016).

European Union Agency for Fundamental Rights. Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II. (Luxemburg: Publications Office of the European Union, 2010). Saatavissa: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf (Katsottu 3.10.2015).

Global Guide to Data Breach Notifications, 2013. World Law Group. Saatavissa: https://iapp.org/media/pdf/knowledge_center/WLG_Global_Data_Breach_Guide.pdf (Katsottu 16.11.2015).

Hirvonen, Ari. Mitkä metodit? Opas oikeustieteen metodologiaan. Yleisen oikeustieteen julkaisuja 17. Helsinki 2011. Saatavissa: http://www.helsinki.fi/oikeustiede/tutkimus_ja_julkaisut/julkaisut/yleinen_oikeustiede/hirvonen_mitka_metodit.pdf (Katsottu 28.2.2016).

The International Comparative Legal Guide to: Data Protection 2015. Hunton & Williams, Global Legal Group. Saatavissa: https://www.hunton.com/files/webupload/ICLG_DP15_Hunton_All_Chapters.pdf (Katsottu 8.11.2015).

iapp Podcast: How To Interpret the New GDPR. Initial Reactions To The Release Of The GDPR Final Draft 12-16-15. Saatavissa: https://soundcloud.com/user-142731699/initial-reactions-to-the-release-of-the-gdpr-final-draft-12-16-15. (Kuunneltu 31.1.2016).

International Association of Privacy Professionals. Data Protection Authorities. 2011 Global Survey. Saatavissa: https://iapp.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf (katsottu 8.11.2015).

Miten internetin jättiyritykset lobbasivat EU:ta ja miten ne paljastettiin. Saatavissa: http://rapport.fi/rapport/juttuidea.php?aid=225485 (Katsottu 14.2.2016).

National Conference of State Legislatures. Security Breach Notification Laws 1.4.2016. Saatavissa: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx. (Katsottu 3.4.2016).

OECD. OECD Privacy Law Enforcement Co-operation. Saatavissa: http://www.oecd.org/sti/ieconomy/privacylawenforcementco-operation.htm (Katsottu 4.6.2015).

OECD. 2013 OECD Privacy Guidelines. Saatavissa: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (Katsottu 1.11.2015).

Reding, Viviane: Making the EU Data Protection Reform irreversible. Lehdistötiedote 11.3.2014. Saatavissa: http://europa.eu/rapid/press-release_SPEECH-14-208_en.htm (Katsottu 3.10.2015).

Suomen sukututkimusseura . Sukututkimuksen käytännesäännöt. Saatavissa: http://www.sukuhistoria.fi/sshy/sivut/sshy/kaytannesaannot.pdf (Katsottu 8.11.2015).

U.S.-EU Safe Harbor List. Saatavissa: https://safeharbor.export.gov/list.aspx (Katsottu 21.11.2015).

Vahtikoirajärjestöjen ja muiden intressiryhmien kannanottoja

American Chamber of Commerce (AmCham, Amerikan kauppakamari). AmCham EU Proposed Amendments on the General Data Protection Regulation. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/AmCham_EU_Proposed_Amendments_on_Data_Protection.pdf (Katsottu 14.11.2015).

eBay Inc. eBay position Industry, Research and Energy Committee draft opinion on the General Data Protection Regulation. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Position-paper_eBay-Inc_ITRE-opinion-on-data-protection-regulation.pdf (Katsottu 15.11.2015).

EDRi. Comments on the draft JURI opinion on the General Data Protection Regulation, s. 33. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/blob/master/raw/lobby-documents/EDRis-comments-on-the-JURI-draft-opinion-on-the-general-data-protection-regulation.pdf (Katsottu 3.4.2016).

Eff. O'Brien, Danny and Reitman, Rainey. The Privacy Shield is Riddled with Surveillance Holes. Saatavissa: https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes. (Katsottu 3.4.2016).

EPIC, Electronic Privacy Center. Saatavissa: https://epic.org/privacy/intl/eu_data_protection_directive.html. (Katsottu 3.4.2016).

European Digital Rights. Article 31 – Communication of a personal data breach to the supervisory authority, Commission Proposal. Saatavissa: http://protectmydata.eu/articles/articles-31-40/article-31/ (Katsottu 20.12.2015).

European Digital Rights. Article 32 – Communication of a personal data breach to the data subject, Commission Proposal. Saatavissa: http://protectmydata.eu/articles/articles-31-40/article-32/ (Katsottu 20.12.2015).

Facebook. Comments from Facebook on the European Commission's proposal for a Regulation "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)" Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Facebook.pdf (Katsottu 14.11.2015).

Microsoft . Microsoft positions and suggestions for the draft General Data Protection Regulation. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Microsoft.docx (Katsottu 15.11.2015).

Privacy International. Our analysis of the European Comission's proposal for a general Data Protection Regulation. Saatavissa: https://www.privacyinternational.org/node/181. (Katsottu 3.4.2016).

Statewatch. New challenges - old problems. Commission proposals on revising the 1995 Data Protection Directive. Saatavissa: http://www.statewatch.org/news/2010/oct/05eu-dp-com.htm (Katsottu 3.4.2016).

Telefónica. Telefónica's proposed amendments to the Proposal for a REGULATION 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 Directive). Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Telefonica-Amendments-on-GDPR-Proposal.pdf (Katsottu 14.11.2015).

Lehdet

Bevitt, Ann & Sabett, Randy. Does the US need an EU-style data protection law? Privacy & Data Protection 15(7). s. 3–5.

Bradford, Anu. The Brussels effect. Northwestern University Law Review. Fall 2012, 107 (1). s. 1–67.

Burdon, Mark, Lane, Bill & von Nessen, Paul. Data breach notification law in the EU and Australia – Where are we now? Computer Law & Security Review. 2012(3). s. 296–307.

Kuner, Christopher. An international legal framework for data protection: Issues and prospects. Computer Law & Security Review. 2009(25). s. 307–317.*Raeste, Juha-Pekka.* Uudet tietosuoja-asetukset panevat tietovuodot kohta kuriin. Helsingin Sanomat 23.1.2016.

King, Nancy J. & Raja, V.T. Protecting the privacy and security of sensitive customer data in the cloud. Computer Law & Security Review. June 2012, 28(3). s. 308–319.

Lyytikäinen, Susanna. Tivi 16.10.2014. Tietovuodon aiheuttaa usein organisaation oma huolimattomuus.

Myrsky, Matti. Tarvitsemmeko oikeuslähdeoppeja? Oikeus 2010 (39);1. s. 50– 53.

Männikkö, Päivi. Ikuisesti rekisterissä. Tietosuoja. 1/2015. s. 43.

Nuotio, Kimmo. Oikeuslähteet ja yleiset opit. LM 2004. s. 1267–1291.

Ollila, Riitta. Henkilötietojen suoja EU:n perusoikeutena. Defensor Legis N:0 5/2014. Referee-artikkeli. s. 814–824.

Pöysti, Tuomas. Julkisen vallan velvoite edistää sähköisen identiteetin ja verkkoyhteiskunnan infrastruktuurin turvallisuutta. Oikeus 1/2000, s. 91–112.

Romanosky, Sasha, Telang, Rahul & Acquisti, Alessandro. Do Data Breach Disclosure Laws Reduce Identity Theft? Journal of Policy Analysis and Management 2011. 30 (2). s. 256–286.

Råman, Jari. European Court of Human Rights: Failure to take effective information security measures to protect sensitive personal data violates right to privacy–I v. Finland, no. 20511/03, 17 July 2008. Computer law & Security Review. 2008, 24(6). s. 562–564.

Råman, Jari. Tietoturvallisuus on myös perusoikeus. Lakimies 5/2006b, s. 818–824.

Schwartz, Paul M. The EU-U.S Privacy collision: A turn to institutions and procedures. Harvard Law Review. May 2013, 126 (7). s. 1966–2009.

Schwartz, P.M. & Solove, D.J. Reconciling personal information in the United States and European Union. California Law Review. August 2014, 102(4). s. 877–916.

Storås, Niclas. Tivi 9.2.2015. Tietosuoja-asetus panee järjestelmät remonttiin.

Svantesson, Dan Jerker B. Data protection in cloud computing–The Swedish perspective. Computer law & Security review, August 2012, 28 (4). s. 476–480.

Valo, Janne. Potilastietojen salassapito potilastietojärjestelmien kannalta. Refereeartikkeli. Helsinki Law Review 2012/2. s. 281–307.

Tuomioistuinratkaisut

Suomi: ylimmät tuomioistuimet

KHO 2009:82.

KKO 1996:34.

KKO 1994:80.

KKO 1992:3.

Euroopan yhteisöjen/ unionin tuomioistuin

Euroopan unionin tuomioistuimen tuomio.6.10.2015. Asia C-362/14.

Euroopan unionin tuomioistuimen tuomio. 13.5.2014. Asia C-131/12.

Euroopan unionin tuomioistuimen tuomio. 9.11.2010. Yhdistetyt asiat C-92/09 ja C-93/09.

Euroopan unionin tuomioistuimen tuomio. 6.11.2003. Asia C-101-1. (Göra hovrättin esittämä ennakkoratkaisupyyntö).

Yhteisöjen tuomioistuimen tuomio 12.11.1969. Asia 29/69.

Euroopan ihmisoikeustuomioistuin

Euroopan ihmisoikeustuomioistuin. Case Satakunnan Markkinapörssi Oy and Satamedia Oy v. Finland. 21.7.2015.

Euroopan ihmisoikeustuomioistuin. Case I v. Finland. 17.7.2008.

Viranomaisten päätökset ja suositukset

Tietosuojavaltuutetun päätös. Dnro 1186/452/2010.

Tietosuojavaltuutetun päätös. Dnro 1475/41/2009.

VAHTI (4/2013). Henkilöstön tietoturvaohje. Valtionhallinnon tietoturvallisuuden johtoryhmä, valtiovarainministeriö, Helsinki.

VAHTI (8/2008). Valtionhallinnon tietoturvasanasto. Valtionhallinnon tietoturvallisuuden johtoryhmä, valtiovarainministeriö, Helsinki.

VAHTI (9/2006). Käyttövaltuushallinnon periaatteet ja hyvät käytännöt. Valtionhallinnon tietoturvallisuuden johtoryhmä, valtiovarainministeriö, Helsinki.

Standardit

SFS-ISO/IEC 29100. Informaatioteknologia. Turvallisuus. Tietosuojan perusteet.

SFS-EN ISO 9241-11. Näyttöpäätteillä tehtävän toimistotyön ergonomiset vaatimukset. Osa 11: Käytettävyyden määrittely ja arviointi.

SFS-ISO/IEC 27000. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Yleiskatsaus ja sanasto.

LYHENTEET

EFF	Electronic Frontier Foundation
EIS	Euroopan ihmisoikeussopimus (62/1999)
EIT	Euroopan ihmisoikeustuomioistuin
EPIC	Electronic Privacy Information Center
et al.	Latinaa: et alii, ja muut
EU	Euroopan unioni
HaVL	Hallintovaliokunnan lausunto
HaVM	Hallintovaliokunnan mietintö
HE	Hallituksen esitys
HetiL	Henkilötietolaki (523/1999)
HRL	Henkilörekisterilaki (471/1987)
IAPP	International Association of Privacy Professionals, tietosuoja-ammattilaisten järjestö
Ibid.	Latinaa: ibidem, samassa paikassa
KSL	Kuluttajansuojalaki (38/1978)
OECD	Organisation for Economic Cooperation and Development, Taloudellisen kehityksen ja yhteistyön järjestö
OSA	Oikeus- ja sisäasioiden neuvosto
PeVL	Perustuslakivaliokunnan lausunto
RL	Rikoslaki (39/1889)
SEU	Sopimus Euroopan unionista
SEUT	Sopimus Euroopan unionin toiminnasta
SVTSL	Sähköisen viestinnän tietosuojalaki (516/2004)
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VTV	Valtiontalouden tarkastusvirasto
WP	Working Party, tietosuojatyöryhmä, joka on perustettu direktiivin 95/46/EY 29 artiklalla

1 JOHDANTO

1.1 Henkilötietojen käsittelyn muuttunut ympäristö

Tietokoneet mahdollistavat suurten tietomäärien varastoimisen ja nopean käsittelemisen. Liike- ja talouselämä, teollisuus, sairaalat ja viranomaiset ovat viime vuosikymmeninä tulleet entistä riippuvaisemmiksi tietokoneista. Nykyaikainen yhteiskunta rakentuu tietotekniikan varaan: näitä järjestelmiä käytetään esimerkiksi liikenteen valvonnassa ja terveydenhuollossa. Tietoverkkojen laajeneminen lisää niiden haavoittuvuutta. Tämä kehitys on toisaalta myös mahdollistanut uudenlaisia rikollisuuden muotoja. Tietotekniikkaan liittyvät rikokset voivat aiheuttaa sekä taloudellisia että ihmisten turvallisuuteen kohdistuvia seurauksia.[1]

Teknologioiden nopean kehityksen myötä henkilötietoja kerätään entistä enemmän. Samalla henkilötietojen käsittelyssä ja siirtämisessä käytettävät keinot ovat muuttuneet radikaalisti. Yksilöillä on tässä digitaalisessa ympäristössä oikeus valvoa tehokkaasti henkilötietojaan. Talouskasvun ja Euroopan unionin teollisuuden kilpailukyvyn kannalta on olennaista, että kuluttajat luottaisivat verkkopalveluihin.[2] Yksityisyydensuojaan

[1] Pihlajamäki 2004, s. 5.
Saarenpään et al. 1997, s. lix mukaan tietoturvallisuusrikokset voidaan luokitella kolmeen tyyppiin:
1) rikokset, joiden tunnusmerkistöön kuuluvat tietoturvallisuusvelvoitteiden laiminlyönti. Tähän tyyppiin kuluvia rikosoikeudellisia säännöksiä on sisällytetty henkilötietolakiin.
2) rikokset, jotka kohdistuvat tieto- ja viestintäjärjestelmiin tai itse tietoon. Tähän tyyppiin on luetettavissa esim. tietojärjestelmään murtautuminen sekä perinteiset rikokset kuten varkaus tai vahingonteko. Pihlajamäki 2004, s. 57 toteaa, että tietomurto vaarantaa tiedon *luottamuksellisuuden:* murtautuminen osoittaa, että järjestelmässä on ollut aukko. Murron jälkeen tietojen luottamuksellisuus ei enää ole varmaa. Vahingonteko kohdistuu Pihlajamäen mukaan tiedon *eheyteen*, sillä tekojen tunnusmerkistöön kuuluu tiedon muuttaminen. Katso myös Kappale 3 KESKEISET KÄSITTEET.
3) rikokset, joiden tunnusmerkistöön kuuluvat informaation oikeudeton julkaiseminen. Tähän tyyppiin kuuluvat esim. salassapitorikos ja tekijänoikeusrikkomus.
Tietoverkkorikollisuus voidaan puolestaan jaotella komission tiedonannon KOM(2007)267 lopullinen, s. 2 mukaan seuraavasti:
1) perinteiset rikollisuuden muodot (esim. petokset ja väärentämisen), jotka on tehty käyttäen sähköisiä viestintäverkkoja ja tietojärjestelmiä
2) laittoman sisällön (mm. rotuvihaan yllyttävän tai lapsen seksuaalista hyväksikäyttöä esittävän materiaalin) julkaiseminen sähköisissä viestimissä.
3) rikokset, joita esiintyy ainoastaan sähköisissä verkoissa (esim. hakkerointi, hyökkäykset tietojärjestelmiä vastaan sekä palvelunesto).
Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52007DC0267&from=FI. (Katsottu 31.3.2016).

[2] Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys/ KOM(2012) 9 lopullinen, s. 2.

liittyvä huoli on yksi merkittävimmistä syistä siihen, että kuluttajat eivät osta tavaroita ja palveluita verkosta.[3]

Usein ajatellaan, että tietoturvauhkat liittyvät lähinnä kolmansiin osapuoliin kuten ammattirikollisiin tai pahantahtoisiin valtioihin. Tämä on myös tietosuojalainsäädännössä ollut pitkälti lähtökohtana. Todellisuudessa oman henkilökunnan huolimattomuus aiheuttaa kuitenkin suurimman osan tietoturvaongelmista. Tietosuojalainsäädännössä tämä on otettu huomioon säätämällä yritysten velvollisuudesta huolehtia organisatorisista toimenpiteistä tietojen suojaamiseksi.[4]

EU:n alueella tapahtui 229 tunnettua tietovuotoa vuosina 2004–2014. Näissä vaarantui 227 miljoonaa henkilötietoa. Organisaatioiden oma huolimattomuus oli yleisin vuodon aiheuttaja.[5]

1.2 Henkilötietodirektiivistä yleiseen tietosuoja-asetukseen

Vuoden 1995 *henkilötietodirektiivi* (95/46/EY) on EU:n tärkein tietosuojasäännös.[6] Sen tavoitteet sisämarkkinoiden toiminnan turvaamisesta ja perusoikeuksien ja yksilön vapauksien tehokkaasta suojaamisesta pätevät yhä. Internet oli vasta yleistymässä, kun henkilötietodirektiivi annettiin 20 vuotta sitten.[7] Kuluneiden vuosikymmenten aikana on tekniikan alalla tapahtunut isoja muutoksia esimerkiksi liittyen esineiden internetiin, Big Dataan ja pilvipalveluihin.[8] Nykyisessä digitaalisessa toimintaympäristössä henkilötietodirektiivin säännöt eivät enää riitä takaamaan oikeutta tehokkaaseen henkilötietojen suojaan.[9]

Nykyinen henkilötietodirektiivi on ”johtanut 28 kansallisen lain tilkkutäkkiin.” Tämä on hankaloittanut yritysten toimintaa ja tullut niille kalliiksi. On arvioitu, että direktiivin

[3] Euroopan digitaalistrategia/ KOM(2010)245 lopullinen, s. 14.
[4] Pitkänen et al. 2013, s. 217.
[5] Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005–2014, s. 3. Lähdettä on käytetty suomenkielisessä artikkelissa Tivissä: Tietovuodon aiheuttaa usein organisaation oma huolimattomuus 16.10.2014.
[6] Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys/ KOM(2012) 9 lopullinen, s. 4.
[7] Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys/ KOM(2012) 9 lopullinen, s. 3.
[8] iapp Podcast: How To Interpret the New GDPR. Initial Reactions To The Release Of The GDPR Final Draft 12-16-15. Saatavissa: https://soundcloud.com/user-142731699/initial-reactions-to-the-release-of-the-gdpr-final-draft-12-16-15. (Kuunneltu 31.1.2016).
[9] Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys/ KOM(2012) 9 lopullinen, s. 3.

vuosittaiset kustannukset yrityksille ovat olleet noin 2,3 miljardia euroa vuosittain.[10] Direktiivin pohjalta EU:n jäsenmaissa laaditut lait ovat muutoksenhakukeinojen, seuraamusten ja sitovuuden suhteen huomattavan erilaisia.[11]

Euroopan komissio antoi tammikuussa 2012 ehdotuksen tietosuojasääntelyn uudistamisesta EU:ssa.[12] Uudistuksen kautta parannetaan yksilön mahdollisuuksia valvoa henkilötietojaan esimerkiksi varmistamalla, että rekisteröidyltä vaaditaan nimenomainen *suostumus* ja antamalla verkkoympäristössä internetin käyttäjille tehokas *oikeus tulla unohdetuksi*. Komission ehdotuksessa lujitetaan tietoturvallisuutta kannustamalla käyttämään teknologioita, jotka minimoivat henkilötietojen tallentamisen ja parantavat siten yksityisyydensuojaa. Tietoturvallisuuden vahvistamiseen kuuluu myös yksityisyydensuojaa tukevien vakioasetusten ja yksityisyydensuojaa koskevien sertifiointijärjestelmien käyttämiseen kannustaminen.[13] Tietoturvallisuutta lujitetaan myös asettamalla rekisterinpitäjille velvollisuus ilmoittaa tietoturvaloukkauksista tietosuojaviranomaisille ja asianomaisille yksilöille.[14] Tietosuoja-asetuksen ydin on tehokkaasti turvata myös sellaisten rekisteröityjen oikeus yksityisyyteen, jotka eivät juuri ole tietoisia tästä heille rekisteröityinä kuuluvasta oikeudestaan.[15] EU:n ns. tietosuojapakettiin kuuluu yleisen tietosuoja-asetuksen lisäksi direktiivi, jota oikeus- ja lainvalvontaviranomaiset soveltavat käsitellessään henkilötietoja esim. rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.[16]

---

[10] Reding 2014: Making the EU Data Protection Reform irreversible. Redingin puhe ennen äänestystä Euroopan parlamentin täysistunnossa. Saatavissa: http://europa.eu/rapid/press-release_SPEECH-14-208_en.htm (Katsottu 3.10.2015). Komission tiedonannon (KOM(2012) 9 lopullinen), s. 8 mukaan tämä nettosäästö kertyy pelkästään hallinnollisen rasituksen kevenemisen johdosta. Saatavissa: http://data.consilium.europa.eu/doc/document/ST-5852-2012-INIT/fi/pdf. (Katsottu 23.11.2015).

[11] European Union Agency for Fundamental Rights. Data Protection in the European Union: the role of National Data Protection Authorities. Strengthening the fundamental rights architecture in the EU II, s. 31. (Luxemburg: Publications Office of the European Union, 2010). Saatavissa: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf (Katsottu 3.10.2015).

[12] Yleinen tietosuoja-asetus/ COM(2012) 11 Final, s. 1. Komission tietosuoja-asetusehdotuksen rakenne on kuvattu liitteessä 1.

[13] Yksityisyydensuoja verkottuvassa maailmassa–Euroopan uusi tietosuojakehys/ KOM(2012) 9 lopullinen, s. 6.

[14] Ibid., s. 7.

[15] Kiss & Szőke 2015, s. 328 lisäävät, että kyse on ”taustaturvaamisesta”, joka on lähestymistapana verrattavissa kuluttajansuojaan: kuluttajille tarjotaan paljon tietoa, ja vaikka he kiinnittävät vain vähän huomiota tai eivät kiinnitä siihen huomiota, suojelun vähimmäistaso turvataan. Täysin kohtuuttomat sopimukset eivät ole sallittuja. Vertaa KSL (38/1978) 3:1.1.

[16] Oikeusministeriö. EU:n tietosuojauudistuksesta päästiin sopuun. Julkaistu 18.12.2015. Saatavissa: http://www.oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2015/12/euntietosuojauudistuksestapaastiinsopuun.html (Katsottu 21.2.2016).

Komissio on todennut, että asetus on sopivin säädöstyyppi henkilötietojen suojaa koskevan kehyksen määrittämiseksi unionissa. *Asetus* on EU:ssa suoraan sovellettavaa oikeutta ja siten asetus on omiaan sekä takaamaan paremman oikeusvarmuuden että vähentämään lainsäädännön hajanaisuutta. *Toissijaisuusperiaatteen* mukaisesti Euroopan unionin tasolla toteutetaan toimia vain, jos jäsenvaltiot eivät voi yksin saavuttaa suunnitellun toiminnan tavoitteita riittävällä tavalla. Toissijaisuusperiaate on vahvistettu Euroopan unionista tehdyn sopimuksen (SEU-sopimus) 5 artiklan 3 kohdassa. Nykyinen henkilötietodirektiivi on johtanut siihen, että tietosuojan taso vaihtelee EU:n jäsenvaltioiden välillä. Perusoikeuskirjan 8 artiklassa kuitenkin taataan oikeus henkilötietojen suojaan, ja se edellyttää, että tietosuojan tason on oltava sama koko EU:n alueella. Sekä EU:n sisällä että EU:n ja kolmansien maiden välillä tapahtuu henkilötietojen siirtoja yhä enemmän ja nopeammin. Jäsenvaltiot eivät kykene tässä tilanteessa yksinään vähentämään henkilötietojen siirtämiseen liittyviä haasteita, erityisesti silloin kun haasteet liittyvät kansallisten lainsäädäntöjen hajanaisuuteen.[17]

Euroopan parlamentti ja neuvosto hyväksyvät lopulliset asetustekstit vuoden 2016 alussa.[18] Tietosuoja-asetus tulee sovellettavaksi kahden vuoden siirtymäajan jälkeen.[19] Voimaan tullessaan asetus korvaa nyt voimassa olevan henkilötietodirektiivin (95/46/EY).[20]

1.3 Rekisterinpitäjän uudet velvollisuudet

Tietosuoja-asetus asettaa rekisterinpitäjille tilivelvollisuuden. Organisaation on pystyttävä osoittamaan, että rekisterinpitäjä huomioi tietosuojasäännökset toiminnassaan. Organisaatiolle ei tietosuoja-asetuksen mukaan siis riitä, että organisaatio noudattaa asetusta. Valvovalla viranomaisella on oikeus ja velvollisuus antaa rekisterinpitäjälle hallinnollinen sakko, jos velvoitteiden toteutuksessa tai dokumentoinnissa on puutteita. Tietosuoja-asetuksen myötä rekisterinpitäjää tulee ohjaamaan periaate, jonka mukaan tuotanto- ja palveluprosessien tietosuoja on suunniteltava huolellisesti (*privacy by de-*

[17] Tietosuoja-asetusehdotus, s. 6. Tietosuoja-asetusehdotuksen s. 4 todetaan, että nykyistä henkilötietojen suojan hajanaisuutta ovat voimakkaasti kritisoineet erityisesti talouden toimijat.
[18] Euroopan komissio – Lehdistötiedote. EU:n tietosuojauudistuksen hyväksyminen vauhdittaa digitaalisten sisämarkkinoiden toteuttamista. Saatavissa: http://europa.eu/rapid/press-release_IP-15-6321_fi.htm (Katsottu 27.1.2016).
[19] Yleinen tietosuoja-asetus/ COM(2012) 11 Final: 91 artikla 2 kohta.
[20] HaVL 2/2015 vp–U 21/2012 vp, s. 4.

sign). Rekisterinpitäjän on myös toteutettava tuotanto- ja palveluprosessien tietosuoja oletusarvoisesti ja sisäänrakennetusti (*privacy by default*).[21]

Voimassa oleva henkilötietodirektiivi ei aseta rekisterinpitäjille velvollisuutta ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista. Muutamat EU:n jäsenvaltiot ovat implementoineet ilmoitusvelvollisuuden kansalliseen lainsäädäntöönsä.[22] Tietosuoja-asetuksen myötä rekisterinpitäjälle on tulossa ilmoitusvelvollisuus tietoturvaloukkauksista.[23] Ilmoitus on tehtävä vähäisiä rikkomuksia lukuun ottamatta aina valvovalle viranomaiselle ja tietyin ehdoin myös rekisteröidylle. Valvontaviranomaisella[24] on tietosuoja-asetusehdotuksen mukaan oikeus määrätä sakkoja rekisterinpitäjälle, jos rekisterinpitäjä on rikkonut tietosuojasääntöjä.

Komission tiedonannossa kattavasta lähestymistavasta henkilötietojensuojaan Euroopan unionissa todetaan, että rekisteröityjen on tärkeää saada ilmoitus, jos heidän tietonsa on vahingossa tai laittomasti tuhottu tai hukattu. Ilmoituksen saaminen on tärkeää myös silloin, jos rekisteröidyn tietoja on muutettu, niitä on paljastettu sivullisille tai niitä on tarkastellut joku sivullinen. Sähköisen viestinnän tietosuojadirektiivin (2002/58/EY) 4 artiklassa[25] säädetään velvollisuudesta ilmoittaa henkilötietojen suojaa koskevista loukkauksista.[26] Tämä velvoite koskee ainoastaan televiestintäalaa. Tietosuojaloukkauksia esiintyy muillakin aloilla ja siksi ilmoitusvelvollisuuden laajentamista muille aloille alettiin tutkia.[27]

---

[21] Andreasson et al. 2015, s. 9– 10.

[22] Itävalta ja Saksa. Muutamissa EU:n jäsenvaltioissa (Belgia, Tanska, Irlanti ja Iso-Britannia) tietosuojaviranomainen on vahvasti suositellut ilmoitusvelvollisuutta.

[23] Bygraven 2014, s. 209 mukaan velvollisuus ilmoittaa tietoturvaloukkauksista on tullut osaksi eurooppalaista lainsäädäntöä Yhdysvaltojen lakien innoittamana. Katso tarkemmin Yhdysvaltoja käsittelevä kappale 8.3.

[24] Tietosuoja-asetuksen mukainen valvontaviranomainen olisi Suomessa tietosuojavaltuutettu. Viestintävirasto: Tietosuoja-asetus tulee.
Saatavissa: https://www.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2015/05/ttn201505211233.html (Katsottu 18.10.2015).

[25] Suomessa direktiivin ilmoitusvelvollisuus pantiin täytäntöön SVTSL 21 §:llä. Nykyään ilmoitusvelvollisuudesta säädetään tietoyhteiskuntakaaren (HE 221/2013 vp) 274 §:ssä ja 275 §:ssä.

[26] Hoikka et al 2016, s. 515 toteavat, että ilmoitusvelvollisuus voi liittyä toetoturvauhkiin ja –loukkauksiin, jotka voivat vaarantaa tai vaarantavat tilaajan tai käyttäjän viestintämahdollisuudet. Ilmoituksesta on käytävä ilmi, mistä tilaaja tai käyttäjä saa lisätietoja. Katso myös tietosuoja-asetuksen asettamat vaatimukset ilmoituksen sisällöstä kappaleessa 7.5.

[27] Komission tiedonanto kattava lähestymistavasta henkilötietojen suojaan Euroopan unionissa, KOM/2010/0609 lopull., kappale Läpinäkyvyyden lisääminen rekisteröidyn kannalta. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52010DC0609&from=FI (Katsottu 23.11.2015).
Elokuussa 2013 tuli voimaan EU:n komission asetus 611/2013 henkilötietojen tietoturvaloukkauksista. Asetus koskee teleyritysten ilmoituksia henkilötietojen tietoturvaloukkauksista. Asetuksen 2 artiklassa säädetään palvelintarjoajan ilmoittamisvelvollisuudesta kansalliselle viranomaiselle (Suomessa Viestintä-

Euroopan tietosuojalainsäädäntöön kohdistuvat muutokset voidaan nähdä osoituksena siitä, ettei Euroopan unioni yritä vältellä ongelmia. Tietosuoja-asetusehdotuksessa ei ole kyse lainsäädännön pienestä muutoksesta, vaan muutos on paljon merkityksellisempi. Tietosuoja-asetusehdotuksen myötä myös siirrytään kysymyksestä ”mihin rekisteröidyillä on oikeus” kysymykseen ”mitä rekisterinpitäjien on tehtävä”. Lobbausaktiviteetit ja yli 4000 muutosehdotusta tietosuoja-asetusehdotukseen osoittavat, että useat organisaatiot pitävät muutosta tietosuojalainsäädännössä käänteentekevänä.[28]

Suomessa organisaatiot eivät ole varautuneet tietosuojasäännösten tiukentumiseen riittävästi.[29] Suuri osa yrityksistä odottaa lopullisen muotoilun valmistumista. Tietojärjestelmien myyjät ja ostajat ovat valmistautuneet muutoksiin vaihtelevasti.[30]

virastolle) ja 3 artiklassa velvollisuudesta ilmoittaa tilaajalle tai henkilölle. WP 29 Working document 01/2011, s. 9 kannatti ilmoitusvelvollisuuden laajentamista telealan lisäksi muihinkin rekisterinpitäjiin. WP 29 suositteli, että komissio käyttäisi henkilötietodirektiiviä muutettaessa samoja määritelmiä kuin sähköisen viestinnän tietosuojadirektiivissä, erityisesti kun kyse on rekisteröidylle ilmoittamisvelvollisuuskynnyksen ylittymisestä (Working document 01/2011, s.10).

[28] Kiss & Szőke 2015, s. 328. Andreasson et al. 2014b, s. 19 toteavat, että kansainväliset toimijat kuten Amazon, Google ja Facebook joutuvat ottamaan huomioon eurooppalaisen sääntelyn. Yhdysvaltalaiset internetjätit ovatkin Yhdysvaltojen hallituksen tukemina lobanneet päättäjiä tietosuoja-asetusehdotusta vastaan.

[29] Andreasson et al. 2015, s.35 huomauttavat lisäksi, että tietosuoja-asetuksen myötä koko kansallinen erityislainsäädännön verkko tulee arvioitavaksi uudelleen Suomessa. Katso myös alaviite 133 Arkistolaitoksen ja Tietosuojavaltuutetun tekemästä tutkimuksesta.

[30] Storås 2015: Tietosuoja-asetus panee järjestelmät remonttiin.

1.4 Tutkielman rakenteesta

Maisteritutkielman aihe esitellään luvussa 2. Tutkielman kannalta keskeisin käsitteistö määritellään luvussa 3.

Tietosuojan periaatteet ja alaa sääntelevä standardointi sekä muu itsesääntely on koottu lukuun 4.[31] Tutkielman luvussa 5 esitellään, miten yksityisyydestä ja henkilötietojen käsittelystä on säädetty perustuslaissa ja henkilötietolaissa.

Luvussa 6 esitellään tietosuojan sääntelyn globaaleja instrumentteja eli OECD:n tietosuojaohjeet, Euroopan neuvoston ihmisoikeussopimus, Euroopan perusoikeuskirja ja henkilötietodirektiivi (95/46/EY).[32]

---

[31] Myrskyn 2010, s. 50 mukaan oikeuslähdeopissa on perinteisesti selvitetty niitä lähteitä, joista lainsoveltajat saavat lainmukaisen perustan ratkaisuilleen. Oikeusjärjestyksen muodostavat oikeusnormit on tapana jakaa oikeussääntöihin ja oikeusperiaatteisiin. Virolainen & Martikainen 2010, s. 382 ovat selittäneet oikeussääntöjen ja periaatteiden merkityseroja seuraavasti: *oikeussäännöt* edustavat konkreettista ja yksityiskohtaista oikeudellista sääntelyä. *Oikeusperiaatteet* puolestaan sisältävät väljiä ja tavoitteellisia linjauksia, joiden toteutumiseen tulisi pyrkiä mahdollisimman suuressa määrin. Oikeusperiaatteilla on vahvasti velvoittavan oikeuslähteen asema silloin, kun ne ilmenevät sellaisenaan laista tai maantavasta. Muutoin oikeusperiaatteet lasketaan sallittuihin oikeuslähteisiin, jotka sisältävät arvoja ja arvostuksia. Sääntöjen ehdottomuus ilmenee siinä, että niitä joko sovelletaan tai ei sovelleta. Tolonen 2003, s. 45 huomauttaa, että oikeusjärjestyksen säännöistä tiedetään niiden voimaantulo ja voimassaolo yksiselitteisesti. Oikeusperiaatteet sen sijaan kehittyvät hitaasti ja niiden sisällöstä voidaan formuloida eri vivahtein.
Oikeuslähteet voidaan jakaa vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin. Aarnion 1989, s. 220 mukaan *vahvasti velvoittava* oikeuslähde tarkoittaa, että oikeuslähteen syrjäyttämisestä seuraa lainsoveltajalle sanktio. Vahvasti velvoittavan oikeuslähteen soveltaminen on siis pakollista. *Oikeudenkäymiskaaren* (4/1734) 1:11 mukaan vahvasti velvoittaviin lähteisiin kuuluvat Suomessa laki ja maantapa. *Heikosti velvoittavan* oikeuslähteen sivuuttamisesta ei seuraa virkavirhesanktiota. Todennäköistä kuitenkin on, että tuomarin päätös muuttuu ylemmissä oikeusasteissa. Lainsäätäjän tarkoitus (*ratio legis*) ja tuomioistuinratkaisut kuuluvat heikosti velvoittavien oikeuslähteiden ryhmään. Aarnio 1989, s. 226–227 toteaa, että lainsäätäjän tarkoitusta voidaan selvittää lainvalmistelutöiden avulla. Lainvalmistelutöihin kuuluvat esimerkiksi erilaiset komiteamietinnöt, hallituksen esitykset eduskunnalle sekä eduskunnan valiokuntien mietinnöt. Peukalosääntönä voidaan pitää, että mitä lähempänä jokin aineisto on eduskunnan päätöksentekoa, sitä suurempi relevanssi sillä on tulkittaessa lainsäätäjän tarkoitusta. Valiokuntapöytäkirjoilla on siksi yleensä tärkein rooli tulkinnassa, jos niissä käsitellään tulkinnanvaraiseksi osoittautunutta ongelmaa. Hallituksen esityksillä on merkittävä painoarvo silloin, kun esitystä ei eduskunnassa ole muutettu. Virolainen ja Martikainen 2010, s. 366 huomauttavat, että tuomioistuinratkaisulla viitataan lähinnä ylimpien oikeusasteiden ennakkopäätöksiin. Aarnion 1989, s. 221 mukaan sallittujen oikeuslähteiden sivuuttamisella ei ole ennustettavia seurauksia. *Sallitut oikeuslähteet* vahvistavat argumentaatiota. Sallittuihin oikeuslähteisiin kuuluvat arvot ja arvoasetelmat (moraali), oikeustiede (lainoppi), oikeusvertailevat ja oikeushistorialliset argumentit sekä teleologiset argumentit (reaaliset argumentit). Aarnio 1989, s. 221 huomauttaa, että sallittujen oikeuslähteiden sivuuttamisella ei ole ennustettavia seurauksia. Virolainen ja Martikainen 2010, s. 366 määrittelevät lisäksi *kielletyt* oikeuslähteet, joihin kuuluvat lain ja hyvä tavan vastaiset ratkaisuperusteet sekä avoimesti (puolue)poliittiset näkemykset. Katso myös alaviite 43 vieraan maan oikeuden asema oikeuslähteenä. Virolainen ja Martikainen 2010, s. 365 huomauttavat, että oikeuslähteistä voidaan puhua myös suppeassa ja laajassa merkityksessä. *Suppeassa* merkityksessä oikeuslähteisiin kuuluvat ainoastaan virallislähteet eli laki, maantapa, lainsäätäjän tarkoitus ja tuomioistuinratkaisut. *Laajassa* merkityksessä oikeuslähteisiin lasketaan virallislähteiden kuuluviksi myös oikeusvertailevat ja oikeushistorialliset argumentit, oikeustiede ja teleologiset perusteet sekä moraaliset näkökohdat.

[32] On kuitenkin huomattava, että tämä luku ei kata kaikkia tietosuojan kannalta merkityksellisiä sopimuksia. Esimerkiksi kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen

Tutkielman 7 luku käsittelee EU:n yleistä tietosuoja-asetusta erityisesti tietoturvanäkökulmasta. Käytännössä tarkastelun painopisteenä on tietosuoja-asetuksen 2 jakso tietoturvallisuudesta, joka sisältää 30 artiklan käsittelyn turvallisuudesta, 31 artiklan henkilötietojen tietoturvaloukkauksesta ilmoittamisesta valvontaviranomaiselle sekä 32 artiklan henkilötietojen tietoturvaloukkauksesta ilmoittamisesta rekisteröidylle. Suomessa velvollisuus ilmoittaa tietoturvaloukkauksista on aiemmin koskenut ainoastaan telealan yrityksiä. Tietosuoja-asetuksen voimaantulon myötä velvollisuus laajenee muillakin aloilla toimiviin rekisterinpitäjiin. Luvussa keskitytään erityisesti rekisterinpitäjälle asetettavaan velvollisuuteen ilmoittaa henkilötietoihin kohdistuneista tietoturvaloukkauksista valvontaviranomaiselle ja rekisteröidylle.

Ulkomaisesta lainsäädännöstä esitellään luvussa 8 Ruotsin, Norjan ja Yhdysvaltojen tietosuojalainsäädäntöä. Kunkin maan kohdalla on esitelty myös se, miten yksityisyydestä on säädetty maan perustuslaissa. Luvussa esitellään myös, miten rekisterinpitäjiä velvoitetaan ilmoittamaan valvontaviranomaisille ja rekisteröidyille henkilötietoihin kohdistuneista tietoturvaloukkauksista.

Luvussa 9 käsitellään henkilötietojen siirtoa EU:n ulkopuolelle. Tässä luvussa käsitellään erityisesti EU:n tuomioistuimen syksyllä 2015 antamaa merkittävää ratkaisua Yhdysvaltojen kanssa tehtyyn Safe Harbor –järjestelyyn liittyen (ns. Schrems-tapaus). Oikeustapaus on tutkielman kannalta mielenkiintoinen, koska Yhdysvaltojen tietosuojalainsäädäntö on yksi maisteritutkielman oikeusvertailulukuun valituista maista.

Tutkielman johtopäätökset on koottu lukuun 10.

(30.1.1976/108, SopS8) III osan 17 artiklan mukaan: ”Kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä.” Jokaisella on myös ”oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan.”
Myös YK:n yleismaailmallinen ihmisoikeuksien julistuksen 12 artiklassa turvataan oikeus yksityiselämän suojaan, kunnian suojaan, kotirauhaan sekä luottamukselliseen viestintään.

2 TUTKIMUSAIHEEN ESITTELY

2.1 Tutkimuksen kohde ja metodi

Tässä maisteritutkielmassa tutkimuskohteena on tietoturvallisuus henkilötietojen käsittelyssä. Tutkielman tavoitteena on määritellä tietoturvallisuuteen liittyviä keskeisiä käsitteitä sekä kuvata niitä käytännön toimenpiteitä, joilla tietoturvallisuutta organisaatioissa toteutetaan. Tutkielmassa käsitellään erityisesti sitä, miten Euroopan unionin tuleva tietosuoja-asetus tulee muuttamaan rekisterinpitäjälle asetettuja tietoturvallisuuteen liittyviä velvoitteita ja minkälaisia tulkinnallisia ongelmia tietosuoja-asetusehdotukseen mahdollisesti liittyy. Tutkielman ydin käsittelee komission tietosuoja-asetusehdotuksen 30–32 §:ä, jotka säätelevät rekisterinpitäjälle ja henkilötietojen käsittelijälle asetettuja tieto-turvallisuusvelvoitteista.

Maisteritutkielma on tutkimusotteeltaan lähinnä oikeusdogmaattinen. *Oikeusdogmatiikka* eli lainoppi tutkii voimassa olevan lain sisältöä. Oikeusdogmatiikan tehtävänä on oikeusnormien tulkinta[33] ja niiden systematisointi.[34] Lainopin systematisointityössä jäsennetään oikeudenalojen käsitteitä, oikeusperiaatteita ja teoreettisia rakennelmia.[35] Nykyisin lainoppi tutkii oikeusääntöjen ohella myös oikeusperiaatteita. Lainopin tehtävänä onkin oikeusperiaatteiden punninta ja niiden yhteensovittaminen.[36] Tiivistäen voidaan todeta, että lainoppi tutkii sitä, mikä on voimassa olevaa oikeutta ja lisäksi sitä, mikä merkitys laista ja muista oikeuslähteistä löytyvällä materiaalilla on.[37] Lainoppia voidaan luonnehtia tulkintatieteeksi, joka tutkii oikeudellisia tekstejä.[38] Suomen liitty-

[33] Aarnio 1999, s. 334 on selittänyt tulkinnan käsitettä seuraavasti: usein normin ilmaisevat tekstit ovat moniselitteisiä ja sallivat useita merkityssisältöjä. Merkityksen täsmentämistä kutsutaan oikeussäännösten tulkinnaksi. Aarnio 1997, s. 37 mukaan tätä oikeusjärjestyksen sisällön selvittämistä voidaan pitää lainopin *praktisena* ulottuvuutena. Vastaavasti oikeussäännösten systematisointi kuuluu lainopin *teoreettiseen* ulottuvuuteen.

[34] Aarnio 1989, s. 48. Aarnion 1989, s. 288 mukaan oikeussäännösten systematisointi luo ja kehittää sitä käsitejärjestelmää, jonka varaan koko oikeudellinen ajattelu rakentuu. Aarnio 2011, s. 12 toteaa, että käsitettä ”metodi” ei yleensä täsmennetä. Aarnio jatkaa, että lainopin kohteeksi määritellään oikeusnormi ja tehtäväksi normin sisällön selvittäminen. Ydinkysymys on, millä metodilla normin sisällöstä saadaan mahdollisimman suuri varmuus. Siltalan 2003, s. 788 mukaan *oikeudellinen systematisointi* merkitsee voimassa olevan oikeuden sääntöjen keskinäisten suhteiden määrittämistä.

[35] Hirvonen 2011, s. 25.

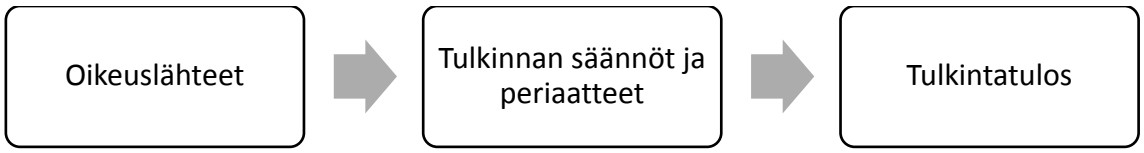
[36] Hirvonen 2011, s. 24. Hirvonen 2011, s. 25 huomauttaa, että ”oikeusperiaatteiden punninta ja tasapainottaminen kuuluvat ensisijaisesti käytännölliseen lainoppiin.” Katso myös alaviite 33 lainopin praktisesta ja teoreettisesta ulottuvuudesta. Tolosen 2003, s. 39–40 mukaan oikeusperiaatteet ovat etupäässä oikeudenalakohtaisia ja niiden merkitys vaihtelee oikeudenaloittain.

[37] Hirvonen 2011, s. 23. Katso oikeuslähteistä tarkemmin alaviitteessä 31.

[38] Hirvonen 2011, s. 36. Hirvosen 2011, s. 37 mukaan oikeusdogmatiikka tuottaa oikeusnormin merkityssisällön tulkinnan menetelmillä.

minen Euroopan Yhteisöihin ja myöhemmin Euroopan Unioniin on muuttanut suomalaista käsitystä voimassa olevasta oikeudesta ja vaikuttanut myös oikeudellisen tulkinnan perusteisiin.[39]

Lainopin tutkimusmenetelmillä tarkoitetaan niitä työkaluja, joita käytetään siirryttäessä oikeuslähteistä ja oikeustapauksen tosiasiakuvauksesta tulkintakannanottoon.[40] Näihin menetelmiin kuuluvat tulkintaperiaatteet[41], ratkaisukäytännöt[42], oikeuslähdeoppi[43] ja periaatteiden etusijajärjestys.[44] Kuva 1 esittää oikeuslähteiden, tulkintasääntöjen ja tulkintatuloksen välistä suhdetta.



Kuva 1. Siirtyminen oikeuslähteistä tulkintatulokseen (Mukaillen Aarnio 1989, s. 194).

Lainopin puitteissa on tavallista verrata kotimaista oikeusjärjestystä, sen normeja ja käytäntöjä, muiden maiden oikeusjärjestyksiin.[45] Tässä maisteritutkielmassa esitellään ja vertaillaan Ruotsin, Norjan ja Yhdysvaltojen tietosuojalainsäädäntöä. Näistä kolmesta Ruotsi on Euroopan unionin jäsenvaltio ja kiinnostava vertailukohde siitä syystä, että henkilötietojen käsittelyä säätelevä normisto perustuu samaan direktiiviin kuin Suomen henkilötietolaki. Norja ei ole EU:n jäsenvaltio ja toimiikin tässä yhteydessä esimerkkinä siitä, miten eurooppalaisessa ei-jäsenvaltiossa on säädetty tietosuojasta. Yhdysvaltojen tietosuojalainsäädäntö poikkeaa huomattavasti eurooppalaisesta tietosuojan sääntelystä. Tutkielmassa Yhdysvaltojen tietosuojalainsäädäntöä verrataan eurooppalaiseen tietosuojalainsäädäntöön. Kiinnostavaa tietoturvallisuuteen liittyen on se, että Yhdysval-

[39] Timonen 1998, s.23 huomauttaa, että unioninjäsenyyden vaikutus suomalaiseen laintulkintaan näkyy esim. siinä, että lainsäädännön ristiriitatilanteita koskeva pääsääntö on ey-oikeuden ensisijaisuus ja muut säännöt ovat sille alisteisia.
[40] Hirvonen 2011, s. 38.
[41] Hirvosen 2011, s. 38–40 mukaan tulkintaa määrittäviä periaatteita ovat: 1) sanamuodon mukainen tulkinta, 2) systemaattinen tulkinta, 3) historiallinen tulkinta, 4) vertaileva tulkinta, 5) supistava ja laajentava tulkinta, 6) analoginen tulkinta, 7) teleologinen tulkinta ja 8) arvoperusteinen tulkinta.
[42] Ratkaisunormit ovat Hirvosen 2011, s. 40–41 mukaan menetelmänormeja, joita käytetään tehtäessä valintoja keskenään kilpailevien normien välillä.
[43] Katso oikeuslähdeopista tarkemmin alaviitteessä 31. Hirvonen 2011, s. 41 huomauttaa, että oikeuslähteet ovat perusteita, joista tulkinnan on lähdettävä liikkeelle. Siltalan 2003, s. 789 mukaan konfliktinratkaisunormeja ovat esim. *lex superior derogat legi inferiori* (normihierarkkisesti ylempi säädös syrjäyttää normihierarkkisesti alemman säädöksen); *lex posterior derogat legi priori* (myöhempi säädös syrjäyttää aikaisemman säädöksen) ja *lex specialis derogat legi generali* (erityislaki syrjäyttää yleislain).
[44] Hirvonen 2011, s. 45. Hirvonen 2011, s. 40 huomauttaa, että eri tulkintamenetelmät johtava usein erilaisiin tulkintatuloksiin. Lainoppineen on tiedettävä tulkintanormien etusijajärjestys. Esimerkiksi EU-oikeudessa korostetaan teleologista tulkintaa ja rikosoikeudessa sanamuodonmukaista tulkintaa.
[45] Hirvonen 2011, s. 26.

loissa useimpien osavaltioiden lainsäädäntö vaatii jo nyt tietoturvaloukkauksista ilmoittamista rekisteröidylle. Euroopan unioni tulee tietosuoja-asetuksen myötä säätämään vastaavanlaisesta velvollisuudesta Euroopassa. Maisteritutkielman lukua 8 voidaan luonnehtia *oikeusvertailevaksi*.[46]

Materiaalina tutkielman teossa on käytetty voimassa olevaa lainsäädäntöä ja lainvalmisteluaineistoa täydennettynä oikeuskirjallisuudella ja teknisillä standardeilla.

2.2 Tutkimusalasta

Tutkimuksen aihe kuuluu *oikeusinformatiikan* alueelle. Oikeusinformatiikka tutkii oikeuden ja tietotekniikan sekä oikeuden ja informaation välisiä suhteita. Oikeusinformatiikan tutkimuskohteena on lisäksi näiden suhteiden yhteydessä ilmenevät oikeudelliset sääntely- ja tulkintakysymykset.[47] Oikeusinformatiikka kuuluu *oikeuden yleistieteisiin*,[48] joita kutsutaan myös oikeuden monitieteiksi.[49]

Saarenpää luonnehtii oikeusinformatiikkaa muutosten oikeustieteeksi. Oikeusinformatiikka on vielä nykyäänkin melko uusi tiede. Oikeusinformatiikkaa voidaan myös kuvailla uudehkoksi oikeudenalaksi, vaikkakin sen historia ulottuu jo yli 60 vuoden taakse. Oikeusinformatiikan kehitysvaiheet liittyvät kiinteästi yhteiskunnan ja teknologian muutoksiin.[50]

Henkilötietojen suoja on osa *persoonallisuusoikeutta*, joka kuuluu siviilioikeuteen. Tarkastelun kohteena on tällöin henkilön identiteetti ja sen suoja käsiteltäessä henkilötietoja. Tietosuojalainsäädäntö järjestää henkilötietojen suojaa ja on yksi vakiintuneimmista oikeusinformatiikan tutkimusaiheista. Tietosuojalainsäädännön sääntelyn ja tulkinnan

[46] Aarnio 1989, s. 235-236 toteaa, että oikeusvertailevalla aineistolla on merkitystä sekä lainsäädännössä, lainkäytössä että oikeusdogmatiikassa. Vieraan maan oikeuden asema oikeuslähteenä vaihtelee. Sallittuna oikeuslähteenä voidaan käyttää vieraan maan lainopillisia tulkintoja ja lainkäyttöratkaisuja silloin, kun mailla on *yhteistä* lainsäädäntöä ja samanlainen tulkintatraditio. Jos vieraan maan lainsäädäntö on samanlaista, mutta ei kuitenkaan yhteistä, voidaan ajatella, että vieraan lain perusteluissa oleva kanta ilmaisee Suomen oikeuden ymmärtämiselle merkityksellisen *lainsäädäntöperiaatteen.* Vieraan maan ratkaisuilla voi olla *vihjearvoa*, vaikka lainsäädäntöperiaate tai tulkintaratkaisu ei ole siirrettävissä Suomeen. Tällöin tulkintaratkaisut voivat antaa viitteitä siitä, minkälaiset tulkinnat ovat mahdollisia ja mitä ongelmia tulkintaan voi liittyä.

[47] Saarenpää 2016, s. 67.

[48] Saarenpää 2016, s. 77. Saarenpää 2016, s. 129 mukaan oikeuskirjallisuudessa on pohdittu kysymystä oikeusinformatiikalle tunnusomaisesta oikeusperiaatteesta. Oikeusinformatiikan sektoreilla on omat periaatteensa, mutta ainoastaan oikeusinformatiikalle ominaista oikeusperiaatetta ei ole löydettävissä. Tässä maisteritutkielmassa esitellään lyhyesti tietosuojaan liittyvät periaatteet (katso kappale 4.1).

[49] Hirvonen 2011, s. 28.

[50] Saarenpää 2016, s. 74.

haasteet lisääntyvät teknologian kehityksen myötä.[51] Tämä maisteritutkielma käsittelee yksityisyyteen ja tietosuojaan liittyviä teemoja ja tutkimus paikantuukin siten *materiaalisen persoonallisuusoikeuden* alalle.[52]

Saarenpää huomauttaa, että oikeusinformatiikka liittyy yhteiskunnan muutokseen palveluyhteiskunnasta tietotekniikkaa hyödyntävään informaatioyhteiskuntaan ja myöhemmin edelleen digitalisoituneeseen verkkoyhteiskuntaan.[53]

Oikeusinformatiikka vaikuttaa keskeisesti muuttuvaan oikeuskulttuuriin, joka koostuu lainsäädännöstä ja sen soveltamiskoneistosta sekä oikeusoloista. Lainsäädännön informatiivisuuden vaatimus on oikeuskulttuurin kannalta merkittävä verkkoyhteiskunnan ilmiö. Lähtökohtana on periaate, jonka mukaan kansalaisten on tunnettava laki.[54] Nykyisin voimassa olevat säädökset ovat verkossa kenen tahansa saatavilla, ja siksi onkin aiheellista kysyä, miltä informatiivisuuden vaatimuksen täyttävän lakitekstin tulisi näyttää.[55]

Oikeusinformatiikalla on monia siteitä muihin tieteisiin ja erityisesti informaatiotieteisiin.[56] Välttämättömiä yhteyksiä oikeusinformatiikalla on myös tietotekniikkaan, tietojenkäsittelyyn ja viestintätieteisiin. Oikeustieteen sisällä tieteidenvälisyys merkitsee tutkimusta ja opetusta, joka ylittää perinteiset systematiikan rajat.[57] Tieteellinen yleissivistys onkin yksi oikeusinformatiikan tunnusmerkeistä.[58]

---

[51] Saarenpää 2016, s. 75–76..

[52] Saarenpään 1996, s. 125 mukaan muita keskeisiä *materiaalisen persoonallisuusoikeuden* tutkimusteemoja ovat tasa-arvo, potilasoikeus ja holhous. Yhteistä näille tutkimusaiheille on ihmisen itsemääräämisoikeutta muotoava yksityisoikeudellinen sääntely. Materiaalisen persoonallisuusoikeuden lähtökohtana on käsitys ihmisen itsemääräämisoikeuden laajuudesta ja sen suojaamisesta yhteiskunnassa. Materiaalinen persoonallisuusoikeus tutkii niitä vapauksia, oikeuksia ja erilaisia yksityisoikeudellisia suojasäännöksiä, jotka koskevat meitä yksilöinä yhteiskunnassa.
Muodollinen persoonallisuusoikeus tutkii ensisijassa oikeussubjekteja ja niiden syntyä, olemassaoloa tunnistamista ja lakkaamista sekä suhdetta muihin oikeussubjekteihin. Muodollinen persoonallisuusoikeus tutkii esim. yksilöiden tunnistamista ja erottelua toisistaan oikeussuhteiden ja valvonnan näkökulmasta.

[53] Saarenpää 2016, s. 79.

[54] Ts. *Ignorantia iuris nocet* (latinaa), joka tarkoittaa, että jos ei tunne lakia, saa kantaa seuraamukset toimiessaan lainvastaisesti.

[55] Saarenpää 2016, s. 84.

[56] Saarenpää 2016, s. 85.

[57] Saarenpää 2016, s. 84. Saarenpää 1999 s. 714 toteaa, että oikeusinformatiikka on oikeustieteen sisällä pitkälti osa oikeusteoriaa, *mutta sillä on liittymiä useille materiaalisen oikeuden aloille.*

[58] Saarenpää 2016, s. 73.

Saarenpään mukaan myös kansainvälisyys on yksi oikeusinformatiikkaa luonnehtivista tunnusmerkeistä.[59] Perinteisesti oikeustiedettä pidetään pääosin kansallisena tieteenä.[60]

Tässä maisteritutkielmassa tarkastellaan EU:n tulevaa tietosuoja-asetusta ja sen myötä tutkielmassa on *eurooppaoikeudellinen* ulottuvuus.

[59] Saarenpää 2016, s. 73.
[60] Saarenpää 2016, s. 86.

3 KESKEISET KÄSITTEET

Yksityisyydelle eli oikeudelle olla yksin[61] ei ole löydetty kansainvälisessä oikeuskirjallisuudessa yleispätevää määritelmää.[62] Itsemääräämisoikeuden rajoissa jokaisella on pääsääntöisesti oikeus olla yksin suhteessa johonkin asiaan, organisaatioihin tai henkilöihin.[63] Oikeusinformatiikan ja persoonallisuusoikeuden näkökulmasta yksityisyyden katsotaan sisältävän yksityiselämän suojan, henkilötietojen suojan ja luottamuksellisen viestin suojan.[64] Yksityisyyden merkitys yhteiskunnassa kasvaa yksilön itsemääräämisoikeuden voimistuessa. Vastaavasti yksityisyyden loukkaamisen riskit kasvavat teknologioiden kehittymisen ja tietotekniikan käytön yleistymisen myötä.[65]

Yksilön oikeus yksityiselämäänsä viranomaisten tai muiden ulkopuolisten mielivaltaista tai aiheetonta puuttumista vastaan on yksityiselämän suojan lähtökohta[66]. *Yksityiselämään* kuuluvat muun muassa yksilön oikeus määrätä itsestään sekä oikeus vapaasti solmia ja ylläpitää suhteita muihin ihmisiin ja ympäristöön. Yksityisyys voidaan ymmärtää yksityiselämän käsitettä laajempana. Yksityisyyteen kuuluvat myös yksilöä läheisesti koskevat tiedot sekä henkilötietojen suoja tietojen käsittelyssä. Tavallisesti yksityisyyteen lasketaan lisäksi oikeus oleskella tietyllä alueella tarvitsematta sietää ulkopuolisten läheisyyttä, katselua, kuuntelua tai häirintää.[67]

Henkilötiedot[68] tarkoittavat henkilötietolain 3 §:n 1 kohdan mukaan ”luonnollista henkilöä taikka hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, jotka voidaan tunnistaa häntä tai hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.” Henkilötietoja tarvitaan esimerkiksi väestön hallinnointiin, hyvinvointipalvelujen tarjoamiseen ja kaupallisiin tarkoituksiin. Yhteiskunnan palvelujen käyttäminen ja toiminta markkinoilla edellyttävät, että yksilö luopuu osittain yksityisyydes-

[61] Saarenpää 2015, s. 313.
[62] Korhonen 2005, s. 21.
[63] Saarenpää 2015, s. 315.
[64] Saarenpää 2015, s. 314.
[65] Saarenpää 2015, s. 314. Saarenpää huomauttaa, että nykyisin henkilötietojen suoja on oma perusoikeutensa.
[66] Hirvelä & Heikkilä 2013, s. 361 EIT:n oikeuskäytännössä yksityiselämä on usein yhteydessä muihin suojan kohteisiin eli perhe-elämään, kotiin ja kirjeenvaihtoon.
[67] HE 184/1999 vp: kohta 2.1., ensimmäinen kappale.
Katso myös PeVL 25/1998 vp–HE 96/1996, s. 2: perustuslakivaliokunta kyseenalaistaa henkilötietolain yksityisyyden suojaa koskevan käsitteen, jota perustuslakivaliokunta pitää liian laajana.
[68] Tietosuoja-asetusehdotus määrittelee erikseen 4 artiklan 1 kohdassa ”rekisteröidyn” ja 2 kohdassa ”henkilötiedon.” Yleisnäkemyksessä tietosuoja-asetuksesta henkilötietojen käsite on kuvattu 4 artiklan 1 kohdassa, joka sisältää myös ”rekisteröidyn” määritelmän.

tään.[69] Henkilötiedon käsite tulkitaan laajasti: olennaista on, että henkilö pystytään näistä tiedoista tunnistamaan.[70] Henkilötiedot voivat olla myös virheellisiä eli niiden ei tarvitse olla varmennettuja tai tosia.[71] Henkilötietojen oikeudellinen määrittely on erilainen EU:ssa ja Yhdysvalloissa. Kansainväliset yritykset joutuvat tekemään monimutkaisia päätöksiä suunnitellessaan ohjelmistoja, palveluita tai tuotteita käytettäväksi sekä EU:n alueella että Yhdysvalloissa.[72] Henkilötiedot käsittävät kaikenlaiset henkilöä, tämän ominaisuuksia tai elinolosuhteita kuvaavat merkinnät, jotka voidaan tunnistaa tiettyä luonnollista henkilöä, hänen perhettään tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi.[73]

Henkilötietojen tietoturvaloukkaus on määritelty tietosuoja-asetuksen 4 artiklan 9 kohdassa. Henkilötietojen tietoturvaloukkaus tarkoittaa sen mukaan tietoturvaloukkausta, jonka seurauksena on siirrettyjen, tallennettujen tai muuten käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen tai saanti.[74]

On yleistä ulkoistaa erilaisia henkilötietojen käsittelytehtäviä palveluntarjoajille.[75] Nämä palveluntarjoajat ovat HetiL:n 3 §:n 6 kohdan mukaisia rekisterinpitäjän lukuun henkilötietoja käsitteleviä tahoja.[76] *Henkilötietojen käsittelijä* on rekisterinpitäjän palveluksessa.[77]

---

[69] Neuvonen 2014, s. 60.
[70] Saarenpää 2015, s. 326.
[71] Pitkänen et al. 2013, s. 42 mukaan tämä ilmenee henkilötietolain säännöksistä (26-29§), joissa säädetään rekisteröidyn tarkastusoikeudesta sekä virheellisten, puutteellisten tai vanhentuneiden tietojen oikaisemisesta ja täydentämisestä.
[72] Schwartz & Solove 2014, s. 902.
[73] HE 96/1998 vp.1 luku Yleiset säännökset, 3 § Määritelmät, Henkilötiedot. lain perustelujen mukaan muotoilu "... henkilön ominaisuuksia tai elinolosuhteita kuvaavia *merkintöjä*" ilmaistaan se, että henkilötietoja ovat jollekin alustalle talletetut tiedot. Sillä, millä keinoin (käsin, koneellisesti, optisesti, sähköisesti, magnetoimalla) tai mille alustalle tieto on talletettu, ei henkilötiedon käsitteen kannalta ole merkitystä.
[74] Kolmikantaneuvotteluissa (katso kappale 7.1) sovittu määritelmä, joka ei ole oikeudellisesti sitova.
[75] WP 169 lausunnon 1/2010, s. 27-31mukaan rekisterinpitäjän ja tiedon käsittelijän käsitteillä on keskeinen rooli direktiivin 95/46/EC soveltamisessa, sillä ne määrittävät, kenen vastuulla tietosuojasäädännön noudattaminen on. Saatavissa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_fi.pdf (Katsottu 23.11.2015).
[76] Pitkänen et al. 2013, s. 57.
Henkilötietodirektiivin 2 artiklan e kohdan mukaan henkilötietojen käsittelijä on luonnollinen tai oikeushenkilö, julkinen viranomainen, virasto tai muu toimielin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Henkilötietodirektiivin määritelmä poikkeaa henkilötietolain määritelmästä, sillä henkilötietodirektiivissä henkilötietojen käsittelijänä pidetään myös sitä tahoa, joka HeTiL:ssa käsitetään henkilötietoja rekisterinpitäjän tai henkilötietojen käsittelijän lukuun käsittelevänä.
[77] HE 96/1998 vp, s. 36. Henkilötietojen käsittelijä on tietosuoja-asetusehdotuksen 4 artiklan 6 kohdan mukaan luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Rekisteröity on HetiL:n 3 § 5 kohdan mukaan henkilö, jota henkilötieto koskee.[78] Esimerkiksi yrityksen henkilötietojärjestelmään kuuluva työntekijä, sähköisessä potilasasiakirjassa mainittu potilas ja luottotiedossa mainittu asiakas voivat olla rekisteröityjä. Rekisteröidyn ei tarvitse olla suoraan nimeltä tunnistettavissa. Luonnollinen henkilö katsotaan rekisteröidyksi myös, kun hänet henkilötietoihin liitettynä voidaan tunnistaa epäsuorasti esim. käyttäjätunnuksen tai saatavilla olevien ominaisuuksien kautta.[79] Henkilötietolaissa käsite ”rekisteröity” liittyy yleisesti kaikkiin henkilöihin, joita henkilötiedot koskevat, vaikka tiedot eivät kuuluisikaan rekisteriin. Henkilötietojen kohteena oleva henkilö on rekisteröity, vaikka hänen henkilötietonsa eivät olisikaan rekisterissä.[80] Tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan rekisteröity on luonnollinen henkilö, joka on tunnistettu tai tunnistettavissa[81] suoraan tai epäsuorasti erityisesti tunnistetietojen perusteella. Tunnistetietoja ovat tietosuoja-asetuksen mukaan esim. henkilönumero, nimi, sijaintitieto, verkkotunnistetieto tai yksi tai useampi rekisteröidylle tunnusomainen fyysinen, fysiologinen, geneettinen, psyykkinen, taloudellinen, kulttuurinen tai sosiaalinen tekijä.[82]

Tietosuoja-asetuksen johdanto-osan 24 kohta rajoittaa epäsuorasti *tunnistettavissa oleva* -käsitettä, sillä verkkopalveluiden käyttäjät voidaan yhdistää heidän käyttämiensä laitteiden, sovellusten, työkalujen ja protokollien internet-tunnisteisiin, kuten IP-osoitteisiin[83] tai evästeisiin. Tällaisissa tilanteissa on mahdollista, että käyttäjästä jää jälkiä, joita voidaan käyttää yhdessä ainutlaatuisten tunnisteiden ja muiden palvelimille toimitettujen tietojen avulla käyttäjien profilointiin ja tunnistamiseen. Tästä seuraa, että tunnistenumeroita, sijaintitietoja, internet-tunnisteita tai muita erityistekijöitä ei sinänsä tarvitse pitää henkilötietoina kaikissa tilanteissa. Tällaisessa tilanteessa tietosuoja-asetus

[78] HE 96/1998 vp, s. 36.
[79] SFS-ISO/IEC 29100, s. 14.
[80] Pitkänen et al. 2013, s. 59. Tämä kielellinen erikoisuus johtuu siitä, että käsitteistö pyrittiin pitämään samana, kun siirryttiin henkilörekisterilaista soveltamisalaltaan laajempaan henkilötietolakiin.
[81] Englanniksi ”who can be identified, directly or indirectly.” Direktiivi artikla 2 a kohta käyttää tässä yhteydessä käsitettä “identifiable” eli ”tunnistettavissa oleva”. Schwartz & Solove 2014, s. 884 toteavat tietosuoja-asetukseen tuodun käsitteen vastaavan sisällöltään direktiivin käsitettä.
[82] Kolmikantaneuvotteluissa (katso kappale 7.1) sovittu määritelmä, joka ei ole oikeudellisesti sitova.. Schwartz & Solova 2014, s. 886 toteavat, että uusien kategorioiden (sijaintitiedot, internet-tunnisteet ja ”geneettiset” tekijät) kautta modernisoidaan rekisteröidyn määritelmää verrattuna henkilötietodirektiivin määritelmään.
[83] Helopuro et al. 2009, s. 291 ovat taustoittaneet henkilötietolain suhdetta staattisiin ja dynaamisiin IP-osoitteisiin. Staattinen IP-osoite on muuttumaton ja sisällytettävissä luetteloihin, jolloin siitä muodostuu luettelotietona henkilötieto henkilötietolain tarkoittamassa merkityksessä. Dynaamista IP-osoitetta ei voi luetteloida, eikä dynaaminen IP-osoite ole yhdistettävissä luonnolliseen henkilöön henkilötietolain tarkoittamassa merkityksessä. Oikeudellisesti dynaamisessa IP-osoitteessa kyse ei ole henkilötiedosta.

jättää liikkumavaraa asiayhteydestä riippuvalle analyysille siitä, onko kyseessä henkilötieto.[84]

Henkilötietojen käsittely[85] tarkoittaa HetiL:n 3 §:n 2 kohdan mukaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä. HetiL:n määritelmä on laaja ja käsittää kaikenlaiset henkilötietoihin kohdistuvat toimenpiteet.[86] Henkilötietojen luovuttaminen ja siirtäminen ovat käsitteinä osittain päällekkäisiä. Siirtämisessä rekisterinpidon vastuu jää siirtäjälle ja siirron saaja toimii rekisterinpitäjän lukuun. Luovuttamisessa tulee tietojen vastaanottajasta rekisterinpitäjä.[87]

Henkilörekisterillä voi olla yksi tai useampi *rekisterinpitäjä*.[88] Rekisterinpitäjällä[89] tarkoitetaan HetiL:n 3 §:n 4 kohdan mukaan 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. Lailla säädetyllä rekisterinpidolla viitataan lähinnä rekistereihin, joita viranomaiset ylläpitävät.[90] Rekisterinpitäjä voi olla esimerkiksi oikeushenkilö, joka ylläpitää henkilörekisteriä asiakkaistaan tai työntekijöistään. Myös luonnollinen henkilö, joka ylläpitää henkilörekisteriä harrastustoimintaansa varten, on rekisterinpitäjä.[91] Henkilötietolain systematiikan mukaan henkilörekisterillä on oltava rekisterinpitäjä. Rekisterinpitäjä määrää re-

[84] Schwartz & Solove 2014, s. 886. Schwartz & Solove 2014, s. 887 toteavat, että tietosuoja-asetusehdotuksen henkilötieto –käsite on hyvin laaja ja tuskin mikään jää säätelemättä EU:n yksityisyyttä koskevan lainsäädännön alueella. Tähän liittyy kuitenkin se ongelma, että säätely velvoittaa raskaasti kaikenlaisia henkilötietoja käsitteleviä toimijoita riippumatta yksilöiden yksityisyyteen kohdistuvasta riskitasosta.

[85] EU:n tuomioistuin on käsitellyt direktiivin 95/46/EY mukaista henkilötietojen käsittely –käsitteen tulkintaa ennakkoratkaisupyynnössä C-101/01–Lindqvist. Tuomion 27-kohdan mukaan: *sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumeronsa tai antamalla tietoja heidän työsuhteestaan ja harrastuksistaan, on pidettävä direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä.*

[86] Saarenpää 2015, s. 326 huomauttaa, että henkilöön liittyvää puhetta säännellään salassapitoa, kunnianloukkausta ja yksityiselämän suojaa joukkoviestinnässä koskevan lainsäädännön kautta. Pelkkä puhe jostakin henkilöstä ei näet ole henkilötietojen käsittelyä.

[87] Pitkänen et al. 2013, s. 55.

[88] Pitkänen et al. 2013, s. 55.

[89] SFS-ISO/IEC 29100, s. 10 tiivistää rekisterinpitäjän määritelmän seuraavasti: Rekisterinpitäjä on *(yksi tai useampi) tietosuojatoimija, joka määrittelee henkilötietojen käsittelemisen tarkoituksen sekä niiden käsittelyn keinot ja joka ei ole luonnollinen henkilö, joka käyttää tietoja henkilökohtaisiin tarkoituksiinsa.*

[90] Pitkänen et al. 2013, s. 57. Esimerkiksi *laki Oikeusrekisterikeskuksesta (625/2012)* 1 § 1 kohta määrittelee oikeusrekisterikeskuksen tehtäväksi ”toimia oikeusministeriön hallinnonalan tietojärjestelmien ja rekisterien rekisterinpitäjänä.”

[91] Pitkänen et al. 2013, s. 55.

kisterin käytöstä ja on vastuussa henkilötietojen käsittelystä.[92] Rekisterinpitäjän kannalta olennaista on, että henkilötietojenkäsittelyprosessit suunnitellaan jo ennen kuin henkilötietoja aletaan käsitellä.[93]

Tietosuojan ja henkilötietojen suojan käsitteitä käytetään usein synonyymeinä. *Henkilötietojen suoja* on oikeudellinen peruskäsite. Oikeuslingvistisestä ja lakiteknisestä näkökulmasta tarkasteltuna henkilötietojen suoja on tietosuojalainsäädännön kautta toteutettavaa yksilön suojaa. Kansainvälisissä yhteyksissä henkilötietojen suojan oikeudellisesta sääntelystä käytetään vakiintuneesti ilmaisua tietosuoja.[94]

Tietosuojaan[95] sisältyy ihmisten yksityiselämän suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä. Tietosuojaan kuuluu esimerkiksi henkilötietojen suojaaminen henkilöä vahingoittavalta tai valtuudettomalta käytöltä. Myös tietojen luottamuksellisuuden säilyttäminen ja tietojen valtuudettoman saannin estäminen sisältyvät tietosuojaan.[96]

Tietoturvallisuus tarkoittaa hallinnollisia ja teknisiä järjestelyjä, joiden tavoitteena on turvata tiedon eheys, luottamuksellisuus ja käytettävyys.

Hallinnollisia eli *organisatorisia* toimia ovat esimerkiksi henkilöiden tehtävien ja vastuiden määrittelyt, koulutus ja ohjeistus[97] sekä toimintalinjaukset ja valvonta.[98] Organisatorisiin keinoihin kuuluvat käytännössä esimerkiksi käyttöoikeuksien jakaminen työtehtävien mukaan sekä käyttöoikeuksien ja käyttäjätunnusten antamisen yhteydessä annettu ohjaus.[99] Lähtökohtana on, että käyttöoikeudet ovat työtehtävien mukaisia ja ajantasaisia, sillä asiattomiin käyttöoikeuksiin liittyy useita riskejä.[100]

---

[92] Neuvonen 2014, s, 75.
[93] Ylipartanen 2010, s. 32 toteaa, että suunnitteluvelvollisuuden toteuttaminen edellyttää lainsäännösten sisällön ja systematiikan tuntemista.
[94] Saarenpää 2015, s. 325.
[95] Myös Neuvonen 2014, s. 64 toteaa, että käsitteitä henkilötietojen suoja ja tietosuoja käytetään usein synonyymeinä. Neuvonen lisää, että käytännössä tietosuojan vaatimukset voivat koskea myös esim. yritys salaisuuksia. Sekaannus selittyy sillä, että joissakin kielissä käsitteitä kuvataan samalla termillä.
Hyvään tiedonhallintatapaan yhdistettynä tiedon suojaamisella tarkoitetaan HE 30/1998 vp, s. 76 mukaan tiedon saatavuutta ja käyttötarkoituksia koskevien rajoitusten (esim. salassapidon) toteuttamiseksi tarpeellisia toimenpiteitä. Toimenpiteet voivat olla teknisiä tai muita menettelytapoihin liittyviä järjestelyitä.
[96] VAHTI 8/2008, s, 105.
[97] *Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä* (159/2007; 20.5 §) velvoittaa laatimaan työntekijöille kirjalliset ohjeet potilastietojen käsittelystä.
[98] Pitkänen et al. 2013, s. 215.
[99] Andreasson ja Koivisto 2013, s. 122.
[100] Andreasson et al. 2014b, s. 77. Näitä riskejä ovat muun muassa se, että tietoja voidaan tahattomasti tai tahallisesti poistaa, muuttaa tai lisätä. Asiattomat käyttöoikeudet avaavat reittejä tietomurtoihin, joista voi

Teknisiin tietoturvatoimiin kuuluvat esimerkiksi käsittelytapahtumien kirjaaminen[101], käyttöoikeuksien määrittely, pääsyn valvonta laitteille ja järjestelmiin sekä tietojen ja järjestelmien luvattoman käytön esto ja suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta (esim. viruksilta).[102] Tietosuojan näkökulmasta tietoturvallisuudella tarkoitetaan niitä toimenpiteitä, joilla rekisteröidyn yksityisyyden, etujen ja oikeuksien turvaamiseen ja suojaamiseen pyritään.[103] On huomattava, ettei tietototurvallisuus rajoitu henkilötietojen suojaan. Tietoturvallisuus on myös osa siviili- ja erityisesti sopimusoikeuden yleisiä oppeja.[104] Tietoturvallisuus suojaa salaisuuksien ja luottamuksellisuuden lisäksi myös informaation ja tietojärjestelmien hyödynnettävyyttä.[105]

Tiedon *eheydellä* viitataan siihen, että tieto säilyy talletettua tietoa vastaavassa muodossa. Toisin sanoen tiedon eheys tarkoittaa tiedon muodon säilyttämistä niin lainvastaiselta kuin tahattomaltakin[106] muuttamiselta.[107] Eheydellä viitataan myös siihen, että mahdolliset muutokset ovat kirjausketjusta todennettavissa.[108]

Luottamuksellisuus merkitsee, että tietoa voivat lukea tai muokata vain ne, joille tällainen oikeus on etukäteen annettu.[109] Tietoturvallisuudessa luottamuksellisuuden suojaamista eli tietojen suojaamista luvatonta käyttöä ja pääsyä vastaan on perinteisesti koros-

---

seurata laajoja selvitystöitä, taloudellisia vahinkoja ja vahinkoa organisaation maineelle. Teknisesti tietojärjestelmien käyttö voi hidastua, jos tietokantaan on tarpeettomia oikeuksia. VAHTI:n 9/2006, s. 17 mukaan käyttövaltuuksia määriteltäessä käyttäjiä ei tule tarkastella yksilötasolla. Lähtökohtana ovat käyttäjäryhmät, joiden jäsenissä on samanlaiset tietotarpeet ja toimenkuvat.

[101] Katso myös kappale 6.3.2 EIT 17.7.2008, I v. Suomi, jossa käsiteltiin käsittelytapahtumien kirjaamisen puuttumista.

[102] VAHTI 8/2008, s, 109; Pitkänen et al. 2013, s. 215.

[103] Andreasson et al. 2014a, s. 14.

[104] Pöysti 2002, s. 60 mainitsee esimerkkeinä ratkaisut KKO 1992:3 ja KKO 1994:80. Ratkaisuissa viitataan tietoturvallisuuteen liittyviin huolenpitovelvoitteisiin ja riskien jakautumiseen osapuolten välillä käytettäessä tietojärjestelmiä. Råman 2006b, s. 818 huomauttaa, että käytännön toimijat tarkastelevat tietoturvallisuutta osana organisaation, sen palveluiden ja tuotteiden turvallisuutta. Juristi tarkastelee tietoturvallisuutta ensisijaisesti yksilön oikeuksien ja yhteiskunnan toimintojen turvaamisen näkökulmasta.

[105] Pöysti 1999, s. 460.

[106] Järvinen 2002, s. 23 mainitsee esimerkkinä, että eheys voi särkyä tiedonsiirronaikaisen virheen takia tai siksi, että levylle on tullut vika-alue.

[107] HE 30/1998, Yksityiskohtaiset perustelut -kappale, 18 § Hyvä tiedonhallintatapa: 7. Kappale.

[108] VAHTI 8/2008, s. 25. Saman lähteen mukaan eheys tarkoittaa myös tietojen ja tietojärjestelmien ristiriidattomuutta, kattavuutta, ajantasaisuutta, käyttökelpoisuutta ja oikeellisuutta. Pöysti 2002, s. 66 toteaa, että korkeimman oikeuden ratkaisukäytännössä auditoitavuudelle on annettu oikeudellista merkitystä osoitettaessa, onko jotakin seikkaa pidettävä uskottavana epäselvyyden vallitessa. Ratkaisussa KKO 1996:34 oli kyse siitä, oliko tietokoneohjatussa postituksessa sopimusehtojen muuttamista tarkoittanut kirje tullut todennäköisesti lähetetyksi.

[109] Järvinen 2002, s. 22. Miettinen 1999, s. 25 erittelee luottamuksellisuuden suppean ja laajan merkityksen. Suppeassa merkityksessä luottamuksellisuus koskee yksityistä ihmistä, ja kyse on tällöin tietosuojasta. Laajassa merkityksessä luottamuksellisuuteen kuuluu kaikki yrityksen toiminnassaan tarvitsemat tiedot.

tettu.[110] Tietoturvallisuus suppeassa merkityksessä nähdäänkin yksinkertaisesti pelkästään pääsyä rajoittavina tekijöinä kuten salasanoina ja palomuureina.[111]

Käytettävyys tarkoittaa, että tieto, tietojärjestelmä tai palvelu on siihen oikeutetuille saatavilla ja hyödynnettävissä haluttuna aikana ja vaaditulla tavalla.[112] Toisaalta käytettävyys voidaan käsittää käyttökelpoisuudeksi, jolloin käsite viittaa myös tiedon laatuun.[113] On arvioitu, että terveydenhuollon tietojärjestelmien käytettävyyden ja tietojärjestelmäratkaisujen parantaminen säästäisi vuosittain 80 miljoonaa euroa. Terveyskeskuskontekstissa määrä vastaa 400 000 lääkärin vastaanottoaikaa.[114]

Käytettävyys helppokäyttöisyytenä[115] on määrätyissä konteksteissa myös osa tietoturvallisuutta. Käyttäjät voivat luoda uusia toimintamalleja tai toimia suunnitellusta poikkea-

[110] Pöysti 2002, s. 64.
[111] Valo 2012, s. 287.
[112] VAHTI 8/2008, s. 54. Käytettävyys tarkoittaa tässä saatavuutta. Tässä merkityksessä se on kuvattu myös SFS-ISO/IEC 27000 –standardissa (s.12), jonka mukaan (saatavuus) on ominaisuus, joka tarkoittaa kohteen olevan saatavilla ja käyttökelpoinen valtuutetun tahon niin vaatiessa. Miettinen 1999, s. 27 havainnollistaa saatavuuden menetystä esimerkillä: tietojen saatavuus on menetetty silloin, jos yrityksen tietoliikenneverkko tietoisesti tukitaan ylimääräisellä liikenteellä, jolloin yrityksen tietokannat eivät väliaikaisesti ole käytettävissä. Järvisen 2002, s. 24 mukaan tällöin on kyse palvelunestohyökkäyksestä: hyökkääjän tavoite on estää häirinnällään palvelun normaali toiminta. Hyökkääjä ei tällöin pyri murtautumaan (luottamuksellisuus) tai sotkemaan (eheys) mitään. VAHTI määrittelee myös käytettävyyden toisen merkityksen (usability). Käytettävyydellä voidaan tarkoittaa myös sitä, kuinka hyvin järjestelmä, laite, ohjelma tai palvelu soveltuu suunniteltuun tarkoitukseen määrätylle kohderyhmälle. Tämän käsitteen synonyymejä ovat helppokäyttöisyys ja käyttäjäystävällisyys. Standardin SFS-EN ISO 2941-11 mukaan käytettävyyden arvioinnissa otetaan huomioon, miten tuloksekkaasti, tehokkaasti ja tyytyväisenä tuotteen käyttäjät voivat työskennellä. Helppokäyttöisyydestä on säädetty esimerkiksi *laissa sähköisestä asioinnista viranomaistoiminnassa* (13/2003; 5.3 §). HE 17/2002 vp, s. 35 mukaan sähköisten asiointipalveluiden kehittämisessä tulee kiinnittää huomiota palveluiden saatavuuden lisäksi myös esteettömyyteen, kohtuuhintaisuuteen sekä siihen, miten palvelut soveltuvat erilaisten käyttäjien tarpeisiin. Esteettömyydellä viitataan tyypillisesti siihen, että palvelua voivat käyttää myös esim. vammaiset.
[113] HE 30/1998 vp, s. 77.
[114] Käyttäjäystävällisillä tietojärjestelmillä jopa 400 000 lääkärin vastaanottoaikaa lisää. Saatavissa: https://www.vtv.fi/ajankohtaista/tiedotteet/2012/kayttajaystavallisilla_tietojarjestelmilla_jopa_400_000_laakarin_vastaanottoaikaa_lisaa.3546.news. (Katsottu 30.7.2015).
[115] Maisteritutkielman kirjoittaja on toiminut käytettävyysasiantuntijana ja myöhemmin käyttöliittymän suunnittelijana ICT-alan yrityksessä vuodesta 2002 alkaen. Näissä tehtävissä käytettävyys on ymmärrettävissä Voutilaisen väitöstyössään 2009, s. 182 esittelemien määritelmien mukaisesti. Nämä suunnittelutyötä tukevat määritelmät on kuvattu SFS-EN ISO 9241-11 –standardissa sekä Jacob Nielsenin heuristiikoissa. Nielseniä pidetään käytettävyysalan edelläkävijänä tietotekniikan alalla. Standardi SFS-EN ISO 9241-11, s. 6 määrittelee käytettävyys-käsitteen seuraavasti: käytettävyys on *mitta, miten hyvin määrätyt käyttäjät voivat käyttää tuotetta määrätyssä käyttötilanteessa saavuttaakseen määritetyt tavoitteet tuloksellisesti, tehokkaasti ja miellyttävästi*. Nielsen 1993, s. 26 määrittelee käytettävyyden osatekijöiksi opittavuuden, tehokkuuden, muistettavuuden, virheiden (vähäisen) määrän ja tyytyväisyyden. Nielsen 1993, s. 115 on kehittänyt käyttöliittymien arviointia ja suunnittelua varten tarkoitetut Nielsenin heuristiikat. Voutilainen 2009, s. 182 toteaa käytettävyyden käsitteen olevan vakiintunut. ICT-alalla SFS-EN ISO 9241-11 –standardi ja Nielsenin heuristiikat ovatkin yleisesti käytössä.

valla tavalla käyttäessään vaikeasti käytettäviä tietojärjestelmiä. On mahdollista, että näin toimiessaan käyttäjät huonontavat tietoturvaa.[116]

Usein tietoturvaa lasketaan kuuluvaksi myös todennus, vastuullisuus ja kiistämättömyys. *Todennus* tarkoittaa osapuolten ja käyttäjien luotettavaa tunnistamista. Sähköpostissa todentaminen pohjautuu tyypillisesti ainoastaan näkyvään lähettäjäosoitteeseen. Todentamistapana tämä on turvaton, sillä osoite on helppo väärentää. Luotettavaan todentamiseen tarvitaan sähköpostin yhteydessä digitaalinen allekirjoitus.[117] *Vastuullisuus tai vastuutettavuus*[118] merkitsee, että tietojen käyttämisestä ja muuttamisesta jää jälki, jonka avulla on jälkikäteen selvittävissä tietoja käsitelleet henkilöt. *Kiistämättömyys* on todisteiden luomista sen varmistamiseksi, etteivät osapuolet voi kiistää osuuttaan tietojenkäsittelyyn jälkikäteen.[119] Kiistämättömyyden tarve tulee esille esimerkiksi sähköisessä kaupankäynnissä, jossa ostotapahtuman vaiheet tulee voida sitovasti todistaa. Kiistämättömyys edellyttää sitä, että tapahtumat on varustettu aikaleimoilla.[120]

Tietoturvallisuudesta henkilötietojen käsittelyssä säädetään *henkilötietolain* (523/1999) 32 §:ssä. Sen mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.[121] Henkilötietojen suojaaminen on siis rekisterinpitäjän velvollisuus.[122] Henkilötietolain 32 §:n suojaamisvelvoite ja henkilötietolain 5 §:n huolellisuusvelvoite edellyttävät teknisiä ja organisatorisia suojatoimia sekä hyvän tietojenkäsittelytavan noudattamista ja huolellisuutta myös silloin, kun se ei pelkästään taloudellisesti katsottuna olisi kannattavaa.[123] Toteutettaessa tietojen suojaamista on HetiL:n 31.1 §: n mukaan otettava huomioon käytettävissä olevat tekniset

[116] Valo 2012, s. 296. Käyttäjät voivat esimerkiksi tulostaa potilastietoja vaikeakäyttöisestä järjestelmästä työnsä helpottamiseksi, vaikka tarkoitus olisi pitää tiedot sähköisinä tietojen turvallisen säilyttämisen varmistamiseksi.
[117] Järvinen 2002, s. 25.
[118] Pitkänen et al. 2013, s. 216 huomauttavat, että tietosuoja-asetusehdotus korostaa vastuutettavuutta ja tarkastettavuutta, jolloin rekisterinpitäjältä odotetaan aktiivisempaa toimintaa kuin pelkkää lain mukaan toimimista. Rekisterinpitäjän tilivelvollisuudesta on säädetty tietosuoja-asetusehdotuksen 22 artiklassa.
[119] Pitkänen et al. 2013, s. 216.
[120] Järvinen 2002, s. 27. Blanchette 2012 s. 10 huomauttaa, että vaikka kiistämättömyys käsitteenä on (tieto)turvallisuuskirjallisuudessa määritelty tarkasti, se ei ole oikeudellisena käsitteenä vakiintunut. Tuomioistuimilla on paine linjata kiistämättömyyteen liittyvää todistusarvoa, kun yhä enemmän tallenteita tuotetaan, vaihdetaan ja tallennetaan digitaalisessa muodossa.
[121] Suojaamisvelvoitteen voidaan katsoa edellyttävän organisaatiokohtaista lokirekisterin ylläpitoa sekä henkilötietojen käsittelyn lainmukaisuuden seurantaa. (Andreasson et al. 2014a, s. 80).
[122] Pitkänen et al. 2013, s. 213.
[123] Pitkänen et al. 2013, s. 221.

mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta. Arkaluonteisia tietoja sisältävän rekisterin suojaamiseen on kiinnitettävä erityistä huomiota.[124] Arkaluonteiset tiedot on lueteltu HetiL:n 11 §:ssä. Yleistäen voidaan todeta, että tietojen suojaaminen paremmin merkitsee enemmän kustannuksia ja vaivaa verrattuna heikompaan suojaan.[125]

[124] Pitkänen et al. 2013, s. 222.
[125] Valo 2012, s. 287.

4 TIETOSUOJAN PERIAATTEET, STANDARDOINTI JA MUU ITSESÄÄNTELY

4.1 Tietosuojan periaatteet

Henkilötietojen suojan lainsäädännöllisen järjestämisen periaatteet ovat hyvin vakiintuneita, mikä on seurausta kansainvälisestä lainvalmistelusta. Selkeimmin tämä ilmenee nykyisellään Euroopan henkilötietodirektiivistä.[126] Lähtökohtana on kaikenlaisesta henkilötietojen käsittelystä säätäminen tietojen kokoamisesta niiden arkistointiin tai tuhoamiseen asti. Tietosuojalainsäädäntö kattaa koko informaation elinkaaren. Saarenpää on luokitellut tietosuojalainsäädännön periaatteet seuraaviin ryhmiin: (1) yleisiin, kaikkia koskeviin periaatteisiin (2) ensisijaisesti henkilötietojen käsittelijöitä koskeviin sekä (3) ensisijaisesti yksilön oikeuksia koskeviin periaatteisiin.[127]

Yleiset periaatteet käsittävät seuraavat oikeusperiaatteet: lakisääteisyys, yksilön tunnistettavuus, avoimuus, tarpeellisuus, tietoturva, hyvä tietojenkäsittelytapa, automaattisen henkilöarvioinnin rajoittaminen, käytännesäännöt, viranomaiskoneiston olemassaolo ja sanktiojärjestelmä.[128]

Rekisterinpitäjiä koskeviin oikeusperiaatteisiin kuuluvat Saarenpään mukaan tarpeellisuus, suunnitelmallisuus, käyttötarkoitussidonnaisuus, huolellisuusvelvoite, tietoturvallisuus, laatuperiaate, tiedottamisvelvollisuus ja ankara vastuu.[129]

Yksilön kannalta tietosuojalainsäädäntömme perustuu seuraaviin periaatteisiin: suostumuksen[130] ensisijaisuus, arkaluonteisten tietojen sekä henkilötunnuksen erityisasema,

[126] Saarenpää 2015, s. 341.
[127] Saarenpää 2015, s. 342.
[128] Saarenpää 2015, s. 342.
[129] Saarenpää 2015, s. 355.
[130] Euroopan tietosuojatyöryhmä on määritellyt suostumuksen käsitettä lausunnossaan WP 187 s. 2. Sen mukaan suostumus on yksi laillisista perusteista henkilötietojen käsittelyssä. Tärkeästä roolistaan huolimatta se ei kuitenkaan ole aina sopivin peruste. Oikein käytettynä suostumus antaa rekisteröidylle työkalun valvoa henkilötietojensa käsittelyä. Väärin käytettynä valvonnasta tulee kuvitteellista, jolloin se muodostuu sopimattomaksi perusteeksi käsittelylle. Saatavissa: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf (Katsottu 13.7.2015). Tietosuojavaltuutetun kannanotossa (1.7.2010 Dnro 1475/41/2009) viitataan henkilötietolain 32 §:än ja yleiseen ”suostumus ei syrjäytä tarpeellisuusvaatimusta” –tietosuojaperiaatteeseen. Asian käsittelyn tarkoituksen kannalta tarpeettomia tietoja ei ole laillista käsitellä, vaikka siihen olisi asiakkaan suostumus.

tarkastus- ja oikaisuoikeus, markkinarauha, kielto ja vastusoikeus sekä tietossuojaviranomaisten palvelut.[131]

Tietoturvallisuus yleisenä periaatteena on informaatioyhteiskunnan ja nykyisen verkkoyhteiskunnan merkittävimpiä yleisiä tunnusmerkkejä. Perinteisiä tietoturvallisuuden muotoja ovat tekninen ja henkilöstöön liittyvä tietoturvallisuus. Nykyisin näiden rinnalle on noussut myös oikeudellinen tietoturvallisuus.

HetiL:n 32.1 §:n mukaan rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi luvattomalta käsittelyltä. Tämä säännös on suhteellisuusperiaatteen mukainen ja koskee kaikkea henkilötietojen käsittelyä.[132]

Laissa viranomaisten toiminnan julkisuudesta (621/1999) eli julkisuuslaissa tietoturvallisuus sisältyy hyvään tiedonhallintapaan[133]. Julkisuuslaki on suhteessa henkilötietolakiin sen sivuuttava erityislaki siltä osin kuin se nimenomaisesti koskee henkilötietojen käsittelyä.[134] Julkisuuslain 18 §:n mukaan viranomaisen tulee *hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä*.

---

[131] Saarenpää 2015, s. 364.

[132] Saarenpää 2015, 347. Saarenpää 1996, s. 128 toteaa, että lähes kaikki *itsemääräämisoikeuteen liittyvät säännökset ovat suhteellisia.* Saarenpään mukaan *se mikä periaatetasolla tunnustetaan keskeiseksi oikeudeksi, joudutaan säännöstasolla sovittamaan yhteiskunnan tekniseen ja taloudelliseen tilaan sekä vallitseviin arvoihin.*

[133] Arkistolaitos ja Tietosuojavaltuutetun toimisto toteuttivat loppuvuodesta 2014 viranomaisille suunnatun kyselyn, jossa selvitettiin hyvän tiedonhallintatavan toteutumista viranomaisissa (Yhteenveto Tietosuojavaltuutetun ja arkistolaitoksen yhteiskyselystä hyvän hallinnon toteutumisesta viranomaisissa 28.1.2015, s. 2). Yhteenvedossa s. 9 kerrotaan, että yli puolet vastaajista ilmoitti, etteivät olleet missään vaiheessa hävittäneet tietoja tietojärjestelmistään. Monesta viranomaisten käyttämästä tietojärjestelmästä puuttui mahdollisuus poistaa tai hävittää tietoja. Käytännössä nyt käytössä olevilla tietojärjestelmillä ei ole aina mahdollista toteuttaa tietosuoja-asetuksen sisältämää rekisteröidyn ”oikeutta tulla unohdetuksi.” Saatavissa: http://www.arkisto.fi/uploads/Palvelut/Julkisen%20hallinnon%20s%C3%A4hk%C3%B6iset%20palvelut/Yhteenveto%20kyselyst%C3%A4%2028%201%2015.pdf . (Katsottu 8.11.2015).
Råmanin 2006a, s. 230 mukaan ostajan on hankintatilanteessa hankala varmistautua siitä, että tilattava ratkaisu on tietoturvallinen. Markkinavetoisessa ympäristössä tyypillistä on, että tietojärjestelmien toimittajat vähentävät kehityskulujaan karsimalla (tietoturvallisuus)testauksesta.
Ostotilanteessa vallitseekin Råmanin 2006a, s. 125 mukaan usein *tiedollinen asymmetria*, jolloin toimittajaosapuoli saattaa tietää, mitkä tuotteet ovat tietoturvallisia. Ostajan sitä vastoin on hankala varmistua tietoturvallisuudesta ennen tuotteen hankkimista.
Råmanin 2006a, s. 77 mukaan selvää on, että lyhyellä tähtäimellä uusien toiminnallisuuksien tuominen kasvattaa tulosta enemmän kuin panostukset tietoturvallisuuteen.
Tietosuojavaltuutettu Reijo Aarnio muistuttaa viranomaisia tulevasta EU:n tietosuoja-asetuksesta, jossa yhtenä keskeisenä elementtinä on henkilön oikeus saada häntä koskevat tiedot hävitetyksi, kun niiden käsittely ei enää ole tarpeellista (Männikkö 2015, s. 43).

[134] Saarenpää 2015, s. 377.

Rekisterinpitäjän toiminnassa tietoturvallisuus käsittää kokonaisuuden, joka ulottuu yksittäisestä työvälineestä järjestelmäsuunnitteluun. Esimerkiksi muistitikkujen tallennuskapasiteetti on kasvanut huomattavasti. Niiden sisältämä tietomäärä voi vastata määrää, joka muutamia vuosia sitten oli organisaatioiden palvelimilla.[135] Organisaatiotasolla tietoturvallisuusvaatimus sisältää henkilöstön koulutusvelvollisuuden.[136] Viranomaisen tulee julkisuuslain 18 §:n 5 kohdan mukaisesti huolehtia palveluksessaan olevien tietoturvallisuuskoulutuksista. *Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010)* täydentää henkilötietolakia.

Taulukko 1 tietosuojaperiaatteet on ryhmitelty yleisiin, rekisterinpitäjiä koskeviin sekä yksilön tietosuojaa koskeviin periaatteisiin.[137]

Taulukko 1. Tietosuojaperiaatteiden ryhmittely.

Yleiset periaatteet	Rekisterinpitäjiä koskevat periaatteet	Yksilön tietosuojaa koskevat periaatteet
Automaattisen henkilöarvioinnin rajoittaminen	Ankara vastuu	Arkaluonteisten tietojen sekä henkilötunnuksen eritysasema
Avoimuus	Huolellisuusvelvoite	Kielto ja vastusoikeus
Hyvä tietojenkäsittelytapa	Käyttötarkoitussidonnaisuus	Markkinarauha
Käytännesäännöt	Laatuperiaate	Suostumuksen ensisijaisuus
Lakisääteisyys	Suunnitelmallisuus	Tarkastus ja oikaisuoikeus
Tarpeellisuus	Tarpeellisuus	Tietossuojaviranomaisten palvelut
Tietoturva	Tiedottamisvelvollisuus	
Viranomaiskoneiston olemassaolo ja sanktiojärjestelmä	Tietoturvallisuus	
Yksilön tunnistettavuus		

4.2 Standardointi ja muu itsesääntely

Tekniikkasidonnainen ja muuttuva verkkoyhteiskunta tarvitsee erilaista aineistoa sen määrittämiseksi, mikä on oikeudellisesti asianmukaista. Verkkoyhteiskunnan sääntelyn tehokkuus edellyttää, että lainsäädäntö, hallinto ja yksityinen toiminta toimivat yhdessä.[138] Standardilla tarkoitetaan yhteistä menettelytapaa luonteeltaan toistuvaan toimin-

[135] Saarenpää 2015, s. 360 mainitsee esimerkkinä tapauksen, jossa vuonna 2008 Yhdistyneissä kuningaskunnissa löydettiin pysäköintipaikalta muistitikku, joka sisälsi noin 12 miljoonan ihmisen verotustiedot sekä niiden käyttöön oikeutettujen henkilöiden käyttäjätunnukset salasanoineen. Muistitikkuihin liittyy muitakin riskitekijöitä kuin tietojen päätyminen sivullisten käsiin. Muistitikut on ennen käyttöä VAHTI:n (4/2013) mukaan tarkastettava haittaohjelmien torjuntaohjelmalla.
[136] Saarenpää & Pöysti et al. 1997, 1997, s. xli.
[137] Saarenpään 2015, s. 341–375 mukaisesti.
[138] Pöysti 2000, s. 96 lisää vielä, että tässä dynaamisessa ympäristössä myös oikeuskäytännön on pysyttävä ajan tasalla.

taan. Sitovuudeltaan standardit ovat *suosituksia*, mutta viranomaiset voivat edellyttää niiden käyttöä.[139] Standardit ovat tekniikan alalla tärkein itsesääntelyn instrumentti. Tietoturvallisuuden sääntelyä harkittaessa tulisikin ottaa huomioon myös alan itsesääntely ja erityisesti standardointi: tietoturvallisuuden taso on riippuvainen tietotekniikasta.[140] Käytännössä tekniset standardit voivat vaikuttaa lakeja tehokkaammin siihen, miten henkilötietoja käsitellään. Tekniset standardit eivät kuitenkaan ole mikään ihmelääke, sillä niitä voidaan soveltaa eri tavoin eri alueilla ja toimialoilla. Todennäköisesti teknisten standardien rooli kasvaa tietojen käsittelyn globaalissa harmonisoinnissa.[141] Tämän maisteritutkielman kannalta keskeisimpiä standardeja ovat informaatioteknologiaa ja turvallisuutta käsittelevät SFS-ISO/IEC 29100 ja SFS-ISO/IEC 27000.

Käytännesäännöt ja standardit täsmentävät esimerkiksi tietoturvallisuusvaatimuksia henkilötietojen suojaamisessa.[142] Käytännesääntöjen kautta annetaan lakitekstiä yksityiskohtaisemmin ohjeita ja tietoa hyvästä henkilötietojen käsittelystä. Käytännesääntöjen tarkastaminen kuuluu tietosuojavaltuutetun tehtäviin HetiL 42 §:n mukaisesti.[143] Vastuu *perusoikeuksien ja yksilön oikeuksien, turvallisuuden ja muiden yleisen edun piiriin kuuluvien tavoitteiden toteuttamisesta* kuuluu julkiselle vallalle. Standardien soveltaminen ei voi poistaa tai korvata tätä vastuuta. Standardien käyttäminen ei tästä syystä ole ongelmatonta.[144]

[139] Suomen Standardointitoimisto SFS ry. Mikä on standardi?
Saatavissa: http://www.sfs.fi/usein_kysyttya (Katsottu 3.10.2015).
[140] Saarenpää & Pöysti et al. 1997, s. 533.
[141] Kuner 2009, s. 314.
[142] Pöysti 2000, s. 96.
[143] Saarenpää 2015, s. 353-354 huomauttaa, että käytännesääntöihin voi sisältyä myös virheellisiä käsityksiä. Esimerkiksi sukututkimuksen käytännesäännöistä on ymmärrettävissä virheellisesti, etteivät henkilötietolain säännökset koskisi kuolleiden henkiöiden tietoja. Sukututkimuksen käytännesäännöt, s. 4. Saatavissa: http://www.sukuhistoria.fi/sshy/sivut/sshy/kaytannesaannot.pdf (Katsottu 8.11.2015).
[144] Saarenpää & Pöysti et al. 1997, s. 537.

5 TIETOTURVAN JA TIETOSUOJAN KANSALLINEN SÄÄNTELY

5.1 Yleisesti tietoturvallisuuden sääntelystä

Suomessa ei ole yleissäädöstä tietoturvallisuudesta[145], vaan tietoturvallisuussäädökset ovat hajaantuneet eri säädöksiin. Tietoturvavaatimuksista on säädetty esimerkiksi *laissa henkilötietojen käsittelystä rajavartiolaitoksessa* (579/2005; 16 § ja 28 §), *laissa henkilötietojen käsittelystä poliisitoimessa* (761/2003; 10a §, 20 § ja 31 §) ja *laissa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista* (617/2009; 8 §, 13,§ 16 § ja 42 §). Myös *tietoyhteiskuntakaaressa* (917/2014; 33 luku), *laissa yksityisyyden suojasta työelämässä (759/2004)* sekä *valmiuslaissa (1552/2011; 60 §, 62 §, 66 § ja 105 §)* on säädetty tietoturvasta. Nämä erityissäännökset on rajattu tämän maisteritutkielman aihealueen ulkopuolelle.

Aiemmin esiteltyjen tietosuojaperiaatteiden lisäksi tässä luvussa esitellään henkilötietolakia ja sen perustuslaillista pohjaa. *Tietosuoja* eli *henkilötietojen suoja* ja *tietoturvallisuus* sekoitetaan yleisesti toisiinsa sekä kotimaisessa että kansainvälisessä keskustelussa. Tämä johtuu pitkälti siitä, että tietosuojalainsäädäntö muodostaa tietoturvallisuusoikeuden keskeisen normilähteen. Tietosuoja ja tietoturvallisuus eroavat kuitenkin merkitykseltään toisistaan. Tietosuoja koostuu oikeudellisista normeista, jotka sääntelevät yksityisyyden suojaa henkilötietojen käsittelyssä. Tietosuojassa on kysymys informaatiota koskevista aineellisista oikeuksista ja tietoturvallisuus on aineellisiin oikeuksiin nähden välineellinen asia.[146] Suomessa henkilötietojen käsittelystä on säännöksiä useassa sadassa laissa.[147]

5.2 Perustuslaki

Yksityiselämää ei ollut suojattu perustuslaissa ennen vuoden 1995 perusoikeusuudistusta (969/1995).[148] Perusoikeusluonne ilmenee henkilötietojen suojassa siten, että henkilö-

[145] Saarenpää 2016, s. 142.
[146] Korhonen 2016, s. 362.
[147] Oikeusministeriö: EU:n tietosuoja-asetuksen edellyttämät lainmuutokset selvitetään työryhmässä. Saatavissa: http://www.oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2016/02/euntietosuoja-asetuksenedellyttamatlainmuutoksetselvitetaantyoryhmassa.html (Katsottu 18.2.2016).
[148] Korhonen 2003, s. 117. HE 309/1993, s. 14 mukaan aiemmassa hallitusmuodossa oli aukkoja perinteisten vapausoikeuksien osalta. Hallitusmuodosta puuttui esimerkiksi yksityiselämää koskeva yleissäännös. Neuvonen 2014, s. 31 toteaa, että perusoikeuksia kutsuttiin aiemmin kansalaisvapauksiksi. Käytännössä perusoikeusuudistusta edeltänyt vuoden 1919 hallitusmuoto sisälsi klassiset vapausoikeudet.

tietojen suoja voi toteutua vertikaalisesti. Tämä tarkoittaa sitä, että yksilö saa suojaa valtion puuttumiselta yksityisyyteen. Euroopan unionin alueella yksityisellä rekisterinpitäjällä on lailla asetettuja velvollisuuksia liittyen yksityisten henkilöiden henkilötietojen käsittelyyn, sillä henkilötietodirektiivi asettaa vaatimuksia myös horisontaalisuhteissa.[149]

Perustuslain 10 §:ssä säädetään yksityiselämän suojasta. PL 10.1 §:n mukaan ”Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla.” Tämä tarkoittaa, että tietosuoja on perusoikeus, jonka yksityiskohdista voidaan säätää laintasoisesti.[150]

PL 10.2 §:ssä turvataan viestinnän luottamuksellisuus: ”*Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton*.” PL 10.2 § on välineneutraali eli kaikenlaiset luottamuksellisen viestin välitystavat saavat saman suojan.[151] Käytännössä jokaisen oikeus luottamukselliseen viestintään turvataan ilman, että ulkopuoliset saavat tiedon lähetettyjen ja vastaanotettujen viestien sisällöstä.[152]

5.3 Henkilötietolaki

5.3.1 Taustaa

Suomessa tietosuojalainsäädäntöä alettiin valmistella 1970-luvulla. Kuitenkin vasta 1988 tuli voimaan ensimmäinen henkilötietojen suojasta säädellyt laki, *henkilörekisterilaki* (471/87). Henkilörekisterilaki oli toissijainen yleislaki eli muussa laissa olevat erityissäännökset syrjäyttivät vastaavat henkilörekisterilain säännökset (HRL 1.1 §).[153]

[149] Neuvonen 2014, s. 60. Neuvonen huomauttaa, että Yhdysvaltojen yksityisyyden suojelun sääntely perustuu juuri vertikaalisuhteisiin. Rekisterinpitäjiä koskevat velvollisuudet kirjattiin 1995 henkilötietodirektiiviin (I Jakso Tietojen laatua koskevat periaatteet, 6 artikla) ja sittemmin myös EU:n perusoikeuskirjan 8 artiklaan. HE 309/ 1993 vp, s. s. 29 *Käytännössä perusoikeuksien vaikutus yksityisten keskinäissuhteisiin välittyy yleensä perusoikeuksia konkretisoivan tavallisen lainsäädännön välityksellä*. Perusoikeuksilla voi tosin olla myös välittömämpiä sovellutuksia yksityisten välisissä suhteissa.

[150] Henkilötietojen suojasta säädettiin aiemmin hallitusmuodon 8.1 §:ssä. Perustuslakivaliokunta on todennut lausunnossaan (PeVL 8/1995 vp–HE 57/1995 vp), että lainsäätäjän liikkumavaraa rajoittaa se, että henkilötietojen suoja sisältyy osittain samassa momentissa lähtökohtaisesti suojatun yksityiselämän piiriin. HE 309/1993 vp, s. 53 Euroopan neuvoston piirissä hyväksytty yksilöiden suojelua henkilötietojen automaattisessa tietojenkäsittelyssä koskeva yleissopimus (SopS 35 ja 36/92) asettaa henkilötietojen suojaa koskevalle lainsäädännölle määrätyn tasovaatimuksen.

[151] Neuvonen 2014, 41.

[152] HE 309/ 1993 vp. s. 53 (kappaleessa Yksityiskohtaiset perustelut).

[153] HE 96/1998 vp, Kappale 2.1. Nykytila, henkilörekisterilaki.

Henkilörekisterilakia on kuvattu ensimmäiseksi suomalaiseksi säännökseksi tietoturvasta informaatioyhteiskunnassa.[154]

Henkilörekisterilain kumosi *henkilötietolaki* (535/1999), jolla voimaan saatettiin *henkilötietodirektiivin* asettamat muutokset lainsäädäntöömme.[155] Henkilötietojen käsittelyyn tehtiin lisäksi perusoikeusuudistuksesta johtuvia tarkastuksia.[156]

Henkilötietolaki säätää PL 10.1 §:n mukaisesti tarkemmin henkilötietojen käsittelystä. Henkilötietolaki on edeltäjänsä tavoin tietosuojaa koskeva yleislaki, joka tulee sovellettavaksi silloin, kun muualla laissa ei toisin säädetä (HeTi 2.1 §).[157] Tietoturvallisuutta ei henkilötietolaissa säädellä yksityiskohtaisesti, vaan henkilötietolaki käyttää yleisiä termejä.[158] Uutta verrattuna henkilörekisterilakiin on se, että henkilötietolaista ilmenee selvästi tietoturvallisuuteen liittyvä *suhteellisuusperiaate*.[159] Laissa ei tavoitella absoluuttista tietoturvaa, vaan tietoturvallisuus on määriteltävä suhteessa suojatarpeeseen. Tällöin myös taloudellisilla näkökulmilla on merkitystä. Tietoturva on merkittävä riskielementti henkilötietojen käsittelyssä, sillä tietojärjestelmien ylläpitäjät asettavat usein taloudellisen tehokkuuden yksilön oikeuksia tärkeämmäksi. Vaadittava tietoturvallisuustaso ei kuitenkaan voi olla matala, koska lain tavoitteena on perusoikeuksien suoja.[160] Suojauksen vaatimustasoa määrittelyssä voidaan lisäksi huomioida tekniset ratkaisut sekä henkilötietojen luonne. Arkaluonteisia tietoja koskevien rekistereiden suojauksen taso vaatii erityishuomiota. Toimenpiteitä toteutettaessa myös tietojen määrä ja ikä on otettava huomioon.[161]

---

[154] Saarenpää 2001, s. 61. Mahkonen 1997, s. 149 kertoo, että henkilörekisterilakia valmisteltaessa ei voitu varautua niihin ongelmiin, joita esim. sähköposti, internet, valvontakamerat ja kansalaiskortti (smart card) toivat mukanaan. Lainsäädännöllisesti uusiin teknologioihin voidaan varautua valitsemalla ilmaisumuotoja, jotka eivät ole sidottuja olemassa olevaan teknologiaan. Tätä kutsutaan välineneutraaliksi sääntelyksi.

[155] Saarenpää 2015, s. 337.

[156] HE 96/1998 vp, Kappale 3.1. Tavoitteet ja keinot niiden saavuttamiseksi. Katso myös 2.4. Nykytilan arviointi, jossa todetaan, että perusoikeusuudistuksen myötä joistakin aiemmin asetustasolla säädetyistä säännöksiä tulee säätää lain tasolla.

[157] Henkilötietojen käsittelystä on myös erityislakeja. Nimenomaan työelämän tarpeita varten on säädetty *laki yksityisyyden suojasta työelämässä* (75/2004). HE 75/2000 vp, s. 13.

[158] Saarenpää 2001, s. 61.

[159] Saarenpää 2001, s. 61.

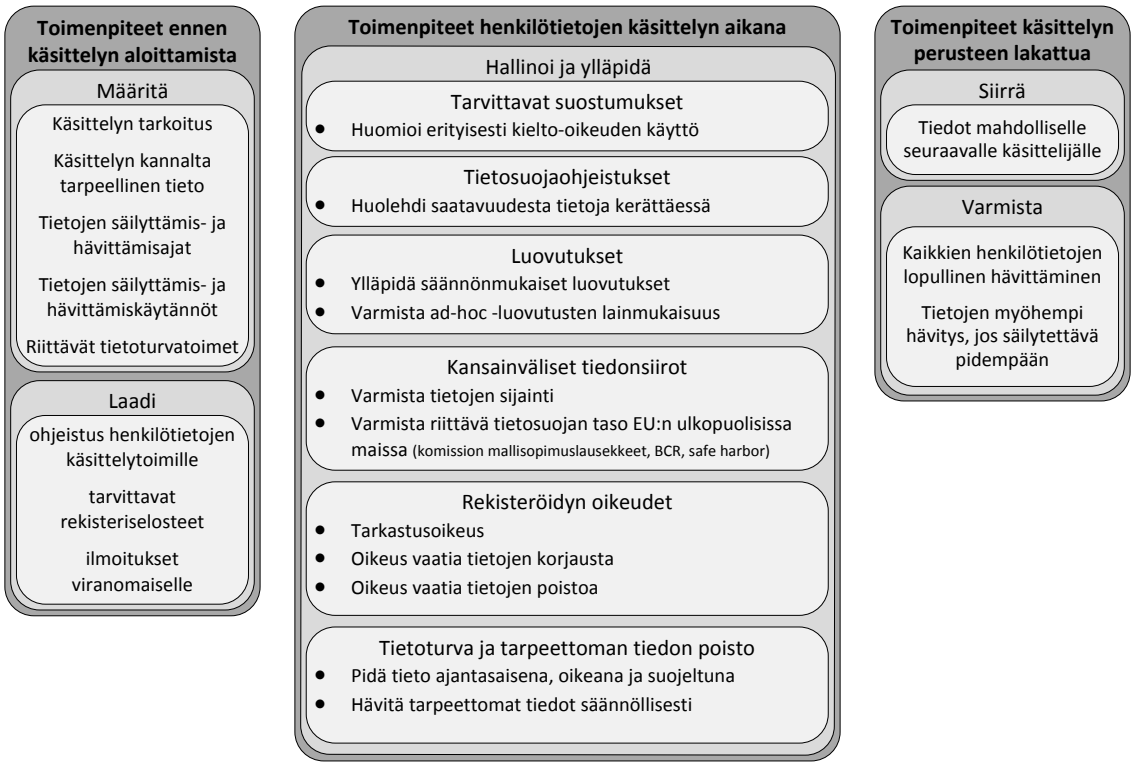
[160] Saarenpää 2015, s. 347-348. Julkisasiamiehen ratkaisuehdotuksessa asiassa C-362/14 Maximillian Schrems vastaan Data Protection Commissioner (kohta 142) on todettu, että englanninkielinen käsite ”adequate” voidaan ymmärtää tarkoittavan juuri ja juuri tyydyttävää tai riittävää tietosuojan tasoa, jolloin sen semanttinen merkitys poikkeaa ranskankielisen käsitteen ”adéquat” merkityksestä. Käsitteen tulkinnan ainoana ohjaavana perusteena voi olla perusoikeuksien suojan korkean tason saavuttamisen tavoite.

[161] HE 96/1998 vp, 7 luku Tietoturvallisuus ja tietojen säilytys, kappale 4.

Tietoturvallisuudesta ja tietojen säilytyksestä säädetään henkilötietolain 7 luvussa. Henkilötietolain 32.1 §:n mukaan rekisterinpitäjän on toteutettava *tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä*.

HetiL:n 32.2 §:ssä säädetään velvollisuuksista sellaiselle itsenäiselle elinkeinonharjoittajalle, joka toimii rekisterinpitäjän lukuun tai jolle rekisterinpitäjä teknisen käyttöyhteyden kautta luovuttaa tietoja. Tällaisen elinkeinonharjoittajan tulee ennen tietojen käsittelyyn ryhtymistä antaa asianmukaiset sitoumukset tai muuten riittävät takeet henkilötietojen suojaamisesta.[162] Tietosuojalainsäädäntöön liittyy keskeisesti sanktiojärjestelmä. Sanktiot ovat viimekätisiä keinoja toteutettaessa henkilötietojen suojaa. Henkilötietojen suojan tärkeys ilmenee kahdessa sanktiolajissa: henkilörekisteririkkomus ja henkilörekisteririkos. Henkilörekisteririkkomus on säädetty rangaistavaksi HetiL 48 §:ssä ja henkilörekisteririkos RL 38:9:ssä. Tietoturvasäännösten rikkominen on säädetty laissa rikkomukseksi, mitä voidaan pitää selvänä vinoumana. Tietoturvan keskeistä merkitystä verkkoyhteiskunnassa ei vielä lain valmisteluvaiheessa ollut täysin sisäistetty.[163] Henkilötietojen käsittely edellyttää, että henkilötietolain säännökset otetaan huomioon jo ennen käsittelytoimien aloittamista. Elinkaarimallin mukaisesti henkilötietolain säännöksiä on noudatettava myös käsittelyn aikana ja käsittelyn loputtua. Kuva 2 esittelee henkilötietojen käsittelyn elinkaarimallin.

[162] HE 96/1998 vp. s.67, Kappale yksityiskohtaiset perustelut.
[163] Saarenpää 2015, s. 354–356.



Kuva 2. Henkilötietojen käsittelyn elinkaarimalli ja HetiL:n asettamat velvollisuudet rekisterinpitäjälle (Mukaillen Pitkänen et al. 2013, s. 309).

Henkilötietolain taustalla oleva elinkaariajatus vastaa vesiputousmallia, jota ei tietojärjestelmien kehitystyössä enää juuri käytetä. Tuleva tietosuoja-asetus ei tule muuttamaan tilannetta. Henkilötietojen käsittelyn elinkaarimallin soveltaminen ketteriin kehitysmenetelmiin asettaa haasteita tietojärjestelmien kehittäjille.[164]

5.3.2 KHO 2009:82, EUT C-73/07, EIT 21.7.2015

Korkeimman hallinto-oikeuden ratkaisussa KHO 2009:82 oli kyse tapauksesta, jossa yhtiö oli julkaissut vuosittain yli miljoonan suomalaisen verotustiedot alueellisissa lehdissä. Yhtiö oli myös luovuttanut tiedot edelleen toiselle yhtiölle tekstiviestipalvelun toteuttamiseksi. Lehdissä julkaistuja tietoja luovutettiin maksua vastaan tekstiviestipalveluna.

Tietosuojavaltuutettu lausui tapauksesta tietoturvavelvoitteeseen sisältyvän *muun muassa se, ettei tietoja luovuteta muuhun tarkoitukseen, kuten tässä tapauksessa nimenomaan kyseiseen hakupalvelun osalta on tapahtunut*. Henkilötietietolain 32 §:n säännökset koskevat myös toimituksellista, taiteellista ja kirjallisista henkilötietojen käsittelyä. Myös sanomalehtien on huolehdittava siitä, että sen tietokannat ovat riittävän suojattuja ja että on toteutettu tarpeelliset tekniset ja hallinnolliset henkilötietojen suojaami-

[164] Pitkänen et al. 2013, s. 310.

seksi. Suojaamisvelvoite on kuitenkin rajattu niihin rekistereissä oleviin tietoihin, joita ei ole julkaistu.[165]

Korkeimman hallinto-oikeuden ratkaistavana ei ollut kysymys siitä, olivatko verotusta koskevat tiedot julkisia. Kysymys ei myöskään ollut oikeudesta julkaista näitä tietoja. Eettisesti kielletty toiminta olisi tullut tuomioistuimen päätöksellä sallituksi, jos julkisten tietojen teknistä käsittelyä niiden kaupallista välittämistä varten toimintana sellaisenaan olisi pidetty journalismina.[166]

EIT katsoi 21.7.2015 antamassaan ratkaisussa, että Suomi sai kieltää verotietojen julkaisemisen Veropörssi-lehdessä.[167]

[165] Pitkänen et al. 2013, s. 225.
[166] Saarenpää 2015, s. 334.
[167] Ratkaisun kohta 55.

5.3.3 Tietosuojavaltuutetun päätös (Dnro 1186/452/2010)

Tietosuojavaltuutettu valvoo HetiL 38.1 §:n mukaisesti henkilötietojen käsittelyä henkilötietolain tavoitteiden toteutumiseksi. Tietosuojavaltuutetun päätös vuodelta 2010 (Dnro 1186/452/2010) käsitteli tapausta, jossa erään henkilön yhteystiedot olivat olleet vuosien ajan salaiset numerotiedotuspalveluissa. Kyseinen henkilö havaitsi tietojensa tulleen julkisiksi ja siten saataville numerotiedotuspalveluun. Teleyritys muutti tiedot takaisin salaisiksi, mutta ei pystynyt selvittämään tietojen julkiseksi tulemisen ajankohtaa ja syytä.

Tietosuojavaltuutettu totesi, että teleyrityksen tulee käsitellä kuluttaja-asiakkaidensa henkilötietoja huolellisesti ja huolehtia niiden suojaamisesta viitaten henkilötietolain 5 §:n mukaiseen huolellisuusvelvoitteeseen ja 32 §:n tietojen suojaamista koskeviin vaatimuksiin.

Tietosuojavaltuutettu katsoi, että rekisterinpitäjälle säädetystä suojaamisvelvoitteesta huolehtiminen edellyttää muun muassa sitä, että teleyrityksen täytyy määritellä, keillä ja millä tavoin sen työntekijöillä on oikeus käsitellä asiakkaiden henkilötietoja.

Yrityksen tulee esimerkiksi käyttäjätunnus- ja salasanajärjestelmän avulla varmistaa, että tietoja pääsevät käsittelemään vain ne työntekijät, joilla on siihen työtehtäviensä johdosta oikeus.

Asiakasrekisteriin tallennettujen henkilötietojen käsittelyn tulisi olla todennettavissa, joka on mahdollista käyttämällä lokitietojärjestelmää. Teleyrityksen on luotava menettelytavat, joiden avulla yrityksen asiakasrekisterin tietojen käsittelyä voidaan seurata.

Tietosuojavaltuutettu katsoi päätöksessään, että lähtökohtaisesti teleyrityksellä tulisi olla edellytykset selvittää, kuka sen edustaja on tehnyt tiettyä henkilöä koskeviin asiakasrekistereihin muutoksia niin, että nämä tiedot ovat muuttuneet salaisista julkisiksi ja päätyneet siten saataville numerotiedotuspalveluun. Tietosuojavaltuutetun mukaan lisäksi muutoksen tekemisen ajankohdan tulisi olla selvitettävissä.

6 TIETOSUOJAN YLIKANSALLINEN SÄÄNTELY

6.1 OECD:n tietosuojaohjeet

Globaalit markkinat ja valtioiden intressi edistää tietotekniikan kehittämistyötä ovat johtaneet siihen, että tietosuojaa koskevaa lainsäädäntöä on pyritty harmonisoimaan. Tämä on edellytys henkilötietojen rajat ylittävälle liikkuvuudelle.[168] OECD:n tietosuojasuosituksen lähtökohtana on *tiedon vapaan liikkuvuuden periaate*. Tämä periaate tarkoittaa, että turhat esteet tietojen liikkuvuudelle rajojen yli tulisi poistaa.[169]

OECD hyväksyi vuonna 1980 suosituksen (OECD Guidelines Covering the Protection of Privacy and Transborder Flows of Personal Data), joka koski yksityisyyden suojaa ja kansainvälistä henkilötietojen siirtoa. Suositus sisältää esimerkiksi henkilötietojen keräämistä, laatua, tietoturvaa, rekisteröidyn tarkastusoikeutta ja kansainvälistä tiedonsiirtoa koskevia yleisperiaatteita.[170] OECD:n suositukset antavat huomattavasti liikkumavaraa kansalliselle lainsäätäjälle.[171]

Siirrettävien tietojen laatu ja määrä ovat muuttuneet vuodesta 1980 ja myös yksityisyyteen liittyvät riskit ja tarve lainvalvontaviranomaisten yhteistyölle ovat kasvaneet.[172] Suosituksia onkin päivitetty vuonna 2013.[173] Päivitetyissä suosituksissa esitellään uusia käsitteitä kuten kansalliset tietosuojastrategiat, tietosuojajohtamisen ohjelmat ja tietoturvaloukkauksesta ilmoittaminen.[174] Rekisterinpitäjillä ei juuri ole ilman lain tuomaa velvoitetta kannustimia paljastaa tietoturvaloukkauksia, sillä tietoturvaloukkaukset vaikuttavat haitallisesti yritysten maineeseen. Velvollisuus ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista edesauttaa tietoturvallisuudesta huolehtimista. Tämän lisäksi se vahvistaa muita periaatteita, joihin kuuluvat vastuullisuus, henkilökohtainen

[168] HE 96/1998, s. 13.: Kappaleessa 2.3. Kansainvälinen kehitys.
[169] Saarenpää & Pöysti et al. 1997, s. 176.
[170] HE 96/1998 vp. s. 13. OECD:n tietosuojasuosituksen yleisperiaatteet ovat: 1) tietojen keräämisen rajoittaminen, 2) tietojen laatu, 3) käyttötarkoituksen määrittely, 4) käytön rajoittaminen, 5) turvallisuuden varmistaminen, 6) avoimuus, 7) yksilön osallistuminen ja 8) rekisterinpitäjän vastuu.
[171] Bygrave 2002, s. 33 toteaa, että sama pätee myös henkilötietodirektiiviin ja tietosuojasopimukseen.
[172] OECD: Report on the cross-border enforcement of privacy laws, 4. Raportin s. 4 todetaan lisäksi, että koska tietojen siirto mihin tahansa paikkaan milloin tahansa on helppoa, myös valtioiden rajat ylittäviä tietoturvaloukkausten odotetaan kasvavan. Saatavissa: http://www.oecd.org/sti/ieconomy/37558845.pdf (katsottu 1.10.2015).
[173] OECD Privacy Law Enforcement Co-operation. Saatavissa: http://www.oecd.org/sti/ieconomy/privacylawenforcementco-operation.htm (Katsottu 4.6.2015).
[174] 2013 OECD Privacy Guidelines. Saatavissa: http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm (Katsottu 1.11.2015).

osallistuminen ja avoimuus.[175] OECD:n suositukset katsotaan soft law'ksi. OECD:n suosituksilla on ollut merkittävä rooli erityisesti maissa, joiden oma lainsäädäntö ei suojaa henkilötietoja.[176] OECD:n ohjeet eivät ole OECD:n jäsenmaita sitovia. Ohjeilla on ollut huomattavan suuri vaikutus tietosuojalainsäädännön voimaansaattamiseen eurooppalaisilla lainkäyttöalueilla, erityisesti Australiassa, Uudessa Seelannissa, Japanissa ja Hong Kongissa.[177]

6.2 Euroopan neuvoston tietosuojasopimus

Euroopan neuvoston tietosuojasopimus vuodelta 1981 toimi henkilörekisterilain ja muiden toisen sukupolven tietosuojalakinen rakenteellisena mallina. Tietosuojasopimus myös vaikutti henkilötietodirektiivin sisältöön.[178] Tietosuojasopimus on ollut Suomessa voimassa huhtikuusta 1992 alkaen. Henkilötietolaki täyttää sopimuksen asettamat vaatimukset.[179] Euroopan neuvoston tietosuojasopimus on toiminut esikuvana henkilötietodirektiiville.[180] Kaikki Euroopan neuvoston jäsenvaltiot Turkkia lukuun ottamatta ovat ratifioineet tietosuojasopimuksen.[181]

Tietosuojasopimuksesta on laadittu selitysmuistio, jonka johdannon II kohdassa todetaan, ettei selitysmuistio ole virallinen väline sopimustekstin tulkinnassa.[182] Tietosuojasopimuksen soveltamisala kattaa automaattisen tietojen käsittelyn, eikä se tule sovellettavaksi henkilötietodirektiivin tapaan tietojen manuaaliseen käsittelyyn.[183] Euroopan

---

[175] The OECD Privacy Framework,.s. 26.
Saatavissa: http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf (Katsottu 1.10.2015)
[176] Blume 2001, s. 6.
[177] Bygrave 2002, s. 32. Bygrave toteaa, että myös lukuisat yritykset ja kauppayhdistykset (trade associations) Pohjois-Amerikassa ovat virallisesti suositelleet OECD:n tietosuojaohjeita. Bygrave 2002, s. 33 mainitsee yhtenä instrumenttina Yhdistyneiden kansakuntien antamat yleisohjeet henkilötietoja sisältävistä tiedostoista (*United Nations Guidelines Concerning Computerized Personal Data Files*), jotka YK:n yleiskokous hyväksyi 14 päivänä joulukuuta 1990. Nämä ohjeet eivät ole laillisesti sitovia. Bygrave arvioi, että YK:n ohjeilla on vain vähän käytännön merkitystä verrattuna henkilötietodirektiiviin, OECD.n tietosuojasuosituksiin ja tietosuojasopimukseen. YK:n suositukset eivät ainoastaan toista muiden instrumenttien sisältöä, vaan sisältävät täydentäviä ohjeita.
[178] Saarenpää 2015, 337.
[179] Korhonen 2003, s. 93. Myös aiempi henkilörekisterilaki täytti tietosuojasopimuksen vaatimukset.
[180] Pöysti 1999, s. 475.
[181] Saatavissa: http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CL=ENG (Katsottu 7.8.2015).
[182] Bygrave 2002, s. 35 kuvaa selitysmuistiota heikoksi. Bygrave perustelee näkemystään selitysmuistion vastuuvapautuslausekkeella. Bygarve toteaa myös, että monet kansainväliset tietosuojasäännökset ovat hajanaisia ja sisältävät vain vähän virallista ohjeistusta tulkintaan.
[183] Bygrave 2002, s. 52. Bygrave huomauttaa myös, että rekisteri/ tiedosto –käsite on edelleen käytössä direktiivissä, kun kyse on manuaalisesta tietojen käsittelystä. Lainsäädännön painopiste oli 1970- ja 1980 –luvuilla tyypillisesti rekistereissä ja tiedostoissa. OECD:n suosituksen, henkilötietodirektiivin ja myöhemmin voimaan tulleiden kansallisten tietosuojalakien painopisteet ovat tietojen käsittelyssä (lähes) riippumatta siitä, miten tieto on järjestetty.

neuvoston tietosuojasopimuksen II luku säätelee tietosuojan perusperiaatteista, joista yksi on 7 artiklan säätelemä tietoturva.

Euroopan neuvoston tietosuojasopimus ei painota käsittelyn laillisuuden perusteena rekisteröidyn itsemääräämisoikeutta ja nimenomaisia suostumuksia. Tämä ilmenee siinä, että tietosuojasopimus ei määrittele nimenomaisesti yksilön oikeuksia määrätä henkilötietojensa käsittelystä. Tietosuojasopimus ei myöskään sisällä määritelmää siitä, mitä sopimuksessa tarkoitetaan laillisella tietojenkäsittelyllä.[184]

6.3 Euroopan ihmisoikeussopimus

6.3.1 Taustaa

Suomen kannalta velvoittavin ihmisoikeussopimus on Euroopan ihmisoikeussopimus (SopS 9/1990),[185] joka on pöytäkirjoineen Suomessa voimassa valtionsisäisesti eduskuntalain tasoisena.[186] EIS:sta tulee soveltaa viranomaistoiminnassa ja tuomioistuimissa.[187] EIS:seen liittyy toimiva valvontajärjestelmä, joka perustuu yksilövalitusoikeuteen (34 artikla)[188], tuomioistuinkontrolliin (19 artikla) sekä tuomioiden täytäntöönpanon valvontaan (46 artikla). Euroopan ihmisoikeustuomioistuin perustettiin 1959 EIS:n sisältämien velvoitteiden takeeksi.[189]

Rooman sopimus vuodelta 1957 ei sisältänyt ihmisoikeusnormeja. Perus- ja ihmisoikeuksiin alettiin myöhemmin viitata oikeuskäytännössä.[190] Jäsenvaltiot kokivat ongelmaksi sen, ettei perusoikeuksista ollut listausta perustamissopimuksissa. EY ei myöskään

[184] Pöysti 1999, s. 475–476.
[185] Hirvelä & Heikkilä 2013, s. 1 toteavat, että Euroopan neuvoston tärkein tehtävä on ihmisoikeuksien suojaaminen, jota se toteuttaa sitovien sopimusten ja ohjaavien suositusten kautta. Merkittävänä osoituksena sitoutumisesta järjestö hyväksyi 1950 EIS:n.
[186] Raition 2013, s.349 mukaan EY:n liittyminen ihmisoikeussopimukseen on ollut Suomelle tärkeä asia siksikin, että Suomi teki elokuussa 2000 aloitteen hallitusten väliselle konferenssille silloin voimassa olleen EY 303 artiklan muuttamiseksi. Tämän muutoksen seurauksena vahvistettiin EY:n toimivalta liittyä Euroopan ihmisoikeussopimukseen.
[187] Hirvelä & Heikkilä 2013, s. 5 käytännössä siis säännösten ristiriitatilanteet ratkaistaan normaalien ristiriidan ratkaisemisperiaatteiden mukaisesti: ylempi säädös ohittaa alemman (*lex superior derogat legi inferiori*). Perustuslakivaliokunnan mukaan (PeVL 2/1990 vp, s. 3) ristiriitatilanteissa kansalliselle lailleon annettava sisältö, joka on sopusoinnussa EIS:n kanssa. Tulkintatilanteessa on siis omaksuttava se vaihtoehto, joka edistää ihmisoikeusmääräysten toteutumista ja on siten ihmisoikeusystävällinen. Hirvelä & Heikkilä 2013, s. 6 selittävät, että lainsäätäjän ei voida ajatella tarkoittaneen säätää lakia, joka olisi ristiriidassa EIS:n kanssa.
[188] Yksityishenkilö, kansalaisjärjestö tai ryhmä voi valittaa EIT:een, jos se katsoo sopimusvaltion loukanneen heitä koskevia, EIS:ssa tunnustettuja oikeuksia. Vastaajana EIT:ssa on kaikissa tapauksissa valtio. Hirvelä & Heikkilä 2013, s. 13 huomauttavat, että jokainen viranomainen tai muu julkista valtaa käyttävä voi omalla laiminlyönnillään tai menettelyllään aiheuttaa valtion vastuun ihmisoikeuksien loukkaamisesta.
[189] Hirvelä & Heikkilä 2013, s. 6.
[190] Raitio 2013, s. 245.

ollut liittynyt osapuoleksi Euroopan ihmisoikeussopimukseen. Lissabonin sopimus muutti tämän tilanteen ja nykyisessä SEU 6(2) artiklassa todetaan nimenomaisesti, että Euroopan unioni liittyy Euroopan ihmisoikeussopimukseen.

Ihmisoikeussopimusten valtiosääntöinen vaikuttavuus käy ilmi Suomen perustuslain 22 §:stä: julkisen vallan on turvattava perusoikeuksien ja ihmisoikeuksien toteutuminen. Tämä tarkoittaa, että sopimusten takaamilla oikeuksilla on suora valtion sisäinen sovellettavuus. Liittyessään Euroopan ihmisoikeussopimukseen Suomi tunnusti Euroopan ihmisoikeustuomioistuimen tuomiovallan asioissa, jotka liittyvät sopimuksen tulkintaan ja soveltamiseen.[191]

Euroopan neuvoston ihmisoikeussopimuksen 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Tämän artiklan tarkoituksena on siis suojata yksilöä viranomaisten mielivaltaiselta puuttumiselta perhe-elämään.[192]

6.3.2 EIT 17.7.2008, I v. Suomi

Euroopan ihmisoikeustuomioistuimen ratkaisussa EIT 17.7.2008, I v. Suomi katsottiin, että sairaala oli laiminlyönyt riittävän potilastietojen käytönvalvonnan järjestämisen.[193] Väärinkäyttö ei tämän laiminlyönnin takia ollut jälkikäteen selvitettävissä. Jälkikäteinen vahingonkorvauksen mahdollisuus ei ole ratkaisun mukaan yksityisyyden suojan toteuttamiseksi riittävää.[194] Tässä yhteydessä vaadittiin tehokas ja käytännöllinen suoja, jolla luvaton käyttö estetään ennakolta.[195] Tapaus osoitti, että tuomioistuimet eivät käsitellessään potilaan vahingonkorvausvaatimuksia tunteneet henkilörekisterilakia[196]

Valittaja oli ollut töissä sairaanhoitajana eräässä sairaalassa. Valittaja oli samassa sairaalassa myös hoidettavana HIV-tartunnan takia. Valittaja epäili kollegoidensa tarkastelleen luvatta valittajasta kerättyjä potilastietoja. EIT katsoi, että pääsyä potilastietojär-

[191] Jyränki ja Husa 2012, s. 100.
[192] Hirvelä & Heikkilä 2013, s. 428.
[193] Ratkaisun kohta 29.
[194] Ratkaisun kohta 47.
[195] Bygrave 2014, s. 95.
[196] Saarenpää 2016, s 238.

jestelmään ei ollut kontrolloitu riittävästi. Jälkikäteen ei väärinkäytöstä pystytty osoittamaan aukottomasti, kun käytöstä ei ollut tallennettu lokitietoja.[197]

Tässä Suomelle langettavassa tuomiossa todettiin, että Suomi oli laiminlyönyt positiiviset velvoitteensa Euroopan ihmisoikeussopimuksen 8 artiklan toteuttamisessa.[198]

Ratkaisussa todetaan myös, että Euroopan ihmisoikeussopimuksen vaikutukset eivät rajaudu ainoastaan yksityisten henkilöiden ja viranomaisten välisiin suhteisiin. Valtion turvaamisvelvollisuus ulottuu lisäksi yksityisten välisiin suhteisiin.[199] Ihmisoikeussopimuksen takaamat oikeudet on turvattava myös henkilötietojen käsittelyedellytyksiä koskevalla lainsäädännöllä. Lainsäädännön on loukkaustilanteissa johdettava korvausvastuuseen.[200]

6.4 Euroopan perusoikeuskirja

Vuoden 1957 Euroopan talousyhteisön sopimus (Rooman sopimus) ei sisältänyt mitään mainintaa perus- tai ihmisoikeuksista. Vielä 1960-luvun alussa EU-tuomioistuin antoi ratkaisuja, joista ilmeni erittäin pidättyväinen suhtautuminen perusoikeuksiin. Näiden ratkaisujen perusteella heräsi keskustelu perusoikeuksien asemasta integraatiossa.[201] Ratkaisussa Stauder v. Stadt Ulm EU-tuomioistuin päätti, että perusoikeudet kuuluvat ”yhteisön oikeuden yleisiin periaatteisiin.”[202] 1980- ja 1990-luvuilla nähtiin, että perus- ja ihmisoikeuksien kehittäminen oli välttämätöntä EU-oikeuden ja integraation lailli-

[197] Ratkaisun kohta 44. Andreassonin ja Koiviston 2013, s. 127 mukaan sähköisellä lokilla tarkoitetaan tiedostoa, johon tallentuvat automaattisesti merkinnät tietojärjestelmän tapahtumista ja niiden aiheuttajista. Loki voi sisältää tiedon siitä, kuka on käyttänyt järjestelmää. Lokit mahdollistavat jälkikäteisen tietojen käytön valvonnan. Pääasiassa lokeja käytetäänkin siihen, että niistä voidaan jälkikäteen seurata ja valvoa tietojen käyttöä asiattoman käytön paljastamiseksi. Lokeihin liittyvistä vaatimuksista säädetään esimerkiksi *laissa sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä* (159/2007) 5.2 §:ssä. *Sosiaali- ja terveysministeriön asetus potilasasiakirjoista* (298/2009) 24.1 § velvoittaa säilyttämään lokitiedot eheinä ja muuttumattomina 12 vuotta niiden syntymisestä. *Yksityisyyden suojasta työelämässä annetun lain* (759/2004) 21 §:n mukaan teknisin menetelmin toteutettava valvonta on käytävä läpi yhteistoimintamenettelyssä, jos käyttäjä on työ- tai virkasuhteessa.
[198] Ratkaisun kohta 48.
[199] Pitkänen et al. 2013, s.19; ratkaisun kohta 36.
[200] Pitkänen et al. 2013, s.19. Myös Råman 2008, s. 562 on analysoinut kyseistä Euroopan ihmisoikeustuomioistuimen päätöstä. Råman käsittelee artikkelissaan henkilötietoihin liittyviä tietomurtoja sekä julkisen että yksityisen sektorin kannalta. Råman toteaa, että kaikkein näkyvimpiä seurauksia tietomurroista ovat suorat kustannukset, jotka johtavat mahdolliseen asiakaskannan pienenemiseen. Tietoturvaloukkauksiin liittyvä negatiivinen julkisuus voi myös vaikuttaa haitallisesti yrityksen osakehintaan. Andreasson et al. 2014b, s. 67 korostavat, että potilasrekisteritietojen käytön seuranta ja valvonta eivät ole työntekijöiden perusteetonta valvontaa. Potilasrekisteritietojen käytön seuranta ja valvonta toteuttavat työntekijän oikeusturvaa ja turvaavat potilaan yksityisyyden suojaa.
[201] Ojanen 2010, s. 119.
[202] Yhteisöjen tuomioistuimen tuomio 12.11.1969. - Erich Stauder v. Stadt Ulm - Sozialamt. - Verwaltungsgericht Stuttgartin esittämä ennakkoratkaisupyyntö. - Asia 29/69, tuomion perustelut, kohta 7.

suuden ja legitimiteetin kannalta. Perusoikeuksien kehittämisessä EU-tuomioistuin säilyi tärkeimpänä toimijana 1980-luvun loppuun asti.[203] Parlamentti, neuvosto ja komissio sekä jäsenvaltiot alkoivat kehittää perusoikeuksia ja ihmisoikeuksia aktiivisemmin vasta 1990-luvulla.[204]

Maastrichtin sopimus vuodelta 1992 muutti EU:n luonnetta taloudellis-teknisestä yhteistyöstä poliittiseksi unioniksi. Muutokset integraation painopisteissä pakottivat kiinnittämään enemmän huomiota myös perusoikeuksiin.[205]

Euroopan unionin perusoikeuskirja allekirjoitettiin 7.12.2000 Nizzan huippukokouksessa.[206] Perusoikeuskirja oli tuolloin luonteeltaan poliittinen julistus, eikä se saanut oikeudellisesti sitovaa asemaa.[207] Vuonna 2009 perusoikeuskirjasta tuli Lissabonin sopimuksen myötä oikeudellisesti sitova SEU 6(1) artiklan mukaisesti. Nykyisin EU-tuomioistuin viittaa ensisijaisesti perusoikeuskirjaan, jos perusoikeuskirja ja ihmisoikeussopimus turvaavat samaa oikeutta.[208] Euroopan perusoikeuskirjaan on koottu EU-kansalaisten oikeudet.[209]

EU:n perusoikeuskirjan II luvun 7 artikla turvaa yksityis- ja perhe-elämän kunnioittamisen. Perusoikeuskirjan 7 artikla turvaa myös jokaisen oikeuden kotinsa ja viestiensä[210] kunnioittamiseen. Tämän artiklan on tarkoitus olla yhdenmukainen Euroopan ihmisoikeussopimuksen 8 artiklan kanssa[211] ja artiklan tulkinnassa sekä soveltamisalan määrittelyssä lähtökohtana on pidetty EIS 8 artiklan tulkintaa EIT:ssa.[212]

Perusoikeuskirjan 8.1 artiklassa taataan jokaisen oikeus henkilötietojensa suojaan. Artiklassa 8.2 säädetään käsittelyn asianmukaisuudesta, käyttötarkoitussidonnaisuudesta, henkilön suostumuksesta ja jokaisen oikeudesta saada tutustua hänestä kerättyihin tietoihin. Perusoikeuskirjan 8.3 artiklassa säädetään riippumattomasta valvontaviranomai-

[203] Ojanen 2010, s. 121.
[204] Ojanen 2010, s. 123.
[205] Ojanen 2010, s. 124.
[206] Raitio 2013, s. 351.
[207] Ojanen 2010, s. 124.
[208] Raitio 2013, s. 351.
[209] Hirvelän & Heikkilän 2013, s. 359 mukaan erityisesti 8 artiklan kohdalla on havaittavissa EIT:n oikeuskäytännön evolutiivisuus ja dynaamisuus: instrumenttina EIS pystyy vastaamaan muuttuviin olosuhteisiin. Artiklaa on sovellettu uusiin aihealueisiin ja sitä on tulkittu joustavasti.
[210] Neuvonen 2014, s. 56 alaviitteessä huomauttaa, että vaikka suomenkielisessä versiossa puhutaan ”viestistä”, muissa kielissä käytetään käsitettä ”kommunikaatio”.
[211] Neuvonen 2014, s. 55.
[212] Neuvonen 2014, s. 56.

sesta.[213] EU:n tuomioistuin on ratkaisukäytännössään katsonut, ettei oikeus henkilötietojen suojaan ole absoluuttinen.[214]

6.5 Henkilötietodirektiivi (95/46/EY)

EY:n henkilötietodirektiivi eli *Euroopan parlamentin ja neuvoston direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta* on tietosuojan instrumenttina maailmanlaajuisesti johtava suunnannäyttäjä ja vertailukohta.[215] Se on vaikuttanut sekä kansallisilla tasoilla että muotoamalla kansainvälisiä tietosuojainstrumentteja. Henkilötietodirektiivin henkilötietojen siirtämistä kolmansiin maihin koskeva säännös on periaatteessa kopioitu *yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä*. Euroopan ulkopuolella direktiivi on toiminut esikuvana esimerkiksi Dubain, Malesian ja Macaon tietosuojalainsäädännöille.[216] Henkilötietodirektiivi on annettu Euroopan yhteisön perustamissopimuksen 100 a artiklan nojalla. Direktiivin tavoitteena on 1 artiklan 1 kohdan mukaisesti turvata yksilöiden perusoikeudet ja -vapaudet, erityisesti oikeus yksityisyyteen henkilötietojen käsittelyssä. Tavoitteena on 1 artiklan 2 kohdan mukaan myös henkilötietojen vapaa liikkuminen EU:n jäsenvaltioiden välillä.

Vielä voimassa oleva henkilötietodirektiivi (95/46/EY) on tärkein säädös eurooppalaisessa tietosuojalainsäädännössä.[217] Direktiivin tavoite on yksilöiden perusoikeuksien ja -vapauksien saattaminen samalle tasolle ja sen kautta henkilötietojen vapaa liikkuvuus Euroopan unionin alueella. Tämä tavoite ilmenee direktiivin johdanto-osan 8-kohdasta.

Tietoturvallisuusperiaate on sisällytetty direktiivin johdanto-osan 25-kohtaan. Sen mukaan ”*tietosuojan periaatteiden on ilmettävä yhtäältä yksilöiden, julkisten viranomaisten, yritysten, virastojen tai muiden toimielinten niissä velvoitteissa, jotka koskevat erityisesti tietojen laatua, teknistä turvallisuutta, ilmoitusmenettelyä valvontaviranomaisel-*

[213] Euroopan unionin tuomioistuin on 13.5.2014 antamassaan ratkaisussa C-131/12 vahvistanut perusoikeuskirjan 7 ja 8 artiklaan perustuvan oikeuden tulla unohdetuksi (ratkaisun kohta 99). Googlea pidettiin kyseisessä ratkaisussa henkilötietodirektiivin rekisterinpitäjänä (ratkaisun kohta 41). Ollila 2014, s. 814-815 on kommentoinut tapausta ja toteaa, että rekisterinpitäjän on yksittäisen henkilön vaatimuksesta arvioitava, ”ovatko hakutuloksissa henkilöön liittyvät linkkien sisältämät tiedot ajanmukaisia, olennaisia, virheellisiä tai puutteellisia”. Ollila huomauttaa myös, että kyseinen (Google Spain SL) ratkaisu on herättänyt maailmanlaajuisesti huomiota, arvostelua ja myös kysymyksiä sen soveltamisesta. Andreasson et al. 2014a, s. 20 toteavat, että ratkaisusta voidaan tehdä se johtopäätös, että EU-tuomioistuin on ottanut merkittävän roolin tietosuojaa korostavana ja lainsäädäntöä luovana toimijana.
[214] Yhteisöjen tuomioistuimen yhdistetyt asiat C-92/09 ja C-93/09, kohta 48.
[215] Bygrave 2014, s. 208.
[216] Bygrave 2010, s. 187-188.
[217] Saarenpää & Pöysti et al. 1997, s. 118.

le ja tietojenkäsittelyn olosuhteita, ja toisaalta rekisteröityjen oikeudessa saada tieto käsittelystä sekä mahdollisuudessa tutustua tietoihin ja pyytää niiden oikaisua, jopa vastustaa käsittelyä tietyissä olosuhteissa."

Direktiivin VII jakso säätelee henkilötietojen käsittelyn luottamuksellisuudesta ja turvallisuudesta.

Henkilötietodirektiivin johdanto-osan 11 kohdan mukaan henkilötietodirektiivi täsmentää ja myös laajentaa tietosuojasopimuksen periaatteita. Tietoturvasta säädetään direktiivin johdanto-osan 46 kohdassa. Direktiivi edellyttää, että henkilötietojen käsittelyssä *toteutetaan asianmukaiset tekniset ja organisaatiotoimenpiteet sekä käsittelyn suunnittelu- että toteuttamisvaiheessa, erityisesti turvallisuuden takaamiseksi ja siten luvattoman käsittelyn estämiseksi.* Direktiivin vaatimus on suhteellisuusperiaatteen mukainen, sillä asianmukainen turvallisuustaso määritellään suhteessa kehityksen tasoon, kustannuksiin sekä tietojenkäsittelyn riskeihin. EY:n henkilötietodirektiivin selitysosan 2 kohdan mukaan tietojärjestelmät on luotu palvelemaan ihmistä. Järjestelmiä käytettäessä on kunnioitettava yksilön perusoikeuksia ja -vapauksia, erityisesti oikeutta yksityisyyteen.

Direktiivit sitovat jäsenvaltiota ainoastaan lainsäädäntötavoitteen osalta. SEUT 288(3) artiklan mukaisesti direktiivi *jättää kansallisten viranomaisten valittavaksi muodon ja keinot* tavoitteen saavuttamiseksi. Direktiivin tarkoituksena on harmonisoida jäsenvaltioiden oikeusjärjestyksiä aineellisesti.[218] Direktiivien vaikutus kansalliseen lainsäädäntöön vaihtelee: osa direktiiveistä säätelee tarkasti kansallisten lakien sisällön, kun taas osa direktiiveistä asettaa vain minimivaatimukset. Henkilötietodirektiivin voidaan katsoa säätelevän tarkasti kansallisten lakien sisällöstä, kun otetaan huomioon henkilötietodirektiivin perustavoite tietojen vapaasta liikkuvuudesta. Yhteisön sisällä tietojen vapaa liikkuvuus edellyttäisi, että kansalliset lait olisivat keskenään identtisiä. Tietosuojalainsäädännöt kuitenkin poikkeavat toisistaan.[219]

Henkilötietodirektiivin 1 artiklassa jäsenvaltioille asetetaan velvoite turvata henkilötietojen käsittelyssä yksilöiden perusoikeudet ja vapaudet sekä erityisesti heidän oikeutensa yksityisyyteen. Direktiivi on asettanut puitteet kansalliselle tietosuojasääntelylle. Kansallisten lakien valmisteluvaiheessa on koettu ongelmalliseksi erottaa direktiivistä

[218] Jyränki ja Husa 2012, s. 224.
[219] Blume 2001, s. 3. Blume 2001, s. 4 kuvaa henkilötietodirektiiviä hybridiksi, sillä osa direktiivin ehdoista jättää kansalliselle lainsäätäjälle liikkumavaraa. Esimerkkeinä näistä heikommin sitovista artikkeleista Blume mainitsee esim. 5 artiklan, joissa jäsenvaltiot velvoitetaan määrittelemään henkilötietojen käsittelyn edellytykset II luvun säännösten rajoissa.

ehdottoman velvoittavat normit niistä normeista, joissa kansallisille lainsäätäjille on jätetty enemmän harkintavaltaa. Tästä syystä pohjoismaiset tietosuojalait eivät sisällöltään vastaa täysin toisiaan.[220]

Henkilötietodirektiivin VIII jaksossa säädetään käsittelyn luottamuksellisuudesta ja turvallisuudesta: tämän jakson 17 artikla sisältää säännökset yleisestä tietoturvallisuusvelvoitteesta.[221] Tätä tietoturvallisuusvelvoitetta täsmennetään muissa artikloissa. Varovaisuusperiaate ja vaatimus tietojen oikeellisuudesta ja täsmällisyydestä ilmenee 6 artiklasta. Direktiivissä taataan rekisteröidyn tiedonsaantioikeudet (12 artikla) sekä käsittelyn luottamuksellisuus (16 artikla). Erityisten riskialttiiden tietojenkäsittelyiden ennakkotarkastuksesta on säädetty 20 artiklassa. IV luvussa säädetään henkilötietojen siirrosta kolmansiin maihin: näiltä edellytetään riittävää tietoturvallisuuden tasoa (25 artikla).[222] Direktiivin johdannossa tietoturvallisuus on nostettu tulkintaperiaatteeksi ja toisaalta myös punnintaperiaatteeksi ratkaistaessa yksityisyyden suojan ja muiden perusoikeuksien välisiä ristiriitoja.[223]

Henkilötietodirektiivi (95/46/EY) sallii kattavammankin sääntelyn ja on siinä suhteessa *vähimmäisdirektiivi*. Toisaalta henkilötietodirektiivi on *enimmäisdirektiivi*, sillä yksilön oikeuksia ei saa rajoittaa enemmän kuin mitä direktiivi sallii.[224]

Henkilötietodirektiivin ohella aiemmin esitellyt Euroopan neuvoston tietosuojasopimus ja OECD:n ohjeet ovat vaikuttaneet useiden maiden tietosuojalainsäädäntöön. Henkilötietodirektiivi on näistä instrumenteista kattavin ja monimutkaisin.[225]

[220] Korhonen 2003, s. 127 ja Blume 2001, s. 4.
[221] Bygrave 2002, s. 67 huomauttaa, että artikla vastaa tietosuojasopimuksen 7 artiklaa, mutta on sitä yksityiskohtaisempi. Bygrave 2014, s. 164 huomauttaa, että Tanskan henkilötietolain (persondataloven, Lov nr. 429 af 31. maj 2000) tietoturvallisuutta koskeva pykälä sisältää erikoisen säännöksen. Persondataloven 41.4 §:n mukaan ”kun julkinen hallinto käsittelee henkilötietoja, josta ulkovallat ovat kiinnostuneita, täytyy niiden huolehtia toimenpiteistä, joilla henkilötiedot voidaan hävittää sodan tai vastaavan tilanteen sattuessa.”
[222] Pöysti 1999, s. 456 täsmentää tähän liittyen, että tietoturvallisuus on osa asianmukaista tietosuojaa.
[223] Ibid.
[224] Saarenpää 2015, s. 337. Jyränki ja Husa jakavat direktiivit vähimmäisdirektiiveihin, puitedirektiiveihin ja harmonisointidirektiiveihin. Jyränki ja Husa 2012, s. 225.
[225] Bygrave 2002, s. 31.

7 TIETOSUOJA-ASETUS JA TIETOTURVALLISUUS

7.1 Tietosuoja-asetuksen valmistelusta

EU:n tietosuojalainsäädännön kehittäminen liittyy Eurooppa-neuvoston hyväksymään Tukholman ohjelmaan. Tukholman ohjelman mukaan Euroopan unionilla tulee olla kattava strategia tietojen suojaamiseksi niin EU:n sisällä kuin EU:n suhteissa muihin maihinkin.[226] Eurooppa-neuvosto toteaa, että EU:n sisäisen turvallisuuden tiedonhallintastrategia perustuu mm. vahvaan tietosuojajärjestelmään ja tietoteknisten järjestelmien yhteensopivuuteen, jolla varmistetaan tietosuoja- ja tietoturvallisuusperiaatteiden noudattaminen.[227]

EU:n sekundaarinormit konkretisoivat primaarinormien sisältämiä periaatteita. Sitovia sekundaarinormeja ovat asetukset, direktiivit ja päätökset. Sekundaarinormeista asetukset ovat suoraan sovellettavia. Tämä tarkoittaa, etteivät ne vaadi kansallisia lainsäädäntötoimia.[228] *Eurooppa-oikeuden ensisijaisuus-periaate* tarkoittaa, että kansallista normia ei saa soveltaa, jos se on ristiriidassa Eurooppa-oikeuden kanssa.[229] Tietosuojan harmonisoiminen oli tärkein syy siihen, miksi lähtökohdaksi otettiin henkilötietojen suojasta säätäminen asetustasolla. Tietosuoja-asetus on henkilötietodirektiiviä yksityiskohtaisempi ja jättää direktiiviä vähemmän asioita kansallisen lainsäätäjän harkintaan.[230]

Euroopan oikeus- ja sisäministerit (OSA-neuvosto) muodostivat *yleisnäkemyksen* tietosuoja-asetuksesta 15. kesäkuuta 2015. Tämän yleisnäkemyksen rakenne on esitetty liitteessä 2. Neuvosto aloitti yleisnäkemyksen pohjalta kolmikantaneuvottelut Euroopan parlamentin ja komission[231] kanssa.[232] Näissä kolmikantaneuvotteluissa päästiin sopimukseen 15.12.2015. Euroopan parlamentti ja neuvosto hyväksyvät lopulliset tekstit

[226] U 21/2012 vp, s. 2 ja Euroopan unionin virallinen lehti, 4.5.2010, C115, s. 10.
[227] Euroopan unionin virallinen lehti, 4.5.2010, C115, s. 19.
[228] Raitio 2013, s. 230.
[229] Raitio 2013, s. 251.
[230] iapp Podcast: How To Interpret the New GDPR. Initial Reactions To The Release Of The GDPR Final Draft 12-16-15. Saatavissa: https://soundcloud.com/user-142731699/initial-reactions-to-the-release-of-the-gdpr-final-draft-12-16-15. (Kuunneltu 31.1.2016).
[231] EU:n tietosuojauudistus. Tietosuojavaltuutetun toimisto.
Saatavissa: http://www.tietosuoja.fi/fi/index/lait/euntietosuojauudistus.html (Katsottu 18.10.2015).
[232] Eurooppa-neuvosto: Yleinen tietosuoja-asetus.
Saatavissa: http://www.consilium.europa.eu/fi/policies/data-protection-reform/data-protection-regulation/ (Katsottu 18.10.2015).

vuoden 2016 alussa. Asetusta aletaan soveltaa kahden kuluttua hyväksymisestä.[233] Asetukseen tuli sisällöllisiä muutoksia kolmikantaneuvotteluiden seurauksena, kuten neuvotteluiden alussa odotettiinkin.[234] Uusia sääntöjä aletaan soveltaa kahden vuoden kuluttua hyväksymisestä. Tämän siirtymäajan aikana komissio tiedottaa yrityksille niiden velvollisuuksista ja kansalaisille näiden oikeuksista.[235] Tietosuoja-asetus jättää kansallisille lainsäätäjille tietyiltä osin liikkumavaraa. Esimerkkinä kansallisesta liikkumavasta on artikla 8, jossa säädetään tietoyhteiskunnan palveluihin liittyvään lasta koskevaan suostumukseen sovellettavista ehdoista. Sosiaalisen median käyttö tulee tietosuoja-asetuksen mukaan edellyttämään alle 16 –vuotiailta vanhempien lupaa, mutta jäsenvaltiot voivat säätää ikärajan 13 vuoteen.[236]

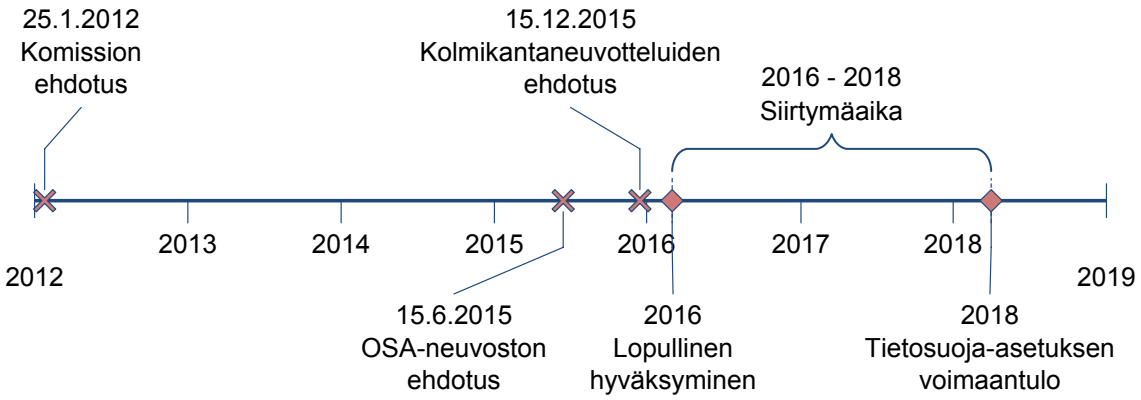
Asetusteksti on tällä hetkellä käännettävänä. Käännöstyön jälkeen asetustekstit julkaistaan Euroopan unionin virallisessa lehdessä. Julkaisemisen odotetaan tapahtuvan vuoden 2016 ensimmäisen vuosineljänneksen aikana. Monet EU:n jäsenmaat ovat jo alkaneet valmistautua tietosuoja-asetuksen voimaantuloon. Siirtymäaikana jäsenmaissa noudatetaan henkilötietodirektiiviä implementoivia kansallisia lakeja niiden sääntelemine menettelyineen. On kuitenkin erittäin todennäköistä, että siirtymäaikana tietosuoja-asetuksen säännökset vaikuttavat siihen, miten tietosuojaviranomaiset suhtautuvat säännösten noudattamiseen. Tästä on esimerkkinä tietosuoja-asetuksen vaatima tietosuojaa koskeva vaikutustenarviointi[237], jota useiden EU:n jäsenmaiden valvontaviranomaiset edellyttävät jo nyt huolimatta siitä, ettei tällaista vaatimusta ole henkilötietodirektiivissä. On myös arvioitu, että säännösten tulkinta tulee eroamaan jäsenvaltioittain. Tietosuoja-asetus ei tule täysin yhdenmukaistamaan eurooppalaista tietosuojasääntelyä, sillä kansallisille lainsäätäjille on jätetty harkintavaltaa useiden säännösten osalta.[238] Suomen osalta tämä tarkoittaa, että kaikki henkilötietojen käsittelystä säätelevät lait on

[233] Euroopan komissio – Lehdistötiedote. EU:n tietosuojauudistuksen hyväksyminen vauhdittaa digitaalisten sisämarkkinoiden toteuttamista. Saatavissa: http://europa.eu/rapid/press-release_IP-15-6321_fi.htm (Katsottu 27.1.2016).
[234] EU:n tietosuojauudistus. Tietosuojavaltuutetun toimisto.
Saatavissa: http://www.tietosuoja.fi/fi/index/lait/euntietosuojauudistus.html (Katsottu 18.10.2015)
[235] Euroopan komissio – Lehdistötiedote. EU:n tietosuojauudistuksen hyväksyminen vauhdittaa digitaalisten sisämarkkinoiden toteuttamista. Saatavissa: http://europa.eu/rapid/press-release_IP-15-6321_fi.htm (Katsottu 5.1.2016).
[236] iapp Podcast: How To Interpret the New GDPR. Initial Reactions To The Release Of The GDPR Final Draft 12-16-15. Saatavissa: https://soundcloud.com/user-142731699/initial-reactions-to-the-release-of-the-gdpr-final-draft-12-16-15. (Kuunneltu 31.1.2016).
[237] 33 artikla.
[238] iapp Podcast: How To Interpret the New GDPR. Initial Reactions To The Release Of The GDPR Final Draft 12-16-15. Saatavissa: https://soundcloud.com/user-142731699/initial-reactions-to-the-release-of-the-gdpr-final-draft-12-16-15. (Kuunneltu 31.1.2016).

saatettava tietosuoja-asetuksen mukaisiksi asetuksen mahdollistaman kansallisen liikkumavaran puitteissa. Asetusta tarkentavaa lainsäädäntöä EU:n jäsenvaltiot voivat antaa erityisesti koskien julkista sektoria.[239]

Kolmikantaneuvotteluissa tehdyt muutokset on esitelty kunkin artiklan kohdalla epävirallisen käännöksen pohjalta.[240] Liite 3 esittää epävirallisen suomennoksen pohjalta tehdyn tietosuoja-asetuksen rakenteen. Komission 2012 antamaan tietosuoja-asetusehdotukseen viitataan silloin, kun sisältö on merkittävästi muuttunut valmistelun aikana.

Tietosuoja-asetusta on valmisteltu neljä vuotta ja tänä aikana sen muuttamiseksi on tehty useita ehdotuksia. Lukemisen havainnollistamiseksi kuvassa 3 on esitetty aikajana, jossa on merkitty tämän maisteritutkielman kannalta keskeisimmät tietosuoja-asetusehdotukset ja myös asetuksen voimaantulo.



Kuva 3. Tietosuoja-asetuksen valmistelun eteneminen.

7.2 Tietosuojakysely ja esimerkkejä eurooppalaisista käytännöistä

Vuonna 2015 tehdyssä tietosuojaa koskevassa tutkimuksessa haastateltiin 28 000 Euroopan unionin kansalaista.[241] Vastaajista yli 90 % haluaisi, että heille ilmoitettaisiin, jos heitä koskevaa tietoa varastettaisiin tai hukattaisiin. Ruotsissa vastaajista peräti 98 % halusi tulla informoiduksi. Suomessa vastaava osuus oli 96 %. Vain 6 % eurooppalaisis-

[239] Oikeusministeriö: EU:n tietosuoja-asetuksen edellyttämät lainmuutokset selvitetään työryhmässä. Saatavissa: http://www.oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2016/02/euntietosuoja-asetuksenedellyttamatlainmuutoksetselvitetaantyoryhmassa.html (Katsottu 18.2.2016).

[240] Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta (yleinen tietosuoja-asetus) [ensimmäinen käsittely] – Poliittinen yhteisymmärrys. Saatavissa: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/fi/pdf (Katsottu 20.2.2016).

[241] European Comission: Data Protection Factsheet. Eurobarometer, s. 1. Saatavissa: http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_eurobarometer_240615_en.pdf (Katsottu 13.9.2015)

ta ei haluaisi tulla informoiduksi.[242] Sosio-ekonominen tausta ei vaikuttanut vastauksiin, vaan kaikissa ryhmissä suurin osa halusi saada ilmoituksen henkilötietoihin kohdistuneesta tietoturvaloukkauksesta.[243] Kyselyssä tiedusteltiin myös, kenen tulisi tehdä ilmoitus, kun henkilötietoihin on kohdistunut tietoturvaloukkaus. Noin 2/3 eurooppalaisista oli sitä mieltä, että henkilötietoja käsittelevän viranomaisen tai yksityisen yrityksen tulisi kertoa heille, jos tietoja on varastettu tai kadotettu.[244] Vain 45 % eurooppalaisista oli sitä mieltä, että ilmoitusvelvollisuus kuuluisi asumisvaltion tietosuojaviranomaiselle.[245]

Yhä useampi EU:n jäsenvaltio on säätänyt lain, jossa asetetaan rekisterinpitäjälle velvollisuus ilmoittaa tietoturvaloukkauksista. Kansalliset lainsäädännöt vaihtelevat suuresti jäsenvaltioittain. Saksassa ilmoitusvelvollisuus koskee kaikkia toimialoja, kun taas esimerkiksi Unkari on rajoittanut ilmoitusvelvollisuuden koskemaan ainoastaan telealan toimijoita.[246] EU:n jäsenvaltiot ovat säätäneet seuraamuksista varsin eri tavoin. Isossa-Britanniassa tietosuojavaltuutettu (Infomation Commissioner's Office, ICO) on toimivaltainen asettamaan enintään 500 000 £:n suuruisen seuraamuksen tietoturvaloukkauksista, jotka todennäköisesti aiheuttavat huomattavaa vahinkoa tai huomattavaa kärsimystä. Saksassa tietosuojavaltuutettu voi asettaa enintään 300 000 €:n sakon, jos rekisterinpitäjä ei ilmoita tietoturvaloukkauksesta tai ei ilmoita siitä ajoissa tai ei ilmoita siitä täydellisesti.[247] Seuraamusmaksujen suuruus on eräissä tapauksissa osoittautunut matalaksi verrattuna tietoturvaloukkauksesta saatuun hyötyyn. Esimerkiksi Isossa-Britanniassa sairaanhoitaja tuomittiin maksamaan 150 £:n jokaisesta rikkomuksesta, kun hän sai tapaturmavakuutusyritykselle myydessään henkilötiedosta 900 £:n suuruisen korvauksen.[248] Muutamissa EU:n jäsenvaltioissa on asetettu erilaisia kynnyksiä, joiden ylittyessä tietoturvaloukkauksesta on ilmoitettava rekisteröidylle.[249]

IAPP:n vertailevan tutkimuksen mukaan Euroopan tietosuojaviranomaiset asettivat seuraamusmaksuja yhteensä 31 miljoonaa euroa. Seuraamusmaksut koostuivat lähes koko-

---

[242] Special Eurobarometer 431, s. 72.
Saatavissa: http://ec.europa.eu/public_opinion/archives/ebs/ebs_431_en.pdf (Katsottu 13.9.2015).
[243] Special Eurobarometer 431, s. 73.
[244] Special Eurobarometer 431, s. 76 mukaan suomalaisista kannatti 79 % ja ruotsalaisista 91 %.
[245] Special Eurobarometer 431, s. 74.
[246] Kierkegaard 2013, s. 127.
[247] Kierkegaard 2013, s. 128. Saksan tietosuojalain (Bundesdatenschutzgesetz) 43 § 2 kohdan mukaan rekisterinpitäjälle voidaan asettaa 300 000 € hallinnollinen seuraamusmaksu, jos osavaltion tietosuojalaissa osavaltion tietosuojaviranomaiselle on asetettu toimivalta asettaa tämänsuuruinen sakko. The International Comparative Legal Guide to: Data Protection 2015, s. 91. Saatavissa: https://www.hunton.com/files/webupload/ICLG_DP15_Hunton_All_Chapters.pdf. (Katsottu 8.11.2015).
[248] Kierkegaard 2013, s. 131.
[249] Kierkegaard 2013, s. 129.

naisuudessaan kolmen jäsenmaan eli Espanjan, Italian ja Ison-Britannian tietosuojaviranomaisten asettamista sakoista.[250]

7.3 Käsittelyn turvallisuus

Tietosuoja-asetuksen johdanto-osassa[251] edellytetään, että asianmukaiset tekniset ja organisatoriset toimenpiteet toteutetaan käsittelyn suunnittelu- ja toteuttamisvaiheessa.[252]

Tietosuoja-asetuksen IV luku säätää rekisterinpitäjästä ja henkilötietojen käsittelijästä. IV luvun 2 jakso sääntelee tietoturvallisuudesta ja sisältää artiklat käsittelyn turvallisuus, henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle ja henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle. Käsittelyn turvallisuutta säätelevän artiklan[253] 1 kohta velvoittaa rekisterinpitäjää ja henkilötietojen käsittelijää. Rekisterinpitäjän ja henkilötietojen käsittelijän on o*ttaen huomioon uusin tekniikka[254] ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä yksilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit, tarvittaessa toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet.* Näitä toimenpiteitä ovat esimerkiksi

- *henkilötietojen julkaiseminen salanimellä ja salaus*[255]*;*
- *kyky taata henkilötietoja käsittelevien järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus;*
- *kyky palauttaa nopeasti tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa;*
- *menettely, jolla testataan, tutkitaan ja arvioidaan säännöllisesti teknisten ja organisatoristen toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi.*[256]

---

[250] Kierkegaard 2013, s. 132; Data Protection Authorities. 2011 Global Survey, s. 21. International Association of Privacy Professionals.
Saatavissa: https://iapp.org/media/pdf/knowledge_center/DPA11_Survey_final.pdf (Katsottu 8.11.2015).
[251] Kolmikantaneuvotteluissa hyväksytyn tietosuoja-asetusehdotuksen johdanto-osan 61 kohdassa.
[252] Skouma & Léonards.2015, s. 56 toteavat, että *privacy by design* –periaatteen mukaisesti tietosuojaan liittyvät vaatimukset tulee huomioida uusien informaatioteknologioiden, liiketoimintamallien ja verkkoinfrastruktuurien suunnitteluvaiheissa.
[253] Kolmikantaneuvotteluissa sovitun tietosuoja-asetusehdotuksen 30 artikla.
[254] Osa-neuvosto ehdotti vaatimusta suhteessa ”saatavilla olevaan” tekniikkaan. Tietosuoja-asetuksessa puhutaan komission ehdotuksen mukaisesti ”uusimmasta” tekniikasta.
[255] OSA-neuvoston ehdottama täsmennys, joka sisältyy myös kolmikantaneuvotteluissa hyväksyttyyn ehdotukseen.

Arvioitaessa asianmukaista turvallisuustasoa[257] on erityisesti kiinnitettävä huomiota *tietojenkäsittelyn aiheuttamiin riskeihin, erityisesti siirrettyjen, tallennettujen tai muutoin käsiteltyjen henkilötietojen vahingossa tapahtuvan tai laittoman tuhoamisen, häviämisen, muuttamisen, luvattoman luovuttamisen tai henkilötietoihin pääsyn vuoksi*.[258]

Tietosuoja-asetuksen 30(2) artiklan mukaan hyväksyttyjen käytännesääntöjen[259] tai hyväksytyn sertifiointimekanismin[260] noudattaminen voi olla yksi tekijä osoitettaessa, että 30(1) artiklan mukaisia vaatimuksia noudatetaan.[261]

Tietosuoja-asetus asettaa rekisterinpitäjälle ja käsittelijälle velvollisuuden huolehtia siitä, *että jokainen rekisterinpitäjän tai käsittelijän alaisuudessa toimiva henkilö, jolla on pääsy henkilötietoihin, saa käsitellä niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin tai jäsenvaltion lainsäädännössä toisin vaadita.*[262]

7.4 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen valvontaviranomaiselle

Tietosuoja-asetus velvoittaa rekisterinpitäjää ilmoittamaan henkilötietojen tietoturvaloukkauksesta valvontaviranomaiselle.[263] Tietosuoja-asetuksen 31(1) artiklan mukaan henkilötietojen tietoturvaloukkaustilanteessa, *joka todennäköisesti aiheuttaa yksilöiden oikeuksien ja vapauksien kannalta suuren riskin, rekisterinpitäjän on ilmoitettava siitä ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitu-*

---

[256] Kolme viimeisintä esimerkkiä sisältyvät kolmikantaneuvotteluiden ehdotukseen, mutta eivät olleet osana OSA-neuvoston yleisnäkemystä.
[257] OSA-neuvoston yleisnäkemyksessä 30 artiklan 1a kohdan & kolmikantaneuvotteluissa hyväksytyn ehdotuksen mukaan.
[258] Kolmikantaneuvottelujen ehdotuksen 30(1a) artikla.
[259] Tietosuoja-asetuksen IV luvun 5 jaksossa säädetään käytännesäännöistä ja sertifioinnista. Hyväksytyistä käytännesäännöistä säännellään ko jakson 38 artiklassa.
[260] Hyväksytystä sertifiointimekanismista käytännesäännöistä säännellään tietosuoja-asetuksen 39 artiklassa.
[261] Kolmikantaneuvotteluiden ehdotuksen 30(2a) kohta.
[262] OSA-neuvoston yleisnäkemyksen 30(2b) artikla, joka hyväksyttiin kolmikantaneuvotteluissa sellaisenaan.
[263] OSA-neuvoston yleisnäkemyksen 31 artikla & kolmikantaneuvotteluiden tuloksena tehty ehdotus. OSA-neuvoston yleisnäkemyksessä esimerkkinä todennäköisestä yksilön oikeuksien ja vapauksien kannalta suuresta riskistä mainitaan *syrjintä, henkilöllisyysvarkaus tai -petos, taloudellinen menetys, salanimellä julkaisemisen luvaton kumoutuminen, maineen vahingoittuminen, salassapitovelvollisuuden alaisten tietojen luottamuksellisuuden menetys tai muu merkittävä taloudellinen tai sosiaalinen vahinko.* Tämä lista ei sisälly kolmikantaneuvotteluissa hyväksyttyyn ehdotukseen. Salanimellä julkaiseminen oli yksi tietosuoja-asetukseen valmistelun aikana lisätyistä määritelmistä (kolmikantaneuvotteluiden 4(3b) artikla).

losta (…) *toimivaltaiselle valvontaviranomaiselle*. Rekisterinpitäjän on toimitettava valvontaviranomaiselle perusteltu selitys, jos ilmoitusta ei anneta 72 tunnin kuluessa.[264]

Valvontaviranomaiselle ei kaikissa tapauksissa tarvitse ilmoittaa henkilötietojen tietoturvaloukkauksista. Tietosuoja-asetuksen 31(1) artiklan mukaan ilmoitusta valvontaviranomaiselle ei tarvitse tehdä, jos *henkilötietoihin kohdistuneesta tietoturvaloukkauksesta ei todennäköisesti aiheudu yksilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä*.[265]

Henkilötietojen käsittelijän on ilmoitettava rekisterinpitäjälle kaikista tietoturvaloukkauksista. Tietosuoja-asetuksen 31(2) artiklassa nimittäin asetetaan *käsittelijälle* velvollisuus ilmoittaa rekisterinpitäjälle henkilötietojen tietoturvaloukkauksesta *viipymättä saatuaan sen tietoonsa*.[266] Tietosuoja-asetuksen 31(2) artiklaan ei siis liity ilmoitusvelvollisuuden poistavia perusteita.

Tietosuoja-asetuksen 31(3) artikla sääntelee tietoturvaloukkauksesta tehtävän ilmoituksen sisällöstä.[267] Sen mukaan ilmoituksessa on kuvattava henkilötietojen tietoturvaloukkaus, mukaan lukien *mahdollisuuksien mukaan*[268] *asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät sekä tietueiden ryhmät ja arvioidut lukumäärät*. Tietosuoja-asetus edellyttää, että ilmoitus sisältää *tietosuojavastaavan nimen ja yhteystiedot tai muun yhteyspisteen, josta voi saada lisätietoja.* Ilmoituksesta on käytävä ilmi *henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset* ja kuvaus toimenpiteistä, *joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta*. Rekisterinpitäjän on *tarvittaessa*[269] suositeltava toimenpiteitä *mahdol-*

---

[264] Oikeus- ja sisäasioiden neuvoston (OSA) yleisnäkemys uudesta tietosuoja-asetuksesta, s. 119. Saatavissa: http://data.consilium.europa.eu/doc/document/ST-9565-2015-INIT/fi/pdf (Katsottu 27.9.2015). Myös European Digital Rights ehdotti 72 tunnin aikarajaa, jota European Digital Rights perustelee henkilötietojen käsittelijöiden laajalla kirjolla: asetus koskee sekä pieniä että suuria yrityksiä. Saatavissa: http://protectmydata.eu/articles/articles-31-40/article-31/ (Katsottu 20.12.2015). Komission tietosuoja-asetusehdotuksessa ehdotettiin säädettäväksi 24 tunnin aikaraja.

[265] Komission tietosuoja-asetusehdotuksessa velvollisuus ilmoittaa oli ehdoton kaikissa tapauksissa. Useat intressitahot vastustivat tätä vaatimusta. Katso kappale 7.7 Intressiryhmien muutosehdotuksia.

[266] OSA-neuvoston yleisnäkemyksen 31 artiklan 2 kohta, joka hyväksyttiin aneuvotteluissa sellaisenaan. Komission tietosuoja-asetusehdotuksessa käytettiin ilmaisua ”*heti*.”

[267] OSA-neuvoston yleisnäkemyksen 31 artiklan 3 kohta, joka hyväksyttiin lähes sellaisenaan kolmikantaneuvotteluissa.

[268] OSA-neuvoston yleisnäkemyksessä vaadittiin lisäksi, että nämä tiedot olisi kuvattava ”tarvittaessa.” Tämä tarkennus ei ole osa kolmikantaneuvotteluissa hyväksyttyä tietosuoja-asetusehdotusta.

[269] ”Tarpeen mukaan” on lisätty kolmikantaneuvotteluissa.

listen haittavaikutusten lieventämiseksi.[270] Ilmoituksessa vaadittavia tietoja ei ole välttämätöntä toimittaa samanaikaisesti.[271]

Tietosuoja-asetuksen 31(4) artikla velvoittaa rekisterinpitäjää dokumentoimaan henkilötietojen tietoturvaloukkaukset. *Rekisterinpitäjän on dokumentoitava kaikki henkilötietojen tietoturvaloukkaukset, mukaan lukien tietoturvaloukkaukseen liittyvät seikat, sen vaikutukset ja toteutetut korjaavat toimet.* Rekisterinpitäjän on siis pidettävä tietoturvaloukkauksista lokia, vaikka tapahtumasta ei tarvitsisikaan ilmoittaa viranomaisille.[272] Artiklan mukaan valvontaviranomaisen on pystyttävä tarkastamaan näiden dokumenttien pohjalta se, että artiklaa 31 on noudatettu.

7.5 Henkilötietojen tietoturvaloukkauksesta ilmoittaminen rekisteröidylle

Tietosuoja-asetus säätää henkilötietojen tietoturvaloukkauksesta ilmoittamisesta valvontaviranomaisen lisäksi myös rekisteröidylle[273]. Tietosuoja-asetuksen 32(1) artiklan mukaan *kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin yksilön oikeuksille ja vapauksille, rekisterinpitäjän ilmoitettava tietoturvaloukkauksesta rekisteröidylle ilman aiheetonta viivytystä*.[274]

Tietosuoja-asetus sääntelee rekisteröidylle tietoturvaloukkauksesta tehtävän ilmoituksen sisällöstä.[275] Tietosuoja-asetuksen 32(2) artiklan mukaan ilmoituksessa on vähintäänkin ilmoitettava *tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta voi saada lisätietoa*; *kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset*[276] ja *kuvattava toimenpiteet, joita rekisterinpitäjä on ehdottanut tai jotka se on toteuttanut henkilötietojen tietoturvaloukkauksen johdosta, tarvittaessa myös toimenpiteet mahdollisten haittavaikutusten lieventämiseksi.*

---

[270] OSA-neuvoston yleisnäkemyksessä ehdotettiin, että nämä seuraukset olisivat rekisterinpitäjän määrittelemiä. Kolmikantaneuvotteluissa hyväksytty ehdotus ei sisällä vastaavaa täsmennystä.
[271] OSA-neuvoston yleisnäkemys & kolmikantaneuvotteluiden tietosuoja-asetusehdotus: Artikla 31(3a).
[272] iapp Podcast: How To Interpret the New GDPR. Initial Reactions To The Release Of The GDPR Final Draft 12-16-15.Saatavissa: https://soundcloud.com/user-142731699/initial-reactions-to-the-release-of-the-gdpr-final-draft-12-16-15. (Kuunneltu 31.1.2016).
[273] OSA-neuvoston yleisnäkemyksen 32 artikla & kolmikantaneuvotteluiden ehdotuksen 32 artikla.
[274] OSA-neuvoston yleisnäkemykseen sisältynyt lista yksilöiden oikeuksien ja vapauksien kannalta suurista riskeistä on poistettu kolmikantaneuvotteluissa hyväksytystä ehdotuksesta. Lista vastaa alaviitteessä 263 esitettyä.
[275] OSA-neuvoston yleisnäkemyksen 32(3) artikla, joka hyväksyttiin lähes sellaisenaan osaksi kolmikantaneuvotteluiden ehdotusta.
[276] Tämä rekisteröidyn oikeuksien kannalta tärkeä tieto ei sisältynyt komission tietosuoja-asetusehdotukseen.

Ilmoitukselle on asetuksessa asetettu myös laadullisia vaatimuksia. Ilmoitus on nimittäin tietosuoja-asetuksen 32(2) artiklan mukaan tehtävä selkeällä ja yksinkertaisella kielellä.[277]

Henkilötietojen tietoturvaloukkauksista ei kaikissa tapauksissa tarvitse ilmoittaa rekisteröidylle. Ilmoitusta ei tarvitse tehdä rekisteröidylle, jos *rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet*[278] *ja tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla tiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta.*

Ilmoitusta ei myöskään vaadita tilanteissa, joissa *rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, että (...)rekisteröidyn oikeuksiin ja vapauksiin kohdistuva suuri riski ei enää todennäköisesti toteudu* tai jos ilmoittaminen *vaatisi kohtuutonta vaivaa.* Viimeksi mainitussa tapauksessa edellytetään kuitenkin, että ilmoittamiseen *on käytettävä julkista tiedonantoa tai vastaavaa toimenpidettä, jolla rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla.*[279]

Tietosuoja-asetus tulee asettamaan valvontaviranomaiselle mahdollisuuden vaatia, että rekisterinpitäjä ilmoittaa rekisteröidylle henkilötietoihin kohdistuneesta tietoturvaloukkauksesta. Tietosuoja-asetuksen 32(4) artiklan mukaan j*os rekisterinpitäjä ei ole vielä ilmoittanut henkilötietojen tietoturvaloukkauksesta rekisteröidylle, valvontaviranomainen voi vaatia ilmoituksen tekemistä.* Arvioituaan, kuinka todennäköisesti loukkaus ai-

[277] Selkeän ja yksinkertaisen kielen vaatimus ei ollut OSA-neuvoston yleiskatsauksessa osa artiklaa, mutta se oli mainittu OSA-neuvoston yleiskatsauksen johdanto-osan 32 kohdassa. Euroopan parlamentti ehdotti artiklaan 32 muutosta, jossa ilmoitukselle asetettiin laadullisia vaatimuksia: ilmoitus tulisi tehdä ymmärrettävällä, selkeällä ja helppotajuisella kielellä. Saatavissa: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0212+0+DOC+XML+V0//EN Kohta Amendment 126 (Katsottu 27.9.2015).

[278] Kolmikantaneuvotteluiden tuloksena saavutetussa ehdotuksessa ei komission tietosuoja-asetusehdotuksen mukaisesti edellytetä, että ”rekisterinpitäjä osoittaa valvontaviranomaista tyydyttävällä tavalla, että se on toteuttanut asianmukaiset tekniset suojatoimenpiteet”. Toisaalta kolmikantaneuvotteluiden ehdotuksessa on huomioitu, että kyseessä voivat olla myös ”organisatoriset toimenpiteet”. Komission ehdotus ei sisältänyt ”organisatorisia toimenpiteitä.”

[279] Kolmikantaneuvotteluissa sovittu ehdotus vastaa lähes OSA-neuvoston ehdotusta. OSA-neuvoston yleisnäkemyksessä on täsmennys siitä, että kohtuuton vaiva viittaa erityisesti tapausten lukumäärään. OSA-neuvoston ehdotus sisälsi lisäksi kohdan, jonka mukaan ilmoitusta ei tarvitsisi tehdä, jos se voisi vahingoittaa tärkeää yleistä etua.

heuttaa suuren riskin, valvontaviranomainen voi myös *vaatia ilmoituksen tekemistä tai päättää, että jokin* ilmoitusvelvollisuuden poistamisen perusteista on olemassa.[280]

7.6 Käsittely Suomen eduskunnassa – valiokuntien lausuntoja

Perustuslakivaliokunnan antaman lausunnon mukaan henkilötietojen suojan osalta yleinen tietosuoja-asetusehdotus ja tietosuojadirektiiviehdotus noudattelevat ja konkretisoivat varsin hyvin EU:n perusoikeuskirjan 8 artiklan määräyksiä henkilötietojen suojasta.[281]

Hallintovaliokunta on katsonut tietoturvaloukkauksista ilmoittamisen olevan tietyissä tilanteissa perusteltua. Hallintovaliokunta totesi lausunnossaan, että vähäiset tietoturvaloukkaukset tulisi rajata ilmoitusvelvollisuuden ulkopuolelle.[282] Hallintovaliokunta totesi myös, että velvollisuus tulisi tehdä ”ilman aiheetonta viivytystä”, eikä sitä tulisi rajata tiettyyn tuntimäärään.[283]

Asetuksen valmisteluvaiheessa esitettiin huomioita siitä, että eri EU-hankkeet tulee sovittaa yhteen, jotta hallinnollinen taakka ei kasvaisi. Tavoitteena oli välttää hankkeiden mahdollisia päällekkäisyyksiä.[284] Hallinnollista taakkaa on pyritty vähentämään riskipohjaisella lähestymistavalla, jolloin sääntelyssä otetaan huomioon henkilötietojen käsittelyyn kulloinkin liittyvät riskit. Näin on pyritty sekä välttämään pieniriskisen toiminnan ylisääntelyä ja toisaalta varmistamaan rekisteröidyn suoja korkean riskin toi-

---

[280] Tämä vaatimus oli osa komission tietosuoja-asetusehdotusta ja sisältyy myös kolmikantaneuvotteluissa hyväksyttyyn ehdotukseen. OSA-neuvoston ehdotuksesta tämä vaatimus oli poistettu.

[281] PeVL 12/2012 vp–U 21/2012 vp, s. 2. Perustuslakivaliokunta (PeVL 12/2012 vp–U 21/2012 vp, s. 3) kiinnitti kuitenkin huomiota siihen, että komissiolle asetusehdotuksessa esitetyt laajat valtuudet antaa delegoituja säädöksiä vaativat täsmällisempää arviointia artiklakohtaisesti.

[282] U 21/2012 vp HaV 03.06.2015 emeritusprofessori Ahti Saarenpää, s. 4 pitää rekisterinpitäjille asetettua velvollisuutta ilmoittaa tietoturvaloukkauksista yhtenä ehdotuksen näkyvistä uutuuksista. Saarenpää huomauttaa, että tietoturvaloukkausten ”vähäisyys” johtaa siihen suoraan kysymykseen, miten tietoturvaloukkauksen vähäisyys määritellään. Saatavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2015-AK-5174.pdf (Katsottu 13.12.2015).

[283] HaVL 6/2013 vp — U 21/2012 vp, s. 2.

[284] HaVL 6/2013 vp s. 5 mainitaan esimerkkinä EU:n tason strategioista ja säädöshankkeista liittyen tietosuojaan ja tietoturvaan EU:n tietoturvadirektiivi (HaVL 5/2013 vp — U 13/2013 vp). Albrecht 2012, s. 5 huomauttaa tietomurroista ilmoittamisvelvollisuuteen liittyen, että vaatimuksen tulee olla yhdenmukainen sähköisen viestinnän tietosuoja- direktiivin (Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla) kanssa. Saatavissa: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/915/915162/915162en.pdf. (Katsottu 10.8.2015).

minnassa.[285] On arvioitu, että rekisterinpitäjälle tulee lisäkustannuksia tietojärjestelmiin tarvittavien muutosten takia.[286]

7.7 Vahtikoirajärjestöjen ja muiden intressiryhmien kannanottoja

Lukuisat järjestöt ovat lausuneet komission tietosuoja-asetusehdotuksesta ja sitä edeltäneestä tiedonannosta kattavasta lähestymistavasta henkilötietojensuojaan Euroopan unionissa. Tässä kappaleessa esitellään vahtikoirajärjestöjen[287] kannanottojen lisäksi taloudellisten toimijoiden ja suurien sosiaalisten medioiden edustamia kannanottoja, erityisesti liittyen tietoturvakysymyksiin.

*Statewatch*in mukaan tiedonantoon kattavasta lähestymistavasta henkilötietojensuojaan Euroopan unionissa sisältyi useita positiivisia ehdotuksia, kuten kansallisten tietosuojaviranomaisten toimivallan vahvistaminen, omien tietojen valvonnan parantaminen, oikeus tulla unohdetuksi, tietoon perustuvan vapaaehtoinen suostumus käsitteen selventäminen ja geneettisen tiedon lisääminen arkaluonteisena suojattaviin tietoihin.[288]

European Digital Rights[289] huomautti, että rekisteröidyt voivat väsyä tietoturvaloukkauksista tehtäviin ilmoituksiin. Näin on jo tapahtunut Yhdysvalloissa, jossa rekisterinpitäjille on säädetty velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista. Tämän vuoksi EDRi suositteli, että ilmoitusvelvollisuus rajattaisiin tapauksiin, joissa tietoturvaloukkauksilla on todennäköisesti vakavia tai haitallisia vaikutuksia.[290] European Digital Rights ehdotti lisäksi, että valvova viranomainen pitäisi julkista rekisteriä tietoturvaloukkausilmoituksista. Vaatimusta EDRi perusteli siten, että julkisen rekisterin ylläpitäminen edesasuttaa yleistä keskustelua tietoturvasta.[291] EDRi:n mukaan hallinnollisten

[285] HaVL 22/2014 vp–U 21/2012 vp, s. 3.
[286] HaVL 11/2012 vp–U 21/2012 vp, s. 5.
[287] Saarenpään 2016, s. 246–247 mukaan informaatio-oikeuden alalla intressitahot ovat tyypillisesti olleet ensisijaisesti ajaneet taloudellisia etuja. Näiden tahojen vastapainoksi on vähitellen muotoutunut vahtikoira- eli watchdog –järjestöjä, jotka ovat osa kansalaisjärjestöjen kehitystä kansalaisyhteiskunnassa. Näiden järjestöjen syntymiseen ovat vaikuttanut informaatio-oikeuden kehittymättömät lainvalmistelutavat. Informaatio-oikeuden alalla tärkeitä vahtikoirajärjestöjä ovat esimerkiksi Privacy International, Electronic Privacy Information Center (EPIC) ja Electronic Frontier Foundation (EFF). Vahtikoirajärjestöjen tuottama aineisto on oikeuslähdeopillisesti tärkeä informaatio-oikeuden alan tutkimukselle.
[288] Saatavissa: http://www.statewatch.org/news/2010/oct/05eu-dp-com.htm (Katsottu 3.4.2016).
[289] Electronic Frontier Finland ry (Effi) on yksi European Digital Rightsin (EDRi) perustajajäsenistä. Saatavissa: https://effi.org/ (Katsottu 3.4.2016).
[290] European Digital Rights. Article 32 – Communication of a personal data breach to the data subject, Commission Proposal. Saatavissa: http://protectmydata.eu/articles/articles-31-40/article-32/ (Katsottu 10.8.2015).
[291] Saatavissa: http://protectmydata.eu/articles/articles-31-40/article-31/ (Katsottu 20.12.2015).

sanktioiden määrää tulisi vähentää komission esittämästä kolmesta luokasta, koska se antaisi tietosuojaviranomaisille enemmän harkintavaltaa.[292]

Privacy International piti tervetulleena tietosuoja-asetusehdotuksen sisältämiä vastuullisuuden ja tilivelvollisuuden vaatimuksia rekisterinpitäjille. Myös velvollisuus ilmoittaa tietoturvaloukkauksista nähtiin tervetulleena uudistuksena.[293] Yhdysvaltalaiset toimijat vaikuttivat omien etujensa mukaisesti henkilötietodirektiivistä käytyihin keskusteluihin ja ovat myös vaikuttaneet tietosuoja-asetuksesta käytyyn keskusteluun. On arveltu, että Yhdysvaltain politiikkamieltymykset tulevat jatkossakin muokkaamaan tietosuojan todellista tasoa erityisesti online-maailman osalta.[294]

Eri intressiryhmät kritisoivat komission tietosuoja-asetusehdotusta siitä, että 31 artiklassa asetettu velvollisuus ilmoittaa valvontaviranomaiselle 24 tunnin kuluessa olisi ollut liian lyhyt. Tämä vaatimus oli tietoliikenneyhtiö Telefónican mukaan mielivaltainen ja perusteeton. Ilmoitus on Telefónican mukaan hyödyllinen vasta sen jälkeen, kun tietoturvaloukkauksen syy on teknisesti vahvistettu. Telefónican mukaan tämä ei yleensä ole mahdollista 24 tunnissa ja se voi haitata kriittistä tietoturvaloukkauksen korjaamista. Telefónica huomautti myös, ettei ilmoitusvelvollisuutta tulisi olla sellaisissa ns. kalastelutapauksissa[295], jossa henkilö vapaaehtoisesti antaa pääsyn henkilötietoihinsa petollisesti toimivalle kolmannelle osapuolelle.[296]

Myös American Chamber of Commerce (lyhenne: AmCham, Amerikan kauppakamari) piti 24 tunnin aikarajaa epärealistisena. American Chamber of Commerce:n mukaan rekisterinpitäjän tulisi tehdä ilmoitus valvontaviranomaiselle vasta sen jälkeen, kun rekisterinpitäjä on riittävällä varmuudella varmistanut, että kyseessä on henkilötietoihin

---

[292] EDRi: Comments on the draft JURI opinion on the General Data Protection Regulation, s. 33. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/blob/master/raw/lobby-documents/EDRis-comments-on-the-JURI-draft-opinion-on-the-general-data-protection-regulation.pdf (Katsottu 3.4.2016).

[293] Privacy International. Our analysis of the European Comission's proposal for a general Data Protection Regulation. Saatavissa: https://www.privacyinternational.org/node/181. (Katsottu 3.4.2016).

[294] Bygrave 2014, s. 107.

[295] Andreassonin et al. 2014a, s. 28 mukaan *kalastelulla* tarkoitetaan huijausviestejä, jotka liikkuvat esimerkiksi sosiaalisen median ja sähköpostin välityksellä. Suomessa uutisoitiin laajasti vuonna 2014 huijausviesteistä, jotka lähetettiin Verohallinnon ja Tullin nimissä useille suomalaisille internetin käyttäjille. Verohallinnon nimissä lähetetyt viestit liittyivät veronpalautuksiin. Tullin nimissä vastaanottajilta kysyttiin pankkitunnuksia väärennetyllä tullattavan lähetyksen vastaanottoilmoituksella.

[296] Telefónica's proposed amendments to the Proposal for a REGULATION 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 Directive), s. 40. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Telefonica-Amendments-on-GDPR-Proposal.pdf (Katsottu 14.11.2015).

kohdistuva tietoturvaloukkaus. Ilmoitusta ei American Chamber of Commerce:n muutosehdotuksessa vaadittaisi siis tehtäväksi heti tapahtuman jälkeen. Lisäksi 24 tunnin aikaraja voi haitata asian tutkintaa ja saattaa hätäännyttää kuluttajia. Ensiarvoisen tärkeää oli American Chamber of Commerce:n mukaan tutkia tietoturvaloukkaus ja tehdä tarkoituksenmukaiset toimenpiteet kuluttajille aiheutuvien menetysten ja vahinkojen minimoimiseksi.[297]

Internetissä toimiva huutokauppayhtiö eBay ehdotti komission tietosuoja-asetusehdotusta muutettavaksi siten, että rekisterinpitäjän tulisi tehdä valvontaviranomaiselle ilmoitus tietoturvaloukkauksesta *kohtuullisessa ajassa* siitä, kun rekisterinpitäjä on saanut tiedon tietoturvaloukkauksen tapahtumisesta.[298]

Eri intressiryhmät ilmaisivat myös huolensa siitä, että komission tietosuoja-asetusehdotuksen mukainen ilmoitusvelvollisuus tulisi kuormittamaan viranomais-resursseja. Telefónican mukaan valvontaviranomaisilla ei ole riittävästi resursseja käsitellä ilmoituksia, mikä tulisi halvaannuttamaan toimivaltaiset viranomaiset. Lisäksi Telefónica huomautti, että ilmoitusvelvollisuus asettaisi eurooppalaisille yrityksille huomattavan taakan. Käytännöllisempänä lähestymistapana Telefónica piti sitä, että yrityksissä kirjataan kaikki käsittelytapahtumat ja nämä tiedot ovat valvontaviranomaisten tarkastettavissa milloin tahansa, mutta ainoastaan vakavammista tapauksista tulisi ilmoittaa valvontaviranomaiselle kohtuullisen ajan kuluessa. Myös Facebook epäili, ettei valvontaviranomaisilla ehkä ole riittäviä resursseja ilmoitusten nopeaa käsittelyä varten, mikä heikentää valvontaviranomaisten tehokkuutta ja luottamusta valvontaviranomaisten rooliin sen varmistamisessa, että rekisterinpitäjät käsittelevät asianmukaisesti henkilötietoihin kohdistuvat tietoturvaloukkaukset.[299]

Facebook huomautti kannanotossaan, että velvollisuus ilmoittaa jopa vähäisemmistä tietoturvaloukkauksista valvontaviranomaiselle on tietosuoja-asetusehdotuksessa ehdo-

---

[297] AmCham EU Proposed Amendments on the General Data Protection Regulation, s.89. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/AmCham_EU_Proposed_Amendments_on_Data_Protection.pdf (Katsottu 14.11.2015).

[298] eBay Inc. position Industry, Research and Energy Committee draft opinion on the General Data Protection Regulation, s. 7. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Position-paper_eBay-Inc_ITRE-opinion-on-data-protection-regulation.pdf (Katsottu 15.11.2015).

[299] Comments from Facebook on the European Commission's proposal for a Regulation "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)", s. 9. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Facebook.pdf (Katsottu 14.11.2015).

ton vaatimus. Facebook huomautti, että tämä ei mahdollista tehokasta priorisointia vakavampiin tapauksiin.[300]

Microsoft ja eBay ehdottivat omissa kannanotoissaan ilmoitusvelvollisuuden rajaamista siten, että ilmoitusta tietoturvaloukkauksesta ei tarvita, jos rekisterinpitäjä on ottanut käyttöönsä riittävät teknologiset toimenpiteet. Näiden teknisten toimenpiteiden avulla tieto muutetaan muotoon, joka ei ole sellaisen henkilön ymmärrettävissä, jolla ei ole lupaa käsitellä tietoja.[301]

Komission tietosuoja-asetusehdotuksen 32(3) artiklassa on määritelty ne tiedot, jotka on ilmoitettava rekisteröidylle tietoturvaloukkauksesta tehtävässä ilmoituksessa. Facebookin mukaan rekisteröidylle tehtävään ilmoitukseen on liitettävä liian paljon tietoa. Facebook piti myös tietosuoja-asetusehdotuksen mukaista aikarajaa (*ilman aiheetonta viivytystä*) liian lyhyenä. Facebookin mukaan tietoturvaloukkausta ei ole tietosuoja-asetusehdotuksessa määritelty tarkasti.[302] eBay ehdotti, ettei ilmoitusta tarvitsisi tehdä rekisteröidylle, jos ilmoituksen tekeminen olisi tosiasiallisesti mahdotonta tai vaatisi rekisterinpitäjältä kohtuutonta vaivaa.[303]

7.8 Hallinnolliset seuraamukset

Tietosuoja-asetukseen tulee sisältymään säännöksiä hallinnollisten seuraamusten määräämisestä.[304] Komission tietosuoja-asetusehdotuksessa seuraamusmaksut olivat huomattavan korkeat ja tämä saikin yritykset reagoimaan asetusehdotuksen valmisteluun. Seuraamusmaksujen suuruus on yksi syy suureen määrään muutoksia, joita asetusehdo-

---

[300] Comments from Facebook on the European Commission's proposal for a Regulation "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)", s. 9. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Facebook.pdf (Katsottu 14.11.2015).

[301] eBay Inc. position Industry, Research and Energy Committee draft opinion on the General Data Protection Regulation, s. 7. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Position-paper_eBay-Inc_ITRE-opinion-on-data-protection-regulation.pdf (Katsottu 15.11.2015);
Microsoft positions and suggestions for the draft General Data Protection Regulation, s. 20. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Microsoft.docx (Katsottu 15.11.2015).

[302] Comments from Facebook on the European Commission's proposal for a Regulation "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)", s. 9. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Facebook.pdf (Katsottu 14.11.2015).

[303] eBay Inc. position Industry, Research and Energy Committee draft opinion on the General Data Protection Regulation, s. 9. Saatavissa: https://github.com/lobbyplag/lobbyplag-data/raw/master/raw/lobby-documents/Position-paper_eBay-Inc_ITRE-opinion-on-data-protection-regulation.pdf (Katsottu 15.11.2015).

[304] HaVL 25/2015 vp., s. 7.

tukseen on tehty.[305] On ennakoitu, että valvontaviranomaiset tulevat panostamaan resursseja tapauksiin, joissa rikkomukset ovat suuria. Todennäköisesti valvovat viranomaiset puuttuvat ensisijaisesti niihin tapauksiin, joissa haittaa aiheutuu merkittävälle määrälle yksilöitä. Nämä tapaukset kannustavat muita rekisterinpitäjiä noudattamaan tietosuoja-asetuksen niille asettamia vaatimuksia.[306]

Seuraamukset on sisällytetty tietosuoja-asetuksen VIII lukuun, jossa säädetään seuraamusten lisäksi myös oikeussuojakeinoista ja vastuista[307]. Hallinnolliset seuraamukset on 79 artiklassa[308] jaettu kahteen tasoon. Pienemmistä rikkomuksista voidaan asettaa suuruudeltaan enintään 10 miljoonan euron sakon tai 2 prosenttia vuotuisesta maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi on suurempi.[309] Tietoturvallisuutta koskevien artiklojen 30–32 vastainen toiminta on sanktioitu tämän lievemmän luokan mukaisesti. Vakavammista rikkomuksista voidaan asettaa korkeampi sakko, ja enimmäissakko on tällöin 20 miljoonaa euroa tai 4 prosenttia vuotuisesta maailmanlaajuisesta liikevaihdosta sen mukaan, kumpi on suurempi.[310] Sakkoja voidaan määrätä tämän korkeamman sanktioluokan mukaisesti esimerkiksi jos rekisterinpitäjä toimii tietosuoja-asetuksen 5 artiklassa säädettyjen henkilötietojen käsittelyä koskevien periaatteiden vastaisesti. Henkilötietojen siirto 41 artiklan säätelemän tietosuojan riittävyyttä koskevan päätöksen perusteella on myös sanktioitu korkeamman kategorian mukaisesti. [311]

[305] Fritsch 2015, s. 164.
[306] Kuner 2013, s. 155.
[307] Henkilötietodirektiivin 24 artiklassa asetetaan jäsenmaille velvollisuus toteuttaa ”tarvittavat toimenpiteet tämän direktiivin säännösten täydellisen soveltamisen varmistamiseksi ja määriteltävä erityisesti sanktiot, joita sovelletaan tämän direktiivin mukaisesti säädettyjen säännösten rikkomistapauksissa.” HetiL 48 § sisältää rangaistussäännökset ja täyttää siten osaltaan direktiivin artiklassa 24 asetettua velvollisuutta. HetiL 48.1 § sisältää viittaussäännöksen RL 38 lukuun tieto- ja viestintärikoksista ja 40 lukuun virkarikoksista. Henkilötietorekisteririkos on säädetty rangaistavaksi RL 38:9:ssä, henkilörekisteriin kohdistuva tietomurto RL 38:8:ssa. HetiL 33 §:ssä säädetyn vaitiolovelvollisuuden rikkomisesta on säädetty rangaistus RL 32:1:sessä. Virkasalaisuuden rikkomisesta on säädetty RL 40:5.1 ja tuottamuksellisesta virkasalaisuuden rikkomisesta RL 40:5.2:sessa. Tietosuojavaltuutetun toimisto on laatinut oppaan henkilötietolain seuraamusjärjestelmästä. Opas on saatavissa osoitteessa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/6JfprbX39/Henkilotietolain_seuraamusjarjestelma.pdf (Katsottu 3.10.2015).
[308] kolmikantaneuvotteluissa hyväksytyn ehdotuksen mukaan
[309] Kolmikantaneuvotteluissa hyväksytyn ehdotuksen 79(3a) artiklan mukaisesti
[310] Kolmikantaneuvotteluissa hyväksytyn ehdotuksen 79(3a, uusi) artiklan kohdan mukaisesti. Saatavissa: http://data.consilium.europa.eu/doc/document/ST-5455-2016-INIT/fi/pdf (Katsottu 21.2.2016). Esimerkkinä voidaan todeta, että 4 prosenttia vuotuisesta maailmanlaajuisesta liikevaihdosta vastaa Walmartin osalta 20 miljardia dollaria ja Samsungin osalta 10 miljardia dollaria. On oletettavaa, etteivät sakot ensimmäisinä vuosina nouse miljardin suuruusluokkaan. Raesteen 2016 mukaan Suomen osalta kaupan keskusliikkeillä 4 % tarkoittaa satoja miljoonia euroja.
[311] Kolmikantaneuvotteluissa hyväksytyn ehdotuksen 79(3a, uusi) artiklan ba- kohta.

Valmistelun aikana seuraamusten suuruus on muuttunut merkittävästi. Komission ehdotuksessa tietosuoja-asetukseksi seuraamukset oli porrastettu kolmeen tasoon. Ensimmäisessä tasossa enimmäissakko oli enintään 250 000 €, tai jos kyseessä oli yritys, 0,5 prosenttia sen vuotuisesta maailmanlaajuisesta liikevaihdosta. Vakavammista rikkomuksista olisi tullut määrät enintään 500 000 €:n sakko tai jos kyseessä oli yritys, 1 prosentti sen vuotuisesta maailmanlaajuisesta liikevaihdosta. Kaikkein vakavimmista rikkomuksista valvontaviranomaisen olisi tullut komission ehdotuksen mukaan määrätä 1 000 000 €:n sakko tai jos kyseessä oli yritys, 2 prosentti sen vuotuisesta maailmanlaajuisesta liikevaihdosta. Tietoturvaloukkauksesta hälyttämisen laiminlyönti viranomaiselle tai rekisteröidylle kuului komission ehdotuksessa tähän ankarimmin sanktioituun luokkaan.

Sakon suuruus määräytyy tietosuoja-asetuksen 79 artiklan mukaan kunkin yksittäisen tapauksen olosuhteiden mukaisesti. Suuruutta arvioitaessa on otettava asianmukaisesti huomioon[312]:

- *henkilötietoryhmät, joihin rikkominen vaikuttaa*;[313]
- *hyväksyttyjen käytännesääntöjen tai hyväksyttyjen (…) sertifiointimekanismien noudattaminen;*
- *jos kyseiselle rekisterinpitäjälle tai henkilötietojen käsittelijälle on aikaisemmin määrätty samasta asiasta toimenpiteitä, näiden toimenpiteiden noudattaminen;*
- *rekisterinpitäjän tai henkilötietojen käsittelijän mahdolliset aiemmat vastaavat rikkomiset;*
- *rekisterinpitäjän tai henkilötietojen käsittelijän toteuttamat toimet rekisteröidyille aiheutuneen vahingon lieventämiseksi;*
- *rekisterinpitäjän tai henkilötietojen käsittelijän vastuun aste, ottaen huomioon heidän (…)toteuttamansa tekniset ja organisatoriset toimenpiteet;*
- *rikkomisen luonne, vakavuus ja kesto, kyseisen tietojenkäsittelyn luonne, laajuus ja tarkoitus huomioon ottaen, sekä niiden rekisteröityjen lukumäärä, joihin rikkominen vaikuttaa, ja heille aiheutuneen vahingon suuruus;*
- *rikkomisen tahallisuus tai tuottamuksellisuus;*
- *tapa, jolla rikkominen tuli valvontaviranomaisen tietoon, erityisesti se, ilmoittiko rekisterinpitäjä tai henkilötietojen käsittelijä rikkomisesta ja missä laajuudessa;*

[312] Kolmikantaneuvotteluiden 79(2a) artikla, joka hyväksyttiin vähäisin muutoksin kolmikantaneuvotteluissa.
[313] Kolmikantaneuvotteluissa tehty lisäys niihin seikkoihin, jotka sakon suuruutta määrättäessä voidaan huomioida.

- *yhteistyön aste valvontaviranomaisen kanssa rikkomisen korjaamiseksi ja sen mahdollisten haittavaikutusten lieventämiseksi;*[314]

- *mahdolliset muut tapaukseen sovellettavat raskauttavat tai lieventävät tekijät* (esim. rikkomisesta suoraan tai välillisesti saadut mahdolliset taloudelliset edut).

Valvontaviranomaisen ei ole pakko määrätä asetuksen noudattamatta jättämisestä sakkoja. Tietosuoja-asetuksen johdanto-osassa[315] todetaan, että sakon sijasta voidaan antaa huomautus, jos asetusten säännösten rikkominen on ollut vähäistä[316] tai sakko olisi luonnolliselle henkilölle kohtuuton rasitus.

7.9 WP 29:n kannanotto 03/2014 henkilötietojen tietoturvaloukkauksiin

Tietosuojatyöryhmä WP 29 on käsitellyt henkilötietojen tietoturvaloukkauksia kannanotossaan 03/2014. Yhteenvedossa todetaan, että kyseistä kannanottoa voidaan soveltaa myös tietosuoja-asetusehdotukseen, vaikka mielipide käsitteleekin direktiiviä 2002/58/EY[317]. Henkilötietojen tietoturvaloukkauksen yhteydessä on WP 29:n mukaan huomioitava esimerkiksi se, onko tieto ollut salattu. Jos salattuun henkilötietoon kohdistuu tietoturvaloukkaus, on huomioitava lisäksi, onko tiedosta olemassa varmuuskopio ja toisaalta myös se, ovatko salausavaimet säilyneet koskemattomina. Myös salauksen tasolla on merkitystä arvioitaessa ilmoittamisvelvollisuuskynnyksen ylittymistä.

Yhtenä esimerkkinä kuvataan tapaus[318], jossa useita kannettavia tietokoneita on varastettu lasten terveydenhoitoyksiköstä. Jos nämä tiedot olisivat olleet salattuja ja palautettavissa varmuuskopioista, tapauksesta ei olisi tarvinnut ilmoittaa vanhemmille. Jos taas tiedot eivät olisi salattuja tai niistä ei olisi varmuuskopioita, olisi vanhemmille tullut ilmoittaa tietoturvaloukkauksesta. Korjaaviin toimenpiteisiin voidaan ryhtyä tietojen uudelleen keräämiseksi esimerkiksi tekemällä tarvittavia lääketieteellisiä testejä ja kartoittamalla tunnettuja terveystekijöitä kuten allergioita.

---

[314] Kolmikantaneuvotteluissa tehty lisäys niihin seikkoihin, jotka sakon suuruutta määrättäessä voidaan huomioida.
[315] Kolmikantaneuvotteluissa hyväksytty (OSA-neuvoston ehdotuksen mukainen) johdanto-osan 118b –kohta.
[316] U 21/2012 vp HaV 03.06.2015 emeritusprofessori Ahti Saarenpää, s. 6 pitää tätä lisäystä onnistuneena sillä varauksella, että ”huomautus aidosti ymmärretään sanktioksi”. Määrällisesti korkeat rahamääräiset hallinnolliset seuraamukset ovat Suomen näkökulmasta uusia. Saarenpään mukaan sanktiot voivat kuitenkin olla perusteltuja, sillä ”riittävän nopeasti asetettavien tehokkaiden sanktioiden puute heikentää nykyisin henkilötietojen suojan toimivuutta”.
Saatavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2015-AK-5174.pdf (Katsottu 13.12.2015).
[317] WP 29:n kannanotto 03/2014: Opinion 03/2014 on Personal Data Breach, s. 3.
[318] Ibid., s. 5.

WP 03/2014 esittelee kannanotossaan myös luottokortteihin liittyvän tapauksen[319], jossa luottokorttikuitteja sisältävä kirjekuori heitetään roskakoriin. Kirjekuori päättyy sivullisen käsiin. Luottokorttikuiteista oli luettavissa kortin koko numero ja allekirjoitukset. Tässä tapauksessa on mahdollista, että rekisteröidylle aiheutuu taloudellista vahinkoa, jos korttitiedot ovat voimassa ja niitä käytetään väärin. Tapaus vaikuttaa todennäköisesti vahingollisesti rekisteröityyn ja rekisteröidylle tulisi ilmoittaa tapauksesta. On mahdollista, ettei tarkkaan tiedetä, mitkä kuitit olivat kirjekuoressa. Tällöin kaupan tulisi ilmoittaa tapauksesta korttimaksun käsittelijälle, jolloin käsittelijä voi seurata mahdollisia maksuvälinepetoksia. Jos kauppa toimii lähinnä paikallisesti, riittävää voi olla ilmoitus paikallisessa sanomalehdessä. Tarpeen voi olla myös tehdä ilmoitus luottokorttiyhtiölle. Jos kirjekuori saadaan palautettua avaamattomana rekisterinpitäjälle, on epätodennäköistä, että se vaikuttaisi haitallisesti rekisteröityihin ja siksi ilmoitusta rekisteröidylle ei vaadittaisi. Esimerkkinä asianmukaisista etukäteisistä suojautumiskeinosta mainitaan työntekijöiden kouluttaminen rikkomusten varalta, asianmukaisten toimistosilppureiden tai silppuripalveluiden käyttö kuittien tuhoamiseen. Lisäksi tulisi käyttää maksupäätelaitteita, jotka eivät sisällytä kuitteihin täydellisiä luottokorttitietoja.

[319] WP 29:n kannanotto 03/2014: Opinion 03/2014 on Personal Data Breach, s. 9.

8 ULKOMAISESTA TIETOSUOJALAINSÄÄDÄNNÖSTÄ

8.1 Ruotsi

Ruotsin hallitusmuodossa (*regeringsform* SFS 1974:152) säädetään, miten valta jaetaan eduskunnan, hallituksen, kuntien, maakäräjien ja tuomioistuinten kesken.[320] Ruotsin hallitusmuodon 2.4 §:ssä säädetään, että julkisen vallan on suojattava yksityiselämää ja perhe-elämää.[321]

Ruotsissa hyväksyttiin henkilötietojen suojaa säätelevä laki 1973.[322] *Datalagen* (1973:289) oli maailman ensimmäinen koko valtiota koskenut yleislaki.[323] Alun perin lain valmistelun oletuksena oli, että tietokoneistettuja henkilötietoja sisältäviä tiedostoja oli noin 4000. Tämän määrän arvioitiin kasvavan 500:lla vuosittain. Yksityisen sektorin odotettiin muodostavan 90 % kasvusta.[324] Tämän arvion perusteella lain ensimmäiseen versioon tehtiin vaatimus luvanvaraisuudesta: rekisterinpitäjän tuli hakea rekisterinpitämistä varten lupa tietosuojalautakunnalta.[325]

Ruotsin henkilötietolaki (*Personuppgiftslag* (1998:204), lyhenne: PuL tai PUL) pani täytäntöön EU:n henkilötietodirektiivin 95/46/EY ja korvasi vuoden 1973 lain.[326] PuL:n 30 § säätelee tietoturvallisuudesta henkilötietojen käsittelyssä. Hallitus tai hallituksen määräämä viranomainen[327] voi PuL 50 § b kohdan mukaan antaa tarkempia määräyksiä rekisterinpitäjälle henkilötietojen käsittelystä.

---

[320] Sveriges fyra grundlagar. Studiematerial från riksdagen, s. 3. Saatavissa: http://www.riksdagen.se/PageFiles/dokument/bestall/svenska/Sveriges_fyra_grundlagar.pdf (Katsottu 4.10.2015).

[321] Sveriges fyra grundlagar. Studiematerial från riksdagen, s. 3: Ruotsin perustuslaki koostuu neljästä laista: hallitusmuoto (regeringsformen 1974:152), painovapausasetus (tryckfrihetsförordningen 1949:105), ilmaisunvapausperustuslaki (yttrandefrihetsgrundlagen 1991:1469) ja kruununperimysjärjestys (successionsordningen, 1988:1489).
Saatavissa: http://www.riksdagen.se/PageFiles/dokument/bestall/svenska/Sveriges_fyra_grundlagar.pdf (Katsottu 4.10.2015).

[322] Seipel 2001, s. 116.

[323] Korhonen s. 2003, s. 112. Kiss & Szőke 2015, s. 313 toteavat, että Saksan Hessenin osavaltiolaki vuodelta 1970 toimi esikuvana monille länsieurooppalaisille laeille (myös Saksalle 1976, Norjalle, Tanskalle ja Ranskalle 1978). 1970-luvulla säädettyjä tietosuojalakeja kutsutaan ensimmäisen sukupolven tietosuojalaeiksi.

[324] Förslaget till datalag Prop. 1973:33, s. 50. Saatavissa: http://data.riksdagen.se/dokument/FW0333 (Katsottu 31.7.2015).

[325] Seipel 2001, s. 117.

[326] LUOTI 4/2006, s. 98. Saman lähteen mukaan manuaalisten rekisterien osalta vanha laki säilyi voimassa vuoteen 2007 asti.

[327] Toisin sanoen tässä tarkoitetaan tietosuojaviranomaista, Öman & Lindblom 2011, s. 436.

Ruotsin tietosuojaviranomainen (Datainspektionen) on julkaissut ohjeen turvallisuusasioista henkilötietojen käsittelyssä.[328] Ruotsin henkilötietolain 30.1 §:ssä on vaatimus siitä, että rekisterinpitäjän ja hänen lukuunsa toimivan välillä täytyy olla kirjallinen sopimus. Ruotsin henkilötietolain 31 §:ssä säädetään riittävistä teknisistä ja organisatorisista toimenpiteistä. Suhteellisuusperiaatteen mukaisesti 31 § määrittelee, että riittävyyttä arvioitaessa huomioon on otettava tekniset ratkaisut, kustannukset, erityiset riskit liittyen henkilötietojen käsittelyyn sekä se kuinka arkaluonteisista tiedoista on kyse. Ruotsin henkilötietolain 31.2 §:ssä määritellään rekisterinpitäjän viimekätinen vastuu: rekisterinpitäjän tulee huolehtia siitä, että henkilötietojen käsittelijä noudattaa turvallisuusjärjestelyitä. Näistä asioista on sovittava kirjallisesti.

Henkilötietolain rekisterinpitäjää vastaa sisällöllisesti Ruotsin henkilötietolaissa *personuppgiftsansvarig*[329], joka on määritelty Ruotsin henkilötietolain 3 §:ssä. Rekisterinpitäjä on yleensä oikeushenkilö (esimerkiksi yhtiö, säätiö tai yhdistys) tai viranomainen, joka käsittelee henkilötietoja toiminnassaan ja joka päättää siitä, mihin tarkoitukseen tietoja käytetään.[330]

Henkilötietojen käsittelijää vastaava käsite on Ruotsin henkilötietolain 3 §:ssä määritelty *personuppgiftsbiträde*.[331] Henkilötietojen käsittelijä käsittelee tietoja rekisterinpitäjän lukuun. Ruotsin tietosuojaviranomaisen mukaan henkilötietojen käsittelijä toimii aina organisaation ulkopuolella. Tietojen käsittelijä voi olla juridinen tai luonnollinen henkilö.[332]

Ruotsin nykyistä henkilötietolakia on kritisoitu siitä, että sitä on hankala soveltaa pilvipalveluihin. Voimassa oleva laki ja direktiivi, johon se perustuu, pohjautuvat ajatukseen

[328] LUOTI 4/2006, s. 99. Ohjeistus on saatavissa: https://www.datainspektionen.se/Documents/faktabroschyr-allmannarad-sakerhet.pdf (Katsottu 13.9.2015).
[329] Suomeksi ”Henkilötiedoista vastuussa oleva.”
[330] Datainspektionen.se: Lagar & Regler. Saatavissa: http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/ (Katsottu 3.8.2015).
[331] Suomeksi ”Henkilötietoja käsittelevä avustaja.”
[332] Datainspektionen.se: Lagar & Regler. Saatavissa: http://www.datainspektionen.se/lagar-och-regler/personuppgiftslagen/personuppgiftsansvarig/ (Katsottu 3.8.2015).

vahvasta ja kontrolloivasta rekisterinpitäjästä. Tällainen rekisterinpitäjä pystyy tosiasiallisesti ohjaamaan ja kontrolloimaan henkilötietojen käsittelijän toimintaa.[333]

Ruotsin henkilötietolain 31.1 §:ssä säädetään, että rekisterinpitäjällä on velvollisuus huolehtia varotoimenpiteistä henkilötietoja käsiteltäessä. Toimenpiteillä on saavutettava asianmukainen turvallisuustaso, jota arvioitaessa voidaan huomioida tekniset mahdollisuudet, toimenpiteiden kustannukset[334], käsittelyyn liittyvät erityiset riskit sekä se, miten arkaluonteisia käsiteltävät henkilötiedot ovat.[335] Ruotsin henkilötietolain 13 §:ssä säädetään, ettei arkaluonteisten tietojen käsittely ole pääsääntöisesti sallittua. Arkaluonteisina tietoina pidetään muun muassa tietoa henkilön rodusta ja etnisestä alkuperästä, tietoa poliittisista mielipiteitä tai uskonnollisesta vakaumuksesta tai ammattiyhdistysliikkeeseen kuulumisesta.

Ruotsin henkilötietolain 31.2 §:n tavoite on varmistaa, että tietoturvan taso säilyy samana siinäkin tapauksessa, että rekisterinpitäjä on ulkoistanut henkilötietojen käsittelyn. Rekisterinpitäjän tulee valvoa henkilötietojen käsittelijän toimintaa. Rekisterinpitäjän on myös varmistettava, että henkilötietojen käsittelijä noudattaa turvallisuuskäytäntöjä.[336] Kun henkilötietojen käsittelijä käsittelee henkilötietoja rekisterinpitäjän lukuun, on siitä laadittava 30.2 §:n mukaan kirjallinen sopimus. Sopimuksessa on määriteltävä erityisesti se, että henkilötietojen käsittelijä saa käsitellä henkilötietoja ainoastaan rekisterinpitäjän ohjeiden mukaisesti.[337]

Ruotsissa ei ole asetettu rekisterinpitäjälle yleistä velvollisuutta ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista valvontaviranomaiselle. Rekisterinpitäjä ei myöskään ole Ruotsissa velvollinen ilmoittamaan tietoturvaloukkauksesta sellaiselle rekisteröidylle, jonka tietoihin tietoturvaloukkaus on kohdistunut. Ilmoitusvelvollisuus on kuitenkin asetettu yleisesti saatavilla olevien sähköisten viestintäpalveluiden tarjoajille.[338]

---

[333] Svantesson 2012, s. 477. Katso myös Svantessonin kommentoima Ruotsin tietosuojavaltuutetun päätös Tillsyn enligt personuppgiftslagen (1998:204) –Salems kommunstyrelse, s. 10. Saatavissa: https://www.datainspektionen.se/Documents/beslut/2011-09-30-salems-kommun.pdf (Katsottu 4.8.2015).

[334] Öman & Lindblom 2011, s. 439 huomauttaa, että toimenpiteiden ei siis tarvitse olla kaikkein parhaimpia, jos se tulisi liian kalliiksi.

[335] Öman & Lindblom 2011, s. 436.

[336] Öman & Lindblom 2011, s. 441.

[337] Öman & Lindblom 2011, s. 442.

[338] Global Guide to Data Breach Notifications, 2013, s. 107.

8.2 Norja

Toukokuussa 2014 Norjan perustuslakiin (*Grunnlov (LOV-1814-05-17*) lisättiin 102 §, joka säätelee yksityisyyden suojasta.[339] Aiemmin Norjan perustuslaki oli poikennut sisällöllisesti Suomen ja Ruotsin perustuslaeista, sillä se ei sisältänyt nimenomaista yksityiselämän suojaa koskevaa määräystä. Tietoturvallisuutta ei ole Norjassa koottu yhteen lakiin.[340]

Norja oli ensimmäisiä maita, joissa säädettiin tietosuojasta. *Lov om personregistre (personregisterloven 1978:48)* hyväksyttiin 1978.[341] Laki kielsi yleisesti sellaiset henkilötietorekisterit, joita joko ylläpidettiin sähköisessä muodossa tai jotka sisälsivät tietyntyyppistä arkaluonteista tietoa. Suuri osa henkilörekistereistä vaati tuolloin tietosuojaviranomaisen luvan, jotta niitä voitiin pitää laillisina.[342] Personregisterloven käsitti yleissäännökset henkilötietojen käsittelystä.[343] Personregisterloven ei sisältänyt kappaletta lain tavoitteesta.[344]

Vuoden 2001 laki *Lov om behandling av personopplysninger (LOV-2000-04-14-31) (personopplysningsloven)* korvasi personregisterloven -lain. Personopplysningsloven on toissijainen yleislaki, jota sovelletaan kaikkeen henkilötietojen käsittelyyn, ellei muussa laissa ole asiasta täsmällisesti säädetty.[345] Tietosuojalakia täydentää tietosuoja-asetus *(Forskrift om behandling av personopplysninger (FOR-2000-12-15-1265) (personopplysningsforskriften))*.[346] Henkilötietodirektiivin mukaisesti Norjan henkilötietolaissa säädetään tietoturvallisuudesta. Vastaavaa säädöstä ei ollut aiemmassa laissa.[347]

Norjan tietosuoja-asetuksen 2–6 §:ssä säädetään rekisterinpitäjän velvollisuudesta ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista. Tietosuojaviranomaiselle

---

Saatavissa: https://iapp.org/media/pdf/knowledge_center/WLG_Global_Data_Breach_Guide.pdf (Katsottu 16.11.2015).

[339] Hva er personvern? Saatavissa: https://www.datatilsynet.no/personvern/Hva-er-personvern/ (Katsottu 22.11.2015).

[340] LUOTI-julkaisu 4/2006, s. 108. Saarenpää & Pöysti et al. 1997, s. lx toteavat, että vuonna 1990 Norjassa asetettiin komitea laatimaan ehdotus yleiseksi tietoturvallisuuslaiksi. Komitean mukaan ”joihinkin yksityisiä, valtionhallintoa sekä valtion sisäistä ja ulkoista turvallisuutta koskeviin tietoihin kohdistui niin tärkeitä intressejä, että näiden tietojen suojaamisesta tulisi säätää lailla.” Ehdotus sai osakseen ankaraa kritiikiä, eikä ehdotus johtanut lain säätämiseen. Ehdotus johti kuitenkin siihen, että vuodesta 1996 alkaen Norjassa on ollut käytössä oma salausjärjestelmä ”Norsk Krypto System”, joka on kehitetty Norjassa.

[341] Schartum, 2001, s. 79.

[342] Schartum, 2001, s. 80.

[343] Wiik Johansen et al. 2001, s. 22.

[344] Wiik Johansen et al. 2001, s. 55.

[345] Schartum 2001, s. 94.

[346] Tietosuoja-asetuksen 2 luvussa (2-1 §- 2-16 §) säädetään tietoturvallisuudesta.

[347] Wiik Johansen et al. 2001, s. 51.

on 2–6 §:n 3 momentin mukaan ilmoitettava, jos on paljastettu henkilötietoja, joiden luottamuksellisuus on välttämätöntä.

Norjan tietosuojaviranomainen (Datatilsynet) ohjeistaa ilmoittamaan myös niille rekisteröidyille, joiden henkilötietoihin on kohdistunut tietoturvaloukkaus. Ilmoitus tulee tietosuojavaltuutetun mukaan tehdä heti, kun tapauksen arviointi on tehty. Lainvalvontaviranomaisia on tärkeää konsultoida ennen ilmoituksen tekemistä, sillä ilmoitukset voivat vaikuttaa tutkintaan. Norjan tietosuojaviranomainen täsmentää, että ilmoituksen tekemistä on siirrettävä myöhemmäksi, jos ilmoituksilla voi olla vaikutusta tapauksen tutkintaan.

Norjan tietosuojaviranomainen on ohjeistanut, mitä tietoja ilmoituksen tulee sisältää. Ilmoituksen sisältö riippuu yksittäisen tapauksen luonteesta ja valitusta ilmoitusmenetelmästä. Pääsääntöisesti ilmoitukseen tulee sisältyä:

- kuvaus, mitä on tapahtunut ja milloin
- tieto, keitä tapaus koskee
- yleiskuvaus, mitä yritys on tehnyt hallitakseen ja pienentääkseen vahinkoa sekä
- mitä toimenpiteitä on tehty vahinkojen korjaamiseksi.[348]

Norjan tietosuojaviranomainen neuvoo, että tietoturvaloukkauksen yhteydessä yritysten on arvioitava, minkälaisista tiedoista on kyse sen määrittelemiseksi, mitä yrityksen on tehtävä, keiden on osallistuttava toimenpiteisiin ja minkälainen ilmoitus tietoturvaloukkauksesta on tehtävä. Esimerkkinä Norjan tietosuojaviranomainen mainitsee tapauksen, jossa varastettu kannettava tietokone sisältäisi salattua tietoa. Ilmoitusta ei tarvitse tehdä, jos tämä tietokone löydettäisiin ja varmistuttaisiin siitä, ettei tietoihin ole koskettu.[349]

Norjan tietosuojaviranomaisen mukaan yksi suurimmista uhkista tietoturvalle on tiedon leviäminen internetissä. Tiedot leviävät uskomattoman nopeasti ja aina on olemassa mahdollisuus, että joku on ladannut tai kopioinut sisältöä. Yritys ei voi koskaan olla täysin varma, että ei ole tapahtunut tiedon luvatonta levittämistä. Vaikka tiedot salataan

[348] Håndtering av personopplysninger på avveier: Vurdere omfanget av dette spesifikke bruddet på personvernet. Saatavissa: https://www.datatilsynet.no/Sikkerhet-internkontroll/ID-tyveri/Personopplysninger-pa-avveier---en-handlingsplan-for-virksomheter/#3 (Katsottu 16.11.2015).
[349] Håndtering av personopplysninger på avveier: Vurdere omfanget av dette spesifikke bruddet på personvernet: Varsle involverte parter. Saatavissa: https://www.datatilsynet.no/Sikkerhet-internkontroll/ID-tyveri/Personopplysninger-pa-avveier---en-handlingsplan-for-virksomheter/#2 (Katsottu 16.11.2015).

ennen kuin se joutuu vääriin käsiin, on mahdollista, että tiedon salaus on myöhemmin purettavissa.[350]

Rekisterinpitäjää vastaa norjalaisessa laissa käsite *behandlingsansvarlig*, joka on määritelty Norjan tietosuojalain 2 §:n 4 kohdassa. Henkilötietojen käsittelijää vastaa on norjalaisessa tietosuojalaissa *databehandler*, joka on määritelty lain 2 §:n 5 kohdassa.

Vaikka Norja ei ole EU:n jäsenmaa[351], vastaa sen kansallinen lainsäädäntö henkilötietodirektiivin vaatimuksia.[352] Norjan henkilötietolain suhteesta muihin lakeihin on säädetty Norjan henkilötietolain 5 §:ssä.

Tietoturvallisuudesta säädetään personopplysningslovenin toisen luvun 13 §:ssä.[353] Personopplysningslovenin 13.1 §:ssä asetetaan vaatimus tietojenkäsittelystä vastaavalle ja tietojen käsittelijälle huolehtia riittävästä tietoturvallisuuden tasosta. Vaadittava tietoturvallisuuden taso vaihtelee ja sen arvioinnissa onkin huomioitava tietoon kohdistuvat uhkat ja mahdolliset seuraukset uhkan realisoituessa. Arvioinnissa keskeisinä elementteinä ovat käsittelyn tarkoitus, henkilötietojen määrä sekä tietojen mahdollinen arkaluonteisuus.[354]

Teknisten, organisatoristen ja fyysisten suojautumiskeinojen lisäksi on perustettava toimintamallit tietoturvaloukkaustilanteita varten. Toimintamalleihin on sisällytettävä ohjeistus tietoturvaloukkauksen kuvaamiseksi ja raportoimiseksi. Toimintamalleissa on myös huomioitava tietoturvallisuuden jatkuva seuranta henkilötietojen käsittelyssä.[355]

Riittävä tietoturvallisuuden taso edellyttää Norjan henkilötietolain 13.2 §:n mukaan tietoturvallisuuteen liittyvää dokumentointia. Dokumentoinnin on kuvattava kaikki turvallisuustoimenpiteet ja vähintäänkin kuvattava menetelmät riskianalyysin toteuttamiseksi sekä tietoturvallisuusmenetelmien käyttöönotto ja seuranta. Dokumentointi on tärkeää,

---

[350] Håndtering av personopplysninger på avveier: Sette igang skadeopprettende tiltak. Saatavissa: https://www.datatilsynet.no/Sikkerhet-internkontroll/ID-tyveri/Personopplysninger-pa-avveier---en-handlingsplan-for-virksomheter/#4 (Katsottu 16.11.2015).

[351] Wiik Johansen et al. 2001, s. 54 toteaa, että vuosittain järjestetään pohjoismaisten tietosuojaviranomaisten kokous, johon osallistuvat Norjan lisäksi Tanska, Suomi, Islanti ja Ruotsi. Norja osallistuu WP 29-tietosuojatyöryhmän toimintaan tarkkailijan roolissa. Norjalla on myös edustaja OECD:n tietoturvallisuutta ja yksityisyyden suojaa käsittelevässä työryhmässä, joka kokoontuu kaksi kertaa vuodessa Pariisissa.

[352] Schartum, 2001, s. 110. LUOTI-julkaisun 4/2006, s. 111 mukaan poikkeuksen EU-direktiivistä tekee lain 21 §, joka säätelee henkilöprofiilien käyttöä.

[353] LUOTI-julkaisussa 4/2006, s. 112 todetaan, että tietoturvallisuudesta on säädelty tässä pykälässä seikkaperäisemmin kuin EU-direktiivissä, johon pykälä perustuu.

[354] Wiik Johansen et al. 2001, s. 130.

[355] Wiik Johansen et al. 2001, s. 132.

koska kaikkien henkilötietoja käsittelevien on oltava tietoisia niistä turvallisuussäännöistä, jotka liittyvät henkilötietojen käsittelyyn. Valvontaviranomainen (*Datatilsynet*) ja muutoksenhakuelin (*Personvernnemnda*) käyttävät dokumentointia sen arvioimiseksi, onko tietoturvallisuuden tasosta huolehdittu riittävällä tavalla.[356]

Norjan henkilötietolain 13.3 § asettaa tietojen käsittelijälle velvollisuuden huolehtia siitä, että kaikki, joilla on pääsy henkilötietoihin, noudattavat tietoturvallisuusvaatimuksia. Norjan henkilötietolain 15 §:ssä säädetään, että henkilötietojenkäsittelijä saa käsitellä henkilötietoja ainoastaan tavalla, josta on sovittu kirjallisesti rekisterinpitäjän kanssa. Rekisterinpitäjän kanssa tehtävässä sopimuksessa on 15.2 §:n mukaan sovittava siitä, että henkilötietojen käsittelijä sitoutuu 13 §:n mukaisiin toimenpiteisiin.

Kuninkaalle on Norjan henkilötietolain 13.4 §:ssä asetettu toimivalta antaa tarkempia säädöksiä tietoturvallisuudesta henkilötietojenkäsittelyssä.

Norja on Schengen-valtiona saanut osallistua EU:n tietosuoja-asetuksen valmisteluun. Norjan oikeusministeriö järjesti kuulemisen, jossa selvitettiin eri toimielinten näkemyksiä siitä, tuleeko EU: yleinen tietosuoja-asetus lisäämään yksilöiden suojaa henkilötietojen käsittelyssä sekä luottamusta verkkopalveluihin. Erityisesti selvitettiin mielipiteitä oikeudesta tietojen siirtämisen järjestelmästä toiseen (18 artikla), oikeudesta tulla unohdetuksi (17 artikla) ja lisäyksistä rekisteröityjen oikeuksiin (artiklat 11–15). Palautetta pyydettiin myös siitä, tuleeko tietosuoja-asetus muuttamaan toimialakohtaisia lakeja, jotka säätelevät henkilötietojen käsittelystä.[357]

Norjan tietosuojaviranomainen on seurannut tiiviisti EU:n tietosuoja-asetuksen valmistelua. Norjan tietosuojaviranomainen osallistui Norjan oikeusministeriön järjestämään kuulemiseen tietosuoja-asetusehdotuksesta. Tietosuojaviranomainen kannatti ajatusta siitä, että tietoturvaloukkauksesta on ilmoitettava 24 tunnin sisällä valvontaviranomaiselle (artikla 31) ja joissakin tapauksissa myös rekisteröidylle (artikla 32). Tietosuojavi-

[356] Wiik Johansen et al. 2001, s. 132.
[357] Høring - EU-kommisjonens forslag til nye personvernregler. Saatavissa: https://www.regjeringen.no/no/dokumenter/horing---eu-kommisjonens-forslag-til-nye/id679008/ (Katsottu 13.9.2015).

ranomainen esitti myös, että olisi selvitettävä, tulisiko valvontaviranomaisen kaikissa tapauksissa tehdä arviointi tietoturvaloukkauksesta ilmoittamisesta rekisteröidylle.[358]

8.3 Yhdysvallat

Oikeudellisena käsitteenä yksityisyys lähti 1800-luvun lopun yhdysvaltalaisesta oikeustieteestä. Yksityisyyskäsitettä kehitettiin erityisesti oikeuskäytännön kautta.[359] Yhdysvalloissa henkilötietojen suojasta ei yleensä puhuta erillisenä ilmiönä, vaan se luetaan osaksi yksityisyyttä.[360] Aiemmin Yhdysvalloilla oli merkittävä rooli kansainvälisessä keskustelussa liittyen yksityisyyteen. Tästä huolimatta muu maailma on seurannut lainsäädäntökehityksessään EU:n mallia.[361]

Vaikka Yhdysvaltojen perustuslaki ei nimenomaisesti mainitse yksityisyyttä, sisältyy siihen useita yksityisyyttä suojaavia säännöksiä. Ensimmäinen lisäys (First Amendment) suojelee tietyissä tapauksissa yksityisyyttä ja turvaa esimerkiksi oikeuden puhua anonyymisti. Neljäs lisäys (Fourth Amendment) turvaa kansalaisten oikeuden olla turvassa henkilöönsä, taloonsa, asiakirjoihinsa ja muuhun omaisuuteensa kohdistuvilta kohtuuttomilta etsinnöiltä ja takavarikoinneilta.[362] Yhdysvaltojen perustuslaissa ei ole erityisiä säännöksiä tietoturvallisuudesta tai tietosuojasta.[363]

Yhdysvalloissa lainsäädännössä henkilötietojen käsitettä ei ole määritelty johdonmukaisesti ja yhteneväisesti. Toisinaan lainsäädännöstä puuttuu erottelu käsitteiden ”tunnistettava” ja ”tunnistettavissa oleva” välillä. Henkilötietojen sijasta käytetään yleisesti ”per-

[358]Datatilsyn: Høringsuttalelse —EU-kommisjonens forslag til nye personvernregler, s. 6. Saatavissa: https://www.regjeringen.no/contentassets/082f55782d6e4d698f8571667f8ef20c/datatilsynet.pdf (Katsottu 13.9.2015).
[359] Saarenpää 2015, s. 230. Schwartz 2013, s. 1970 toteaa, että kansainvälinen keskustelu yksityisyydestä alkoi Samuel Warrenin ja Louis Brandeisin 1890 kirjoittamasta artikkelista.
[360] Saarenpää 2015, s. 232.
[361] Schwartz 2013, s. 1967–1968. EU:lla on ollut merkittävä rooli kansainvälisessä yksityisyyskeskusteluissa 1990-luvulta lähtien. Whitman 2006, s. 875–876 on tarkastellut yksityisyyskäsityksen arvopohjaa Euroopassa ja Yhdysvalloissa. Whitmanin mukaan eurooppalaiset ovat ylpeitä yksityisyyden ja perheelämän suojasta, jonka henkilötietodirektiivi ja EU:n perusoikeuskirja tarjoaa eurooppalaisille. Eurooppalaisen näkemyksen mukaan yksityisyyttä kunnioitetaan perusoikeutena. Eurooppalaisesta näkökulmasta katsottuna Yhdysvalloissa tällaista perusoikeus on joko heikko tai sitä ei ole olemassa.Toisaalta on huomattava, että myös arvomaailma eroaa huomattavasti. Yhdysvalloissa yksityisyys liittyy keskeisesti siihen, ettei valtio saa puuttua vapauksiin ja erityisesti kenenkään kotiin. Euroopassa yksityisyyskeskusteluun liittyvät kunniakysymykset, mikä eurooppalaisesta näkökulmasta näyttää puuttuvan yhdysvaltalaisesta yksityisyyskäsitteestä. Yhdysvaltalaisesta näkökulmasta katsottuna on vierasta, että valtio voi puuttua esimerkiksi lapselle annettavaan nimeen.
[362] Solove et al. 2006, s. 33.
[363] Saarenpää & Pöysti et al. 1997, s. 197.

sonally identifiabe information" –käsitettä, joka kattaa molemmat käsitteet "tunnistettu" ja "tunnistettavissa oleva."[364]

Yhdysvalloissa ei liittovaltiotason yleislakia, joka säätelisi henkilötietojen käsittelyä. Henkilötietojen käsittelyn sääntely perustuu Yhdysvalloissa sektorikohtaiseen erityissääntelyyn.[365] Yhdysvaltojen liittovaltiotason tietosuojalainsäädäntö on rajoitettu koskemaan julkista sektoria sekä muutamia arkaluonteisia aloja kuten terveydenhuolto ja pankkitoiminta.[366] *Health Insurance Portability and Accountability Act* ja *Gramm-Leach-Bliley Act* ovat liittovaltiotasolla sovellettavia tietosuojalakeja.[367] Tietoturvallisuuteen liittyvä terminologia on Yhdysvalloissa vakiintumatonta.[368] Yksityisellä sektorilla henkilötietojen käsittelyn sääntely on jätetty pääsääntöisesti alan itsesääntelyn varaan.[369]

Kalifornia oli osavaltioista ensimmäinen, jossa säädettiin laki (*Civil Code Sec. 1798.82*) henkilötietojen tietoturvaloukkauksista ilmoittamisesta. Civil Code Sec. 1798.82 astui voimaan heinäkuussa 2003.[370]

Vuonna 2005 ChoisePoint lähetti yli 30 000 Kalifornian asukkaalle kirjeen, jossa se ilmoitti joutuneensa suuren tietoturvaloukkauksen kohteeksi. Ilmoitus perustui Kalifor-

[364] Schwartz & Solove 2014, s. 887 toteavat, että monissa laeissa (esim. *Video Privacy Act*, 18 U.S.C § 2710(a)(3)(2012)) käytetään käsitettä "personally identifiable information."
[365] Pitkänen et al. 2013, s. 184–185. Schwartz & Solova 2014, s. 892 toteavat, että EU:n lähestymistavassa henkilötietoihin on se etu, että se tunnistaa yhä laajenevan mahdollisuuden yhdistää teknologian avulla hajanaisia tiedonmuruja yksittäiseen ihmiseen. Toisaalta on olemassa riski, että EU:n määritelmä henkilötiedoista on liian laaja.
[366] Bradford 2012, s. 22. Bradford 2012 s. 3 kirjoittaa artikkelissaan Bryssel-vaikutuksesta, jolla Bradford tarkoittaa markkinamekanismia, jonka kautta EU pystyy vaikuttamaan muiden valtioiden lainsäädäntöön. Yhtenä esimerkkinä Bradford 2012 s. 24 mainitsee eurooppalaisen tietosuojasääntelyn, joka käytännössä on asettanut vaatimuksia myös esim. yhdysvaltalaisille yrityksille.
[367] Kierkegaard 2013, s. 125. King & Raja 2012, s. 311 toteavat, että toisin kuin EU:ssa Yhdysvalloissa ei ole liittovaltiotason lailla määritelty arkaluonteisia tietoja. Osavaltiotasolla on sen sijaan määritelty useita arkaluonteisen kuluttajatiedon ryhmiä, joihin kohdistuu erityisen tietoturvan vaatimus. Osavaltiotasolla on esimerkiksi säädetty tiedoista, jotka kerätään alle 13- vuotiaista verkkopalveluiden käyttäjistä.
[368] Saarenpää & Pöysti et al. 1997, s. 295 Tietoturvasta puhuttaessa käytetään esim. seuraavia ilmaisuja: "information security", "data security", "computer security", "computer system security" ja "information system security."
[369] Bradford 2012, s. 23.
[370] Kierkegaard 2013, s. 119. Alun perin laki jätti avoimeksi sen, mitä tietoja ilmoitukseen tuli sisältää. Ilmoituksen sisällöstä säädettiin tarkemmin 2011 (Senate Bill 24, "SB 24"). Burdon et al. 2012, s. 297 huomauttaa, että lait, jotka velvoittavat ilmoittamaan henkilötietojen tietoturvaloukkauksista edesauttavat yksilöiden oikeutta tietää henkilötietojensa käytöstä ja myös väärinkäytöstä. Toisaalta nämä lait voidaan nähdä myös markkinaperusteisina kannustimina yrityksille, jotta ne kehittäisivät toimintatapojaan liittyen tietoturvallisuuteen. California Civil Code § 1729.98(a) oli 2003 voimaan tullessaan ensimmäinen säädös, jossa oli vaatimus ilmoittaa tietomurroista. Siitä tuli perusta muille lakien kehityshankkeille koko Yhdysvalloissa.

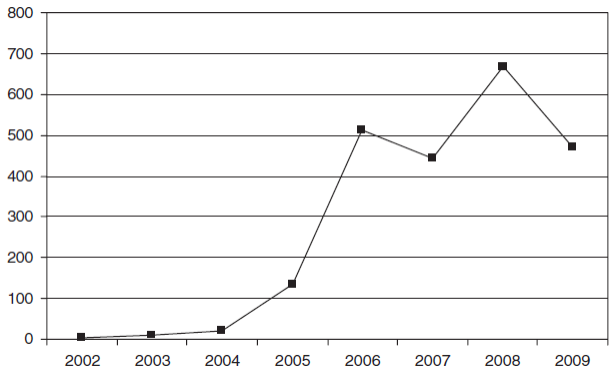
nian lakiin[371], jossa vaadittiin ilmoitus, kun tietoturvaloukkaus kohdistui henkilötietoihin. Tuohon aikaan Kalifornia oli Yhdysvaltioiden osavaltioista ainoa, joka vaati ilmoituksen tietoturvan loukkauksesta. Yli 145 000 henkilön henkilötietoihin päästiin käsiksi laittomasti. Tämä johti yli 700 identiteettivarkauteen[372] eri muodoissaan.[373] ChoisePoint -tapauksen jälkeen useimmat osavaltiot ovat säätäneet henkilötietoihin kohdistuvista tietoturvaloukkauksista ilmoittamisesta.[374] Liittovaltiotasolla ilmoitusvelvollisuudesta ei ole olemassa säädöstä.[375]

Vuonna 2005 yhdysvalloissa identiteettivarkaudet johtivat yritysten ja asiakkaiden osalta 56 miljardin dollarin menetyksiin. Peräti 35 prosenttia identiteettivarkaudesta johtui yrityksiin kohdistuneista tietoturvaloukkauksista. Useat osavaltiot ovat hyväksyneet lakeja, jotka velvoittavat yrityksiä ilmoittamaan tietoturvaloukkauksista kuluttajille, jos heidän henkilötietojaan on hävinnyt tai varastettu. Näiden tietoturvaloukkauksista ilmoittamaan velvoittavien lakien odotettiin vähentävän identiteettivarkauksia. Myöhemmin onkin osoitettu, että nämä lait vähentävät identiteettivarkauksia keskimäärin 6,1 %, kun kyse on tietoturvaloukkauksen seurauksena tehdyistä identiteettivarkauksista.[376]

Kuvassa 4 on esitetty vuosina 2002–2009 Yhdysvalloissa vuosittain raportoitujen henkilötietoihin kohdistuneiden tietoturvaloukkausten määrät. On huomattava, että henkilöt (rekisteröidyt) ovat itse raportoineet heihin kohdistuneet identiteettivarkaudet ja kulutta-

[371] S.B. 1386, kodifioitu Cal. Civ. Code § 1792.82 (a).
[372] *Identiteetin varastamisella* tarkoitetaan toisen henkilötietojen väärinkäyttöä omaksi ja taloudelliseksi hyödyksi tai toisen vahingoittamiseksi. Tekijä voi esiintyä toisena henkilönä laillisesti tai laittomasti haltuunsa saamiensa toisen tunnistetietojen avulla, asioida hänen nimissään, käyttää toisen oikeuksia tai esimerkiksi toisen tiliä. Uhrille vahinko syntyy vasta henkilötietoja käytettäessä. Suppeimmassa merkityksessä identiteettivarkaudella tarkoitetaan erityisiin identifiointitietoihin kuten henkilötunnuksiin, käyttäjätunnuksiin, luottokortin numeroihin ja salasanoihin kohdistuvia tekoja. Tyypillisesi vasta näiden erityisten henkilötietojen väärinkäyttäminen mahdollistaa pääsyn hyödyntää tietoja taloudellisesti. (OM 4/41/2013, s.4) Suomessa identiteettivarkaus on kriminalisoitu rikoslain (39/1889) 38:9a:ssä. Identiteettivarkautta koskeva säännös on uusi (HE 232/2014, s.5).
[373] Solove et al. 2006, s. 699. ChoisePoint huomasi petoksen lokakuussa 2004, mutta siitä ilmoitettiin rekisteröidyille vasta helmikuussa 2005, jotta rikostutkintaan ei kohdistuisi haittaa. Myöhemmin ChoisePoint ilmoitti tietomurroista myös muissa osavaltioissa vakituisesti asuville. Tätä seurasi useiden muidenkin yritysten ja yhteisöjen ilmoitukset henkilötietoihin kohdistuneista tietomurroista. Kongressi järjesti tämän jälkeen aiheesta lukuisia kuulemisia ja teki useita aiheeseen liittyviä lakialoitteita.
Solove et al. 2006, s. 700 pohtii, tulisiko rekisteröidyn saada korvaus jo siitä, että hänen tietoihinsa on luvatta päästy käsiksi. Soloven mukaan kompensaation puolesta voidaan argumentoida siten, että rekisteröity on tällöin alttiimpi tulevaisuudessa tapahtuville haitoille. Toisaalta identiteettivarkautta ei ehkä koskaan tapahdu, vaikka henkilötiedot ovatkin joutuneet luvattoman käsittelyn kohteeksi.
[374] Schwartz & Solove 2014, s. 889 toteavat, että vuonna 2014 yhteensä 47 osavaltiota oli säätänyt velvolisuudesta ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista.
[375] Kierkegaard 2013, s. 119.
[376] Romanosky et al. 2011, s. 256.

jien tietoisuus on lisääntynyt sen jälkeen, kun laki on velvoittanut rekisterinpitäjiä ilmoittamaan tietoturvaloukkauksista. Mitä useammalle ihmiselle ilmoituksia on tehty, sitä useampi kuluttajista tulee tarkastamaan luottotietonsa ja identiteettivarkaudet huomataan näin todennäköisemmin. Toisaalta, mitä useammat osavaltiot säätävät velvollisuudesta ilmoittaa tietoturvaloukkauksista, sitä enemmän media asiasta kiinnostuu. Käytännössä määrällisesti suureen tietoturvaloukkausten kasvuun saattaa siis vaikuttaa ihmisten tietoisuuden ja aktiivisuuden kasvaminen median uutisoinnin seurauksena.[377] Vuonna 2009 Kaliforniassa raportoitiin osavaltioista eniten identiteettivarkauksia, yhteensä 42 000. Pohjois-Dakotassa identiteettivarkauksia raportoitiin samana vuonna osavaltioista vähiten, yhteensä 192.



Kuva 4. Raportoidut henkilötietoihin kohdistuneet tietoturvaloukkaukset Yhdysvalloissa 2002–2009 (Romanosky & al. 2011, s. 264).

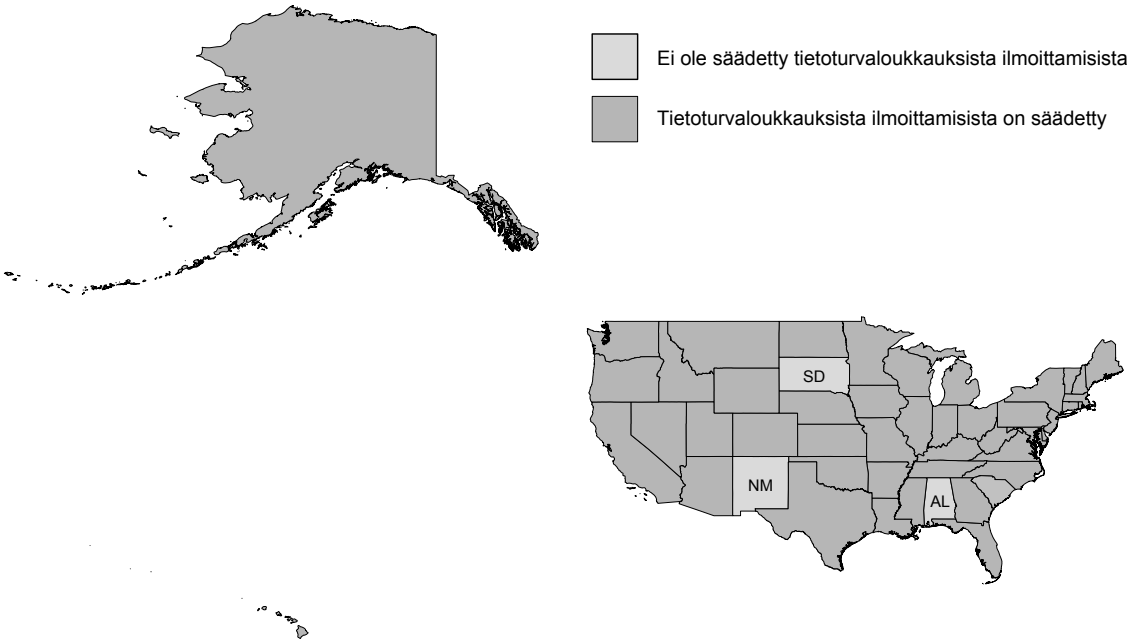
Henkilötietojen tietoturvaloukkauksiin liittyvästä ilmoitusvelvollisuudesta säädetään osavaltioittain hyvin eri tavoin. Kaliforniassa ilmoitusvelvollisuuskynnys on matala ja ilmoitus on tehtävä Kaliforniassa asuville, jonka salaamattomaan henkilötietoon on tai on *kohtuullista uskoa*, että on päästy luvattomasti käsiksi. Käytännössä Kalifornian lainsäädäntö ei siis edellytä tosiasiallista todistetta luvattomasta käytöstä. Useimmissa osavaltioissa lainsäädäntö ei edellytä henkilötietojen tietoturvaloukkauksesta ilmoittamista, jos ei ole kohtuullista todennäköisyyttä sille, että tietoturvaloukkauksesta epäillylle on haittaa.[378] Jos henkilötieto on salattu, ilmoitusta tietoturvaloukkauksesta ei tarvitse pääsääntöisesti tehdä missään osavaltiossa.[379] Ilmoitusvelvollisuus eroaa osavaltiokohtaisesti sen suhteen, koskeeko se ainoastaan julkista sektoria vai sekä julkista että yksityistä

[377] Romanosky et al. 2011, s. 277.
[378] Kierkegaard 2013, s. 120. Vahinkoon liittyvä riski –kriteeri vaihtelee huomattavasti osavaltioittain.
[379] Kierkegaard 2013, s. 120. Poikkeuksen tähän pääsääntöön tekee Wyomingin osavaltio. Muutamissa osavaltioissa on lisäksi säädetty poikkeuksista liittyen salattuihin henkilötietoihin silloin, kun ilmoitus tietoturvaloukkauksesta haittaisi rikostutkintaa. Näitä osavaltioita ovat esimerkiksi Utah, Vermont ja Rhode Island.

sektoria. Eroavaisuuksia osavaltioittain on myös ilmoituksen tekemisen määräajoissa, määritelmissä sekä hallinnollisten seuraamusmaksujen suuruudessa.[380] Erilaiset osavaltiokohtaiset säädökset tekevät ilmoitusvelvollisuutta koskevista säädöksistä puutteellisen ja sen on nähty vaikeuttavan yritysten osavaltioiden rajat ylittävää liiketoimintaa.[381] Vain muutamissa osavaltioissa velvollisuus ilmoittaa tietoturvaloukkauksesta on sidottu muuhun kuin etunimeen tai etunimen alkukirjaimeen yhdistettynä sukunimeen.[382]

Suurin osa osavaltioista vaatii, että henkilötietoihin kohdistuvista tietoturvaloukkauksista ilmoitetaan niille rekisteröidyille, joiden henkilötietoihin tietoturvaloukkaus on kohdistunut. Useiden osavaltioiden lakien mukaan ilmoitus on tehtävä myös osavaltion ja joskus myös liittovaltion viranomaisille.[383] Kuvasta 5 selviää, mitkä Yhdysvaltojen osavaltiot ovat säätäneet rekisterinpitäjille velvollisuuden ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista vuoteen 2016 mennessä. Kuten aiemmin on todettu, vuonna 2005 vain Kaliforniassa oli säädetty ilmoittamisvelvollisuudesta.

[380] Kierkegaard 2013, s. 121. Oklahoman osavaltiossa ilmoitusvelvollisuus on asetettu koskemaan ainoastaan julkista sektoria.
[381] Kierkegaard 2013, s. 122. Myös EU:ssa on tunnistettu, että erilaiset kansalliset tietosuojalainsäädännöt vaikuttavat negatiivisesti liiketoimintaan. Katso luku 1 JOHDANTO.
[382] Schwartz & Solova 2014, s. 890. Mainen, Georgian ja Oregonin lainsäädännössä henkilötiedoksi katsotaan muitakin tekijöitä, jos nämä tekijät riittävät mahdollistamaan identiteettivarkauden.
[383] Global Guide to Data Breach Notifications, 2013, s. 119. Saatavissa: https://iapp.org/media/pdf/knowledge_center/WLG_Global_Data_Breach_Guide.pdf (Katsottu 22.11.2015).



Kuva 5. Yhdysvaltojen osavaltioista 47 oli 1.4.2016 mennessä saattanut voimaan lain, jossa velvoitetaan ilmoittamaan henkilötietoihin kohdistuvista tietoturvaloukkauksista.[384]

Yhdysvallat ei EU:n tapaan rajoita tietojen siirtoa muihin maihin. Yhdysvallat ei myöskään ole perustanut kansallista tietosuojaviranomaista.[385] Kansallista tietosuojaviranomaista Yhdysvalloissa vastaa lähinnä Federal Trade Commission (FTC).[386] Yhdysvalloissa arkaluonteisia tietoja suojataan vain rajoitetusti ja alakohtaisesti. Yhdysvallat antaa yrityksille laajan vapauden kokeilla erilaisia henkilötietojen käsittelyn keinoja. Uusien alojen yrityksiä ei juurikaan säännellä henkilötietojen käsittelyn suhteen. Toisaalta tämä asettaa jo säännellyillä aloilla toimivat yritykset eri asemaan verrattuna uusilla aloilla toimiviin.[387]

On arvioitu, että Yhdysvaltojen kannalta EU:n tietosuoja-asetus on tiettyjen säännösten suhteen henkilötietodirektiiviä joustavampi. Komission tietosuoja-asetusehdotuksen 41 artiklassa säädetään siirrosta tietosuojan tason riittävyyttä koskevan päätöksen perusteella. Siirto voidaan 41 artiklan 1 kohdan mukaan ”toteuttaa, jos komissio on päättänyt, että kyseinen kolmas maa tai kolmannen maan alue tai tietojenkäsittelyn sektori tai kyseinen kansainvälinen järjestö tarjoaa riittävän tietosuojan tason.” Tämä on tulkittavissa

[384] National Conference of State Legislatures. Security Breach Notification Laws 1.4.2016. Saatavissa: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx (Katsottu 3.4.2016).
[385] Schwartz 2013,s. 1977.
[386] Schwartz 2013,s. 1977. Bygrave 2014, s. 178 luonnehtii FTC:a liittovaltion tietosuojaviranomaiseksi. FTC:n toimivalta on laajentunut huomattavasti viimeisimmän 15 vuoden aikana, mutta toimivalta on silti rajoitetumpi kuin Euroopan tietosuojaviranomaisilla.
[387] Schwartz 2013, s. 1978. Uudet teknologiayritykset voivat esimerkiksi louhia tietoa ja lähettää kohdennettua mainontaa internetin kautta tavalla, joka on nykyisten säädösten mukaan teleyrityksiltä kielletty näiden omalla toimialalla.

niin, että yksittäinen osavaltio tai tietyt yritykset voisivat saada komissiolta päätöksen tietosuojan riittävästä tasosta.[388]

Yhdysvalloissa ei ole sellaista lainsäädäntöä, jonka nojalla Euroopan komissio olisi katsonut lainsäädännön turvaavan tietosuojan riittävän tason vaatimuksen. Tästä syystä tietojen siirto EU:sta ei olisikaan ollut mahdollista ilman erityistä Safe Harbor –järjestelyä.[389] Tämän järjestelyn katsottiin täyttäneen henkilötietodirektiivissä vaaditun riittävän tietosuojatason vaatimuksen.[390] Safe Harbor –järjestely on loppuvuodesta 2015 todettu pätemättömäksi.[391]

Henkilötietojen joustava siirto Euroopasta Yhdysvaltoihin on katsottu tärkeäksi muun muassa kaupallisista syistä.[392] Yhdysvallat on pyrkinyt vastaamaan EU:n henkilötietodirektiivin vaatimuksiin useilla järjestelyillä (Safe Harbor[393], konsernin sisäiset sitovat tietosuojasäännöt[394], mallisopimuslausekkeet[395]). EU:n henkilötietodirektiivi ja nyttemmin ehdotus yleiseksi tietosuoja-asetukseksi ovat pyrkineet perustamaan *de facto* kansainvälisen vertailukohdan yritysten informaatioprosesseille.[396]

---

[388] Schwartz & Solove 2014, s. 902. Kolmikantaneuvotteluissa 41 artikla on säilynyt lähes komission ehdotuksen mukaisena.

[389] Bygrave 2014, s. 198 huomauttaa, että vaikuttaa siltä, että EU on tarjonnut USA:lle mahdollisuuden Safe Harbor–sopimukseen, mutta muille kolmansille maille ei ole tarjottu mahdollisuutta neuvotella tällaisesta sopimuksesta.

[390] Pitkänen et al. 2013, s. 184–185. Bygrave 2014, s. 177 huomauttaa, että Euroopan parlamentilta puuttui toimivalta estää Safe Harbor –sopimus, vaikka Euroopan parlamentti suhtautui sopimukseen kriittisesti.

[391] Katso tarkemmin Kappale 9.1.2.

[392] HE 137/2000, s. 4.

[393] Pitkänen et al. 2013, s. 185 toteavat, että henkilötietojen siirtäminen EU:n ja Yhdysvaltojen välillä voidaan toteuttaa erityisen Safe Harbor –järjestelyn avulla. EU-tuomioistuimen lokakuussa 2015 antamassa ratkaisussa C-362/14 komission Safe Harbor-päätös todettiin pätemättömäksi. Jan-Phillip Albrecht on jo aiemmin esittänyt, että Safe Harbor (”turvasatama”) järjestely poistettaisiin kahden vuoden siirtymäajan jälkeen. Saatavissa: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/pr/922/922387/922387en.pdf (Katsottu 12.8.2015). Myös komissio on tiedonannossaan katsonut, että on selvää, ettei Safe Harbor –järjestelmää voida jatkaa nykyisellään siinä havaittujen heikkouksien takia.Komissio katsoi kuitenkin, että Safe harbor –päätöksen kumoaminen vaikuttaisi haitallisesti niiden eurooppalaisten ja yhdysvaltalaisten yritysten etuihin, jotka ovat siihen liittyneet. Siksi Safe Harbor –järjestelmää olisikin komission mukaan vahvistettava. COM(2013) 846 final/ Komission tiedonanto Euroopan parlamentille ja neuvostolle: Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon, s. 8. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52013DC0846&from=FI (Katsottu 7.11.2015).

[394] Binding Corporate rules, BCR. Pitkänen et al. 2013, s. 191 toteavat, että riittävät takeet henkilöiden yksityisyyden ja oikeuksien suojasta voidaan antaa käyttämällä konsernin sisäisiä sitovia sääntöjä. Tietosuojatyöryhmä on hyväksynyt tätä koskevan asiakirjan WP 74, joka käsittelee periaatteita ja menettelyitä kansainvälisissä tiedonsiirroissa.

[395] Henkilötietoja voidaan siirtää henkilötietolain 23 §:n 8 kohdan mukaan, *jos siirto tapahtuu komission hyväksymiä mallisopimuslausekkeita käyttäen*.

[396] Schwartz 2013, s. 1968.

Harvard Law Review:ssa 2013 julkaistussa artikkelissa todetaan, ettei EU ole koskaan virallisesti päättänyt, että Yhdysvaltojen lähestymistapa yksityisyyteen on riittävä tai vastaavasti riittämätön. Yhdysvallat ei myöskään koskaan ole vaatinut riittävyydestä päättämistä. EU:ssa vallitsee tästä huolimatta yhteisymmärrys siitä, että taso on Yhdysvalloissa riittämätön.[397] Tietosuojatyöryhmä WP 29:n[398] antaman lausunnon mukaan ”nykyisellään kapea-alaisista sektorikohtaisista laeista muodostuvaa kokonaisuutta ei voida pitää sellaisena, joka riittävässä määrin turvaisi henkilötietojen siirron Euroopan unionista.”[399]

Obaman hallinto on tunnistanut yksityisyysnäkökulman tärkeän roolin Yhdysvaltojen taloudelle.[400] Yhdysvaltojen toimialakohtaiseen tietosuojalainsäädäntöön yhdistyy teollisuuden itsesääntely ja aktiiviset sääntelyviranomaiset. Yhdysvaltojen näkökulmasta EU:n tietosuoja-asetusta voidaan vastaavasti pitää yleisenä ja yhtenäisenä sekä vapaampana ja kaupankäynnille ystävällisempänä verrattuna Yhdysvaltoihin.[401]

[397] Schwartz 2013,s. 1980. EU:n komissio totesi samana vuonna antamassaan tiedonannossa, että ” Luottamus [Euroopan unionin ja Yhdysvaltojen väliseen] kumppanuuteen on kuitenkin heikentynyt, joten nyt tarvitaan toimia sen palauttamiseksi. Yhdysvaltojen harjoittamaa laajamittaista tiedustelutietojen keruuta koskevat paljastukset ovat herättäneet syvää huolta EU:ssa ja sen jäsenvaltioiden ja Euroopan kansalaisten keskuudessa erityisesti siltä osin kuin on kyse henkilötietojen suojasta. Yksityisen viestinnän joukkoseurantaa, kohdistuipa se sitten kansalaisiin, yrityksiin tai poliittisiin johtajiin, ei voida hyväksyä.” COM(2013) 846 final/ Komission tiedonanto Euroopan parlamentille ja neuvostolle: Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon, s. 2. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52013DC0846&from=FI (Katsottu 14.12.2015).
[398] Tietosuojatyöryhmä on perustettu direktiivin 95/46/EY 29 artiklalla. Työryhmä käsittelee tietosuojaan ja yksityisyyden suojaan liittyviä kysymyksiä. Työryhmä on riippumaton EU:n neuvoa-antava elin.
[399] Working Party on the Protection of Individuals with regard to the Processing of Personal Datas, s. 2.
[400] Bevitt & Sabett, 2015, s. 4 mainitsevat konkreettisena esimerkkinä *Consumer Privacy Bill of Rights* –ehdotuksen, jonka tavoitteena on luoda kattava oikeudellinen kehys yksityisyydestä verkkoympäristössä. Aiheesta tarkemmin: Administration Discussion Draft: *Consumer Privacy Bill of Rights Act of 2015* https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf (Katsottu 3.8.2015).
[401] Bevitt & Sabett, 2015, s. 5.

9 HENKILÖTIETOJEN SIIRTO EU:N ULKOPUOLELLE

9.1.1 Yleiset edellytykset

HetiL:n 22.1 §:n mukaan henkilötietoja ei saa siirtää EU:n/ ETA:n ulkopuolisiin maihin, jos tietoja ei ole Suomessa käsitelty henkilötietolain mukaisesti. Henkilötietojen siirto ei tarkoita ainoastaan esimerkiksi henkilötietoja sisältävän aineiston lähettämistä sähköpostitse, vaan siirtoon lasketaan kuuluvaksi myös esimerkiksi käyttöyhteyden avaaminen kolmannessa maassa sijaitsevalle yrityksen yhteistyökumppanille tai tietojen tarkastelu globaalin yrityksen sisäisessä tietoverkossa.[402] Henkilötietolain 22 §:ssä säädetään yleisistä edellytyksistä siirrettäessä henkilötietoja EU:n ulkopuolelle. HetiL:n 22.1:n mukaan pääsääntö on, että henkilötietoja voidaan siirtää EU:n jäsenvaltioiden alueen tai ETA:n ulkopuolelle ainoastaan, jos vastaanottavassa maassa taataan tietosuojan riittävä taso.

HetiL:n 22a §:ssä säädetään komission päätöksistä.[403] Henkilötietoja voidaan siirtää EU:n ja ETA:n ulkopuolelle, jos komissio on todennut kyseisen maan takaavan riittävän tietosuojan tason.[404]

EU-komissio on todennut, että Yhdysvaltain tietosuojan taso on riittämätön. Yhdysvaltain ja EU:n välisen kaupankäynnin mahdollistamiseksi EU-komissio teki päätöksen Safe Harbor -järjestelystä. Yhdysvaltain kauppaministeriö[405] hallinnoi järjestelmää, jossa organisaatiot itsensä sertifioimalla sitoutuvat noudattamaan Safe Harbor -periaatteita ja useimmin kysyttyjä kysymyksiä käsitellessään EU:n/ETA:n alueelta peräisin olevien henkilötietoja.[406]

9.1.2 Maximilliam Schrems v. Data Protection Commissioner

Tiedonannossaan Euroopan komissio on todennut, että ”henkilötietojen siirto on tärkeä ja välttämätön osa transatlanttisia suhteita. Se on olennainen osa Atlantin yli käytävää

[402] Vanto 2011, s. 84.
[403] Henkilötietolakia on muutettu lisäämällä siihen säännökset komission päätöksenteosta ja päätösten velvoittavuudesta. Laki henkilötietolain muuttamisesta (986/2000) tuli voimaan 1.12.2000.
[404] Euroopan komission lista maista, joiden tietosuojan tason komissio on katsonut riittäväksi on saatavissa: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (Katsottu 22.11.2015).
[405] Yhdysvaltain kauppamisteriön ylläpitämä lista organisaatioista, jotka ovat sitoutuneet noudattamaan Safe Harbor –periaatteita on saatavissa: https://safeharbor.export.gov/list.aspx (Katsottu 21.11.2015).
[406] Vanto 2011, s. 86.

kauppaa. Tämä koskee myös muun muassa sosiaalisen median ja pilvipalveluiden alalla toimivia uusia ja kasvavia digitaaliyrityksiä."[407] Kyseisestä kaupankäynnistä tehtiin 26.7.2000 komission päätös 2000/520/EY[408], jossa komissio katsoi, että Safe Harbor -järjestelmän yhteydessä Yhdysvallat takaa siirrettyjen henkilötietojen suojan riitävän tason.[409]

Lokakuussa 2015 antamassaan ratkaisussa C-362/14 EU:n tuomioistuin on todennut Safe Harbor -päätöksen pätemättömäksi. Tapauksessa Irlannin tietosuojavaltuutettu oli kieltäytynyt tutkimasta kantelua, jonka Schrems oli tehnyt sen vuoksi, että Facebook Irland Ltd. säilyttää käyttäjiensä tietoja palvelimilla, jotka sijaitsevat Yhdysvalloissa.[410] Schrems katsoi, etteivät Yhdysvaltojen oikeus ja käytännöt, ottaen huomioon Edward Snowdenin tekemät paljastukset, tarjoa riittävää suojaa tarkkailulta, jota viranomaiset kohdistavat maahan siirrettyihin tietoihin. Schrems on Itävallan kansalainen ja käyttänyt Facebookia vuodesta 2008.[411]

Ratkaisussa katsottiin, että kansallisten valvontaviranomaisten on voitava tutkia täysin itsenäisesti, noudatetaanko henkilötietodirektiivin vaatimuksia, kun henkilön tietoja siirretään kolmanteen maahan.[412] Yhdysvaltojen kansalliseen turvallisuuteen, yleiseen etuun ja lakien noudattamiseen liittyvät vaatimukset ovat ensisijaisia suhteessa Safe Harbor –järjestelmään.[413] Yhdysvaltalaiset yritykset ovat velvollisia syrjäyttämään Safe Harbor -säännökset silloin, kun ne ovat ristiriidassa edellä mainittujen vaatimusten kanssa. EU:n tuomioistuin totesi ratkaisussaan, että Safe Harbor -järjestelmää on sovellettava ainoastaan siihen suostuvissa yhdysvaltalaisissa yrityksissä. Safe Harbor –järjestelmä ei sido Yhdysvaltojen viranomaisia.[414]

Unionin tuomioistuin katsoi ratkaisussaan, että säännöstöllä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön, loukataan yksityiselämän kunnioittamista koskevan perusoikeuden keskeistä sisältöä.[415] Unionin tuomioistuin katsoi myös,

[407] COM(2013) 846 final/ Komission tiedonanto Euroopan parlamentille ja neuvostolle: Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon, s. 2.
[408] Julkisasiamies Yves Bot: Ratkaisuehdotus 23.9.2015 asiassa C-362/14.
[409] Euroopan unionin tuomioistuin: Lehdistötiedote 117/15. Saatavissa: http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117fi.pdf (Katsottu 1.11.2015).
[410] Julkisasiamies Yves Bot: Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohta 22.
[411] Lehdistötiedote 117/15, s. 1.
[412] C-362/14 Ratkaisun 95 kohta.
[413] C-362/14 Ratkaisun 86 kohta.
[414] C-362/14 Ratkaisun 82 kohta.
[415] C-362/14 Ratkaisun 93 kohta.

että säännöstöllä, jossa yksityiselle ei anneta mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua itseään koskeviin henkilötietoihin, saada nämä tiedot oikaistuksi tai poistetuiksi, loukataan tehokasta oikeussuojaa koskevan perusoikeuden keskeistä sisältöä.[416]

Komissio on antanut tiedonannon ratkaisuun liittyen. Tämän tiedonannon mukaan Safe Harbor -järjestelyä ei voida käyttää oikeusperustana siirrettäessä henkilötietoja Yhdysvaltoihin. Henkilötietojen siirtämistä voidaan jatkaa mallisopimuslausekkeiden ja konsernin sisäisten sitovien sääntöjen perusteella.[417]

WP29 ilmoitti ratkaisusta C-362/14 antamassaan lausunnossa, että jos Yhdysvaltojen viranomaisten kanssa ei löydetä sopivaa ratkaisua tammikuun 2016 loppuun mennessä, ja riippuen vaihtoehtoisten henkilötietojen siirtoon käytettävien työkalujen arvioinnista, tietosuojaviranomaisten on toteutettava kaikki tarvittavat ja tarkoituksenmukaiset toimet mukaan lukien koordinoidut täytäntöönpanotoimet.[418]

Euroopan komissio ja Yhdysvallat ovat alkuvuodesta 2016 tehneet Privacy Shield -sopimuksen ja päässeet yhteisymmärrykseen uusista Atlantin yli tapahtuvan tiedonsiirron puitteista. Sopimuksella turvataan EU:n kansalaisten perusoikeudet siirrettäessä heidän henkilötietojaan Yhdysvaltoihin. Yrityksille taataan oikeusvarmuus. Sopimuksessa otetaan huomioon Euroopan unionin tuomioistuimen ns. Schrems-ratkaisussa asettamat vaatimukset. Sopimuksen mukaan jokaisen eurooppalaisten henkilötietoja käsittelevän yrityksen on sitouduttava noudattamaan Euroopan tietosuojaviranomaisten päätöksiä. EU:n kansalaisilla on käytettävissään useita oikeussuojakeinoja, jos he katsovat, että heidän tietojaan on käytetty väärin uuden järjestelyn puitteissa.[419]

Muiden muassa Electronic Frontier Foundation on katsonut, ettei Privacy Shield täytä unionin tuomioistuimen vaatimuksia. Effin mukaan Privacy Shield mahdollistaa edelleen Yhdysvaltojen muiden maiden kansalaisiin kohdistuvan joukkoseurannan. Järjeste-

[416] C-362/14 Ratkaisun 95 kohta.
[417] Komission tiedonanto. COM(2015)566 final. The Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgement by the Court of Justice in Case 362/14 (Scherems)COM(2015) 566 final, s, 4.
[418] Statement of the Article 29 Working Party, Brussels, 16 October 2015, s. 1.
[419] Euroopan komissio – Lehdistötiedote. EU:n komissio ja Yhdysvallat sopivat uusista Atlantin yli tapahtuvan tiedonsiirron puitteista: yksityisyyden suojaa koskeva Privacy Shield –sopimus. Saatavissa: http://europa.eu/rapid/press-release_IP-16-216_fi.htm (Katsottu 14.2.2016).

lyyn kuuluvat riidanratkaisukeinot eivät myöskään ole riippumattomia.[420] Yli 20 kansalaisjärjestöä on kehottanut Euroopan johtajia vastustamaan Privacy Shield –sopimuksen hyväksymistä. Kansalaisjärjestöjen mukaan poliittinen sopimus ei tarjoa riittävää tietosuojaa eikä ole linjassa EU:n tuomioistuimen asiassa C-362/14 antaman ratkaisun kanssa. Kansalaisjärjestöjen mukaan Yhdysvaltojen on tehtävä muutoksia kansallisiin lakeihinsa EU:n tuomioistuimen päätöksen mukaisesti.[421]

[420] Eff. Saatavissa: https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes (Katsottu 3.4.2016).
[421] EPIC, Electronic Privacy Center.
Saatavissa: https://epic.org/privacy/intl/eu_data_protection_directive.html. (Katsottu 3.4.2016).

10 JOHTOPÄÄTÖKSET

Tietosuoja-asetus korvaa nykyisen henkilötietodirektiivin alkuvuodesta 2018. Asetuksena se on sellaisenaan sovellettavaa oikeutta koko EU:n alueella. Tietosuoja-asetuksen myötä yleiset henkilötietojen käsittelyyn liittyvät periaatteet säilyvät pääosin sellaisenaan. Tietosuoja-asetuksella on tarkoitus yhdenmukaistaa koko EU:n alueella sekä vaatimusten että seuraamusten soveltamiskäytäntöä henkilötietojen käsittelyssä. Tällä pyritään lisäämään kansalaisten luottamusta EU:n kansalaisten henkilötietoja käsitteleviin toimijoihin.[422] Tietosuoja-asetusehdotus tuo mukanaan esimerkiksi seuraavanlaisia muutoksia: tietosuoja-asetuksen säännöksiä tullaan soveltamaan rekisterinpitäjän lisäksi myös henkilötietojen käsittelijään, tietoturvaloukkauksista ilmoittaminen tulee tietyissä tilanteissa pakolliseksi ja säännösten noudattamatta jättämisestä voi seurata hallinnollinen seuraamusmaksu.[423] Näistä muutoksista tässä maisteritutkielmassa on keskitytty kuvaamaan erityisesti rekisterinpitäjälle asetettua ilmoittamisvelvollisuutta tietoturvaloukkauksista.

Tietosuoja-asetuksen tavoitteena on harmonisoida ja yhtenäistää hajanaista eurooppalaista tietosuojasääntelyä sekä helpottaa digitaalisen liiketoiminnan rakentamista Euroopan laajuisesti. Tietosuoja-asetuksella luodaan mekanismit, jotka kannustavat ja pakottavat yhtiöitä ottamaan toimintansa suunnittelussa yksityisyyden suojan ja tietosuojakysymykset huomioon.[424]

Rekisterinpitäjillä ei ole ilman lain tuomaa velvoitetta kannustimia paljastaa tietoturvaloukkauksia. Tietoturvaloukkauksilla on negatiivinen vaikutus yritysten maineeseen. Tutkimusten mukaan EU:n kansalaiset pitävät tärkeänä saada tietää, jos heidän henkilötietoihinsa on kohdistunut tietoturvaloukkaus. Tietosuoja-asetus tuleekin asettamaan rekisterinpitäjälle velvollisuuden tehdä ilmoitus valvontaviranomaiselle ja rekisteröidylle, kun rekisteröidyn henkilötietoihin kohdistuu tietoturvaloukkaus. Vastaavanlainen velvollisuus on jo aiemmin koskenut telealan toimijoita. Tietosuoja-asetuksen ilmoitus ei kuitenkaan koske vähäisiä tietoturvaloukkauksia. Voidaankin esittää kysymys siitä,

[422] Yleinen tietosuoja-asetus/ COM(2012) 11 Final, s. 19; Pitkänen et al. 2013, s. 26. Luottamuspulaa aiheuttavat tavanomaisten verkkorikosten lisäksi joidenkin valtioiden laajamittainen verkkovalvonta- ja tiedustelutoiminta kuten Euroopan unionin tuomioistuimen ns. Schrems-ratkaisu osoitti.
[423] Pitkänen et al. 2013, s. 26.
[424] Andreasson et al. 2014b, s. 20 jatkaa, että tämä voi muodostua myös kilpailueduksi suhteessa yhdysvaltalaisiin toimijoihin, joita kohtaan luottamus on heikentynyt Edward Snowdenin paljastusten seurauksena.

kuinka objektiivisesti rekisterinpitäjät pystyvät tekemään arvion tietoturvaloukkauksen luonteesta ja vaikutuksista. Tietoturvaloukkausten ilmoittaminen voi toisaalta vaikuttaa negatiivisesti rekisterinpitäjän maineeseen. Rekisteröidyn kannalta ilmoitus tietoturvaloukkauksesta antaa mahdollisuuden tehdä tarvittavia toimenpiteitä tietoturvaloukkauksen vaikutusten minimoimiseksi. Toisaalta ilmoitusten vaatiminen merkityksettömistä tietoturvaloukkautumisista saattaisi aiheuttaa rekisteröityjen turhautumisen ilmoituksiin, jolloin he mahdollisesti vain sivuuttaisivat tehdyt ilmoitukset. Tällöin ilmoituksista ei saataisi sitä hyötyä, jota niillä on alun perin tavoiteltu. Ilmoituksillahan pyritään siihen, että rekisteröidyt voivat ryhtyä toimenpiteisiin vahinkojen minimoimiseksi. Useat rekisterinpitäjät myös viittasivat tietosuoja-asetusehdotuksesta antamissaan kannanotoissaan valvontaviranomaisten mahdollisiin resurssivajeisiin, jos ilmoitusvelvollisuus säilyisi tietosuoja-asetusehdotuksen mukaisesti rajoittamattomana.

Tietosuoja-asetusehdotukseen tehtiin valmistelun aikana yli 4000 muutosehdotusta. Täysin selvää ei ole, missä määrin intressiryhmien kannanotot ovat suoranaisesti vaikuttaneet asetuksen sisältöön. Väitetään, että internetjätit toivat mukanaan aggressiivisen lobbauskulttuurin ja että internetjätit rahoittivat kaikessa hiljaisuudessa näennäisesti puolueettomina esiintyneitä tietosuojalobbareita.[425] Valmistelun aikana muutoksia tehtiin myös tässä maisteritutkielmassa esitettyyn velvollisuuteen ilmoittaa henkilötietojen tietoturvaloukkauksista. Alkuperäisessä komission ehdotuksessa ilmoitusvelvollisuus oli tehtävä valvontaviranomaiselle kaikista henkilötietojen tietoturvaloukkauksista. Lopullisen kompromissitekstin mukaan ilmoitusta tietoturvaloukkauksesta ei tarvitse tehdä, jos henkilötiedot on suojattu teknisesti esimerkiksi salauksen avulla. Ilmoitusta ei myöskään tarvitse tehdä, jos rekisterinpitäjä on toteuttanut jatkotoimenpiteitä, joilla varmistetaan, ettei rekisteröidyn oikeuksien ja vapauksien kannalta suuri riski todennäköisesti tapahdu. Esimerkiksi eBay oli omassa kannanotossaan huomauttanut, että tietojen salaaminen poistaisi velvollisuuden tehdä ilmoitus tietoturvaloukkauksesta. Toisaalta on huomattava, että WP29 on esittänyt, että salauksen yhteydessä olisi arvioitava salauksen tasoa eli mikä tahansa salaus[426] sinänsä ei olisi riittävä peruste. Rekisteröidyn

[425] Miten internetin jättiyritykset lobbasivat EU:ta ja miten ne paljastettiin. Saatavissa: http://rapport.fi/rapport/juttuidea.php?aid=225485 (Katsottu 14.2.2016).

[426] Kuner 2013, s. 97 toteaa, ettei salaus ole riittävä tae kaikkia uhkia vastaan. Salaus suojaa tietoa luvattomalta pääsyltä siihen, kun tietoja siirretään tai tallennetaan, mutta se ei suojaa tietoja sellaiselta käyttäjältä, jotka pystyvät avaamaan salauksen. Kuner huomauttaa myös liittyen kansainvälisiin tiedonsiirtoihin, että salatun tiedon siirtäminen toiseen maahan sisältää pienemmän riskin kuin se, että tieto säilytetään lähtömaassa salaamattomana.

oikeuksien varmistamiseksi olisi tärkeää, että tietosuoja-asetusta sovellettaessa huomioitaisiin tämä WP29:n lausuma täsmennys.

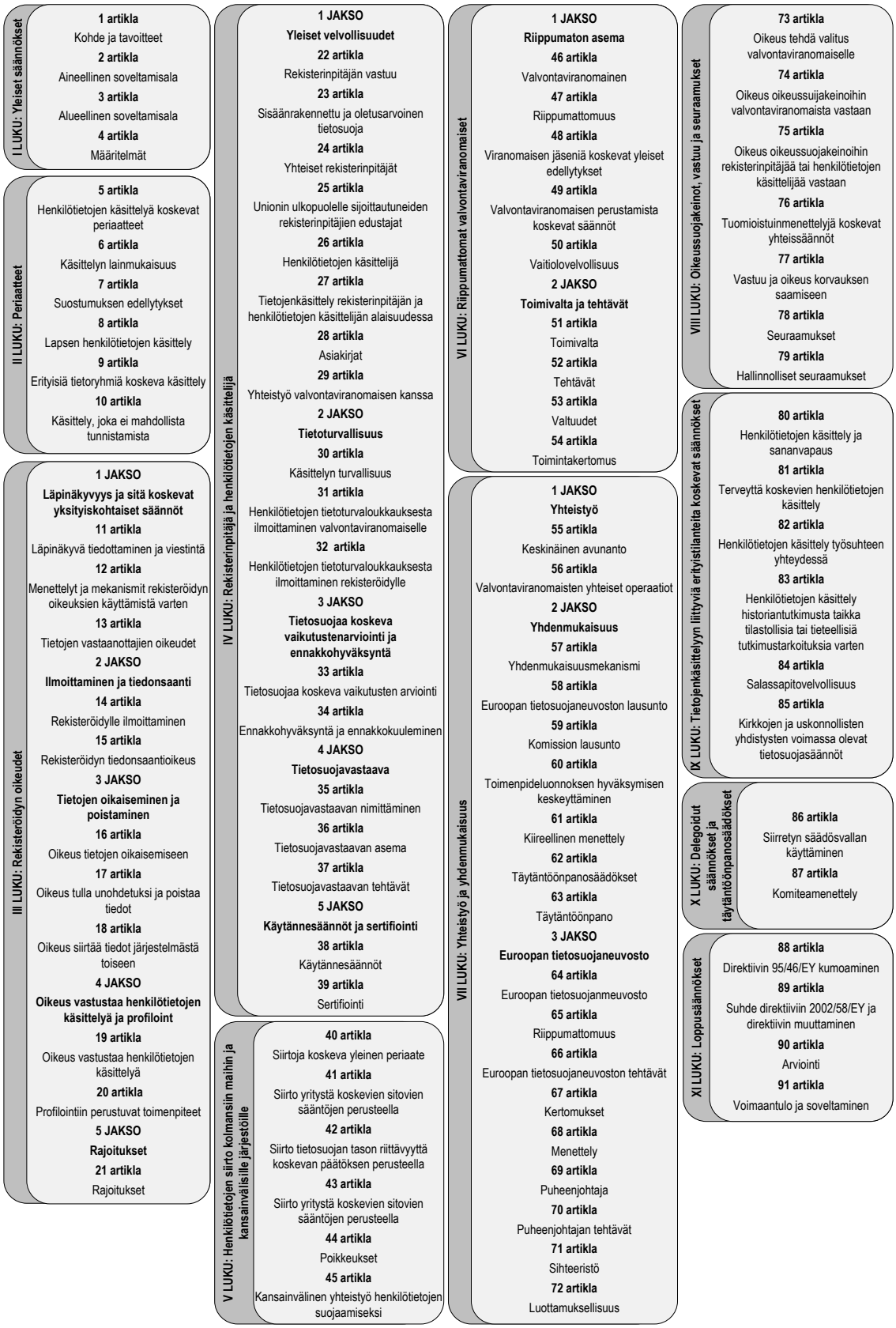
Tietosuoja-asetus asettaa voimaantullessaan vaatimuksia myös tietojärjestelmille. Tietojärjestelmien tulee olla kyvykkäitä tunnistamaan tietoturvaloukkaukset. Rekisterinpitäjille asetettu velvollisuus ilmoittaa tietoturvaloukkauksista voi toteutua tehokkaasti vain, jos tietojärjestelmiin on implementoitu kyvykkyys hälyttää järjestelmään kohdistuvasta tietoturvaloukkauksesta kuten hakkeroinnista. Tietojärjestelmien tulee myös tukea tietosuoja-asetuksen mukaista rekisteröidyn oikeutta tulla unohdetuksi. Todennäköisesti useat rekisterinpitäjät joutuvat päivittämään ohjelmistojaan, mikä vaatii rekisterinpitäjiltä taloudellisia resursseja ja myös tietotaitoa ohjelmistojen tietoturvallisuusvaatimusten määrittelystä.

Tämän maisteritutkielman oikeusvertailevassa osuudessa esiteltiin, miten tietoturvasta henkilötietoja käsiteltäessä on säädetty Ruotsissa, Norjassa ja Yhdysvalloissa. Monet tietosuojaan liittyvät haasteet ovat samoja sekä Euroopassa ja Yhdysvalloissa, vaikka lainsäädännöllinen viitekehys ja käsitys yksityisyydestä poikkeavat toisistaan merkittävästi. Sekä EU:ssa että Yhdysvalloissa ongelmaksi on tunnistettu se, että tietosuojan taso vaihtelee valtioittain (osavaltioittain).

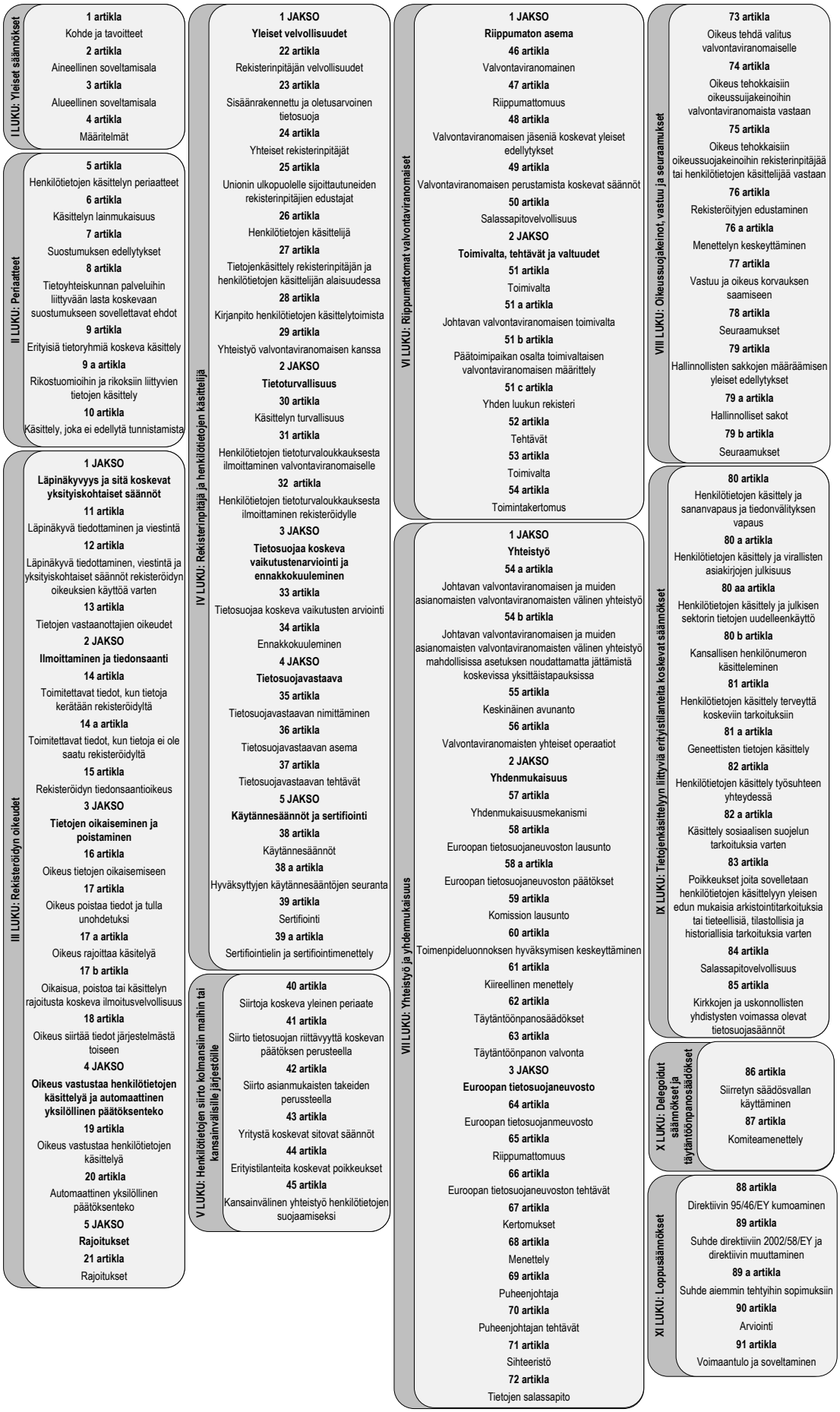
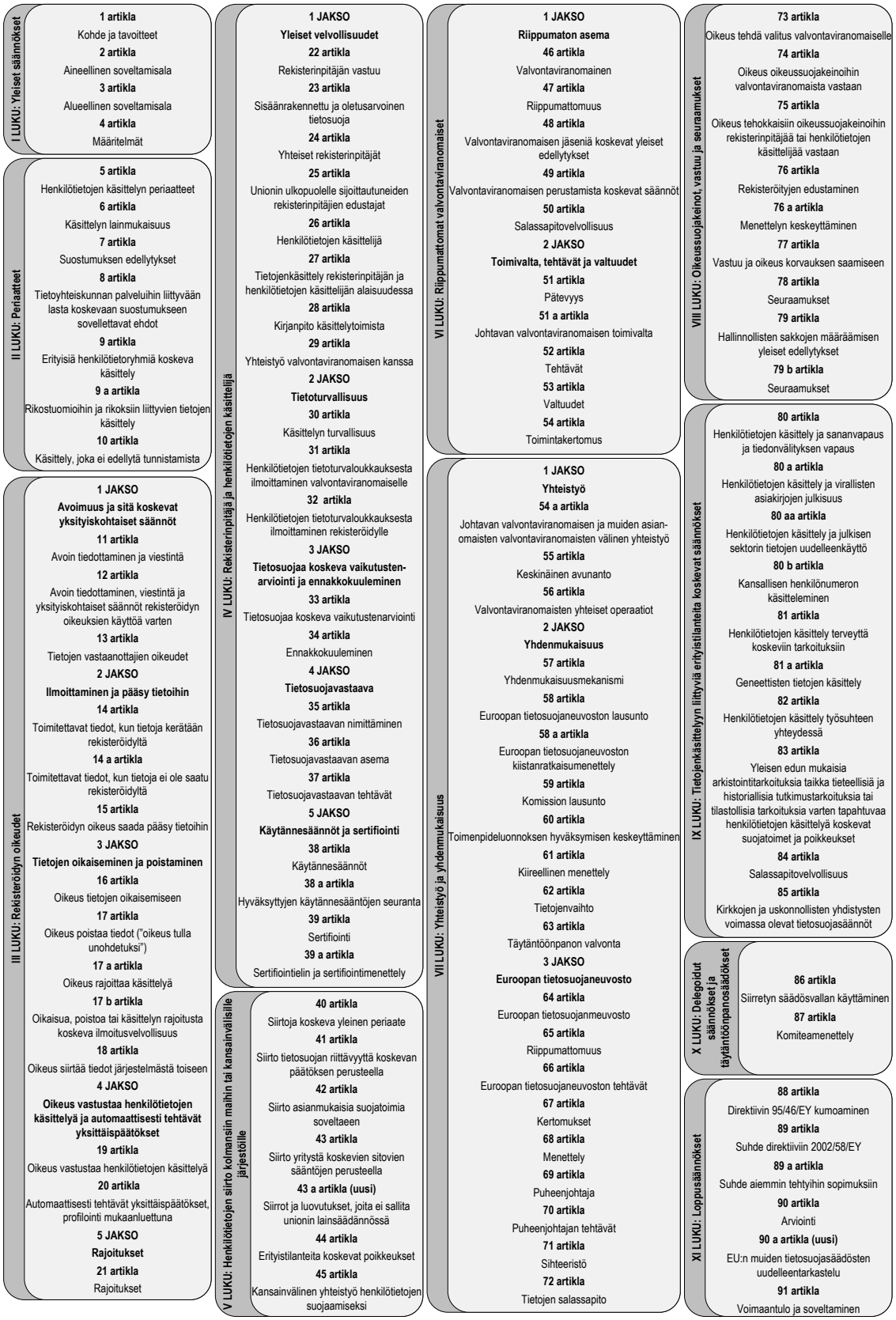
Yhdysvalloissa on havaittu, että velvollisuus ilmoittaa henkilötietoihin kohdistuvista tietoturvaloukkauksista on lisännyt tehtyjen ilmoitusten määrää. Yhdysvalloissa asiaa säätelevien lakien voimaantulon ja aiheen mediassa saaman huomion takia myös yleinen tietoisuus tietoturvaloukkauksista on viimeisen vuosikymmenen aikana lisääntynyt. On oletettavaa, että vastaava ilmiö nousee tietosuoja-asetuksen voimaantulon myötä myös Euroopassa.

Selvältä vaikuttaa, että yksilön oikeudet henkilötietojensa suojaan tulevat tietosuoja-asetuksen myötä lujittumaan. Tietosuoja-asetusehdotus tähtää myös siihen, että ihmiset luottaisivat verkkopalveluihin ja siten myös käyttäisivät verkkopalveluja entistä enemmän. Tietosuoja-asetus antaa luottamuksen syntymiselle edellytyksiä, mutta käytännön vaikutukset talouteen selviävät vasta tietosuoja-asetuksen voimaantulon jälkeen.

LIITE 1. Euroopan komission ehdotus asetukseksi henkilötietojen suojasta COM(2012) 11 Final.



LIITE 2. OSA-neuvoston yleisnäkemys asetukseksi henkilötietojen suojasta 15.6.2015.



LIITE 3. Rakenne epävirallisen suomennoksen pohjalta (kolmikantaneuvotteluiden ehdotus 15.12.2015).