PRIVACY SHIELD

SÄÄNTELYN KEHITYS HENKILÖTIETOJEN SIIRTÄMISESSÄ EUROOPAN UNIONISTA YHDYSVALTOIHIN

Kaisa Hokkinen
Maisteritutkielma
Oikeusinformatiikka
Oikeustieteiden tiedekunta
Lapin yliopisto
2018

Lapin yliopisto
Oikeustieteiden tiedekunta

Työn nimi: Privacy Shield - Sääntelyn kehitys henkilötietojen siirtämisessä Euroopan unionista Yhdysvaltoihin

Tekijä: Kaisa Hokkinen

Oppiaine: Oikeusinformatiikka

Työn laji: Tutkielma_X Laudaturtyö _ Lisensiaatintyö_

Sivumäärä: 87

Vuosi**:** 2018

Tiivistelmä

Teknologian kehityksen ja kansainvälisen kaupan kasvun myötä henkilötietoja siirretään yhä enemmän valtioiden rajojen yli. Henkilötietojen suojalla on Euroopan unionin oikeudessa perusoikeusasema, joka kuvastaa henkilötietojen käsittelyltä vaadittavaa korkeaa tietosuojan tasoa. Henkilötietojen siirtoa Euroopan unionin alueelta kolmansiin maihin on pitkään säädellyt henkilötietodirektiivi, mutta sen tulee toukokuussa 2018 korvaamaan vielä tarkempia säännöksiä sisältävä tietosuoja-asetus.

Henkilötietoja voidaan siirtää unionin ulkopuolelle muun muassa Euroopan komission päätöksellä, jossa se toteaa tietyn valtion takaavan riittävän tietosuojan tason. Euroopan unioni ja Yhdysvallat ovat toistensa tärkeimpiä kauppakumppaneita. Henkilötietojen siirtoa unionista Yhdysvaltoihin määrittivät pitkään vapaaehtoisuuteen ja itsesääntelyyn perustuvat Safe Harbor-periaatteet, jotka oli saatettu voimaan komission päätöksellä vuonna 2000. Safe Harbor-järjestely oli kritiikin alaisena alusta alkaen ja viimeistään vuoden 2013 paljastukset Yhdysvaltojen harjoittamasta, tietoverkoissa tapahtuvasta massavalvonnasta asettivat järjestelyn tehokkuuden kyseenalaiseksi. Euroopan unionin tuomioistuin kumosi Safe Harbor-päätöksen tuomiollaan lokakuussa 2015.

Safe Harbor-periaatteiden tilalle pyrittiin luomaan turvallisempi, tarkempi ja tehokkaampi järjestely henkilötietojen siirtämiselle unionista Yhdysvaltoihin. Privacy Shield-järjestely, joka sisältää monia uusia velvoitteita henkilötietoja käsitteleville yrityksille ja rajoitteita Yhdysvaltain viranomaisten pääsylle järjestelyn nojalla siirrettyihin henkilötietoihin, tuli komission päätöksellä voimaan heinäkuussa 2016. Järjestelyn tehokkuudesta ja henkilötietojen suojan todellisesta tasosta vallitsee kuitenkin edelleen eriäviä näkemyksiä ja järjestelyn pätevyys on jo haastettu Euroopan unionin tuomioistuimessa.

Avainsanat: henkilötieto, henkilötietojen suoja, yksityisyys, yksityisyyden suoja, tietosuoja,

Privacy Shield, Safe Harbor, Euroopan unioni, Yhdysvallat

Muita tietoja:

Suostun tutkielman luovuttamiseen Rovaniemen hovioikeuden käyttöön: X

Suostun tutkielman luovuttamiseen kirjastossa käytettäväksi: X

Suostun tutkielman luovuttamiseen Lapin maakuntakirjastossa käytettäväksi: X

SISÄLLYSLUETTELO

LÄHTEET

Kirjallisuus

Aarnio, Aulis. Luentoja lainopillisen tutkimuksen teoriasta. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja. Helsinki 2011.

Aarnio, Aulis. Mitä lainoppi on? Helsinki 1978.

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.

Boehm, Franziska. Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonized Data Protection Principles for Information Exchange at EU-level. Heidelberg 2012.

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

Bygrave Lee A. & Bing Jon. Internet Governance. Infrastructure and Institutions. Oxford University Press 2009.

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

Heisenberg, Dorothee. Negotiating Privacy: The European Union, The United States and Personal Data Protection. The United States of America 2005.

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

Husa, Jaakko. Oikeusvertailu. Viro 2013.

Korhonen, Rauno. Perusrekisterit ja tietosuoja. Helsinki 2003.

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

Neuvonen, Riku. Yksityisyyden suoja Suomessa. Helsinki 2014.

Ojanen, Tuomas. Perusoikeusjuridiikka. Helsinki 2015.*xOjanen, Tuomas*. EU-oikeuden perusteita. Keuruu 2016.

Pesonen, Pirkko. Yritysviestinnän säännöt. Jyväskylä 2012.

Pesonen, Pirkko. Sosiaalisen median lait. Viro 2013.

Petersmann, Ernst-Ulrich, Pollack, Mark A. Transatlantic Economic Disputes. The EU, the US, and the WTO. Oxford University Press, New York 2003.

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

Pitkänen Olli, Korpisaari Päivi, Korhonen Rauno. Miten kansallista lainsäädäntöämme pitää muuttaa EU:n yleisen tietosuoja-asetuksen vuoksi? Teoksessa: Viestinnän muuttuva sääntely: viestintäoikeuden vuosikirja 2016 / Päivi Korpisaari (toim.). Helsinki, Helsingin yliopiston oikeustieteellinen tiedekunta, 2017.

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

Raitio, Juha. Euroopan unionin oikeus. Helsinki 2016.

Saarenpää, Ahti. Oikeusinformatiikka. Teoksessa: Niemi Marja-Leena (toim.) Oikeus tänään | Osa I. Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja sarja C 64 2016. s. 67 – 273.

Saarenpää, Ahti. Oikeuden valtatie ja arkipäivän perusoikeudet. Teoksessa: Aarto, Markus ja Vartiainen, Markku (toim.): Oikeus kansainvälisessä maailmassa – Ilkka Saraviidan juhlakirja. Helsinki 2008, s. 135 – 146.

Salminen, Markus. Tietosuoja sähköisessä liiketoiminnassa. Talentum Media Oy 2009.

Saraviita, Ilkka. Suomalainen perusoikeusjärjestelmä. Jyväskylä 2005.

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

Vanto, Jarno J. Henkilötietolaki käytännössä. Helsinki 2011.

Voutilainen, Tomi. Oikeus tietoon – Informaatio-oikeuden perusteet. Porvoo: Bookwell Oy 2012.

Kotimaiset virallislähteet ja muu virallisaineisto

Oikeusministeriö, Tietosuojavaltuutetun toimisto. Selvityksiä ja ohjeita 4/2017. Miten valmistautua EU:n tietosuoja-asetukseen? Saatavissa: http://www.tietosuoja.fi/material/attachments/tietosuojavaltuutettu/tietosuojavaltuutetuntoimisto/oppaat/1Em8rT7IF/Miten_valmistautua_EUn_tietosuoja-asetukseen.pdf (Katsottu 20.4.2018).

Pitkänen, Olli (toim.) Tietosuojasäädösten muutostarve. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017. Saatavissa: http://tietokayttoon.fi/documents/10616/3866814/41_2017_Tietosuojas%C3%A4%C3%A4d%C3%B6sten+muutostarve/2c4ad983-8d90-480e-9b05-e3de9c9297c4?version=1.1 (Katsottu 24.4.2018).

Oikeusministeriö. Mietintöjä ja lausuntoja 35/2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö. Saatavissa: http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80098/OMML_35_2017_EUn_yleinen_tietosuoja.pdf?sequence=1&isAllowed=y (Katsottu 24.4.2018).

Oikeusministeriö. Mietintöjä ja lausuntoja 52/2017. Henkilötietojen suoja rikosasian käsittelyssä ja kansallista turvallisuutta ylläpidettäessä. Tietosuojadirektiivityöryhmän mietintö. Saatavissa: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/160258/52_2017_Henkilotietojen_suoja.pdf?sequence=1&isAllowed=y (Katsottu 24.4.2018).

Oikeusministeriö. Lausunto 31.5.2016 Eduskunnan hallintovaliokunnalle. Komission tiedonanto: Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi - E 37/2016 vp. Saatavissa: https://www.eduskunta.fi/FI/vaski/JulkaisuMetatieto/Documents/EDK-2016-AK-62908.pdf (Katsottu 30.4.2018).

Perustuslakivaliokunta. Lausunto PeVL 40/2017 vp – HE 82/2017 vp. Saatavissa: https://www.eduskunta.fi/FI/vaski/Lausunto/Sivut/PeVL_40+2017.aspx (Katsottu 30.4.2018).

Hallituksen esitys HE 9/2018 vp. Hallituksen esitys eduskunnalle yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi. Saatavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_9+2018.aspx (Katsottu 23.4.2018).

Hallituksen esitys HE 82/2017 vp. Hallituksen esitys eduskunnalle laiksi tietoyhteiskuntakaaren muuttamisesta. Saatavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_82+2017.aspx (Katsottu 30.4.2018).

Hallituksen esitys HE 31/2018 vp. Hallituksen esitys eduskunnalle laiksi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sekä eräiksi siihen liittyviksi laeiksi. Saatavissa: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Sivut/HE_31+2018.aspx (Katsottu 30.4.2018).

Euroopan unionin lähteet

Euroopan unionista tehty sopimus. Konsolidoitu toisinto. Euroopan unionin virallinen lehti 2016/C 202/01. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=FI (Katsottu 23.4.2018).

Euroopan unionin toiminnasta tehty sopimus. Konsolidoitu toisinto. Euroopan unionin virallinen lehti 2016/C 202/1. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=OJ:C:2016:202:FULL&from=FI (Katsottu 23.4.2018).

Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta. (2007/C 306/01). Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12007L/TXT&from=FI (Katsottu 22.4.2018).

Euroopan unionin perusoikeuskirja (2012/C 326/02). Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:12012P/TXT&from=FI (Katsottu 24.4.2018).

Euroopan parlamentti ja neuvosto. Asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32001R0045&from=FI (Katsottu 21.4.2018).

Euroopan parlamentti ja neuvosto. Asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus). Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:32016R0679&from=FI (Katsottu 24.4.2018).

Euroopan parlamentti ja neuvosto. Direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Saatavissa: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:fi:HTML (Katsottu 11.4.2018).

Euroopan parlamentti ja neuvosto. Direktiivi (2002/58/EY) henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla. Saatavissa: https://edps.europa.eu/sites/edp/files/publication/dir_2002_58_fi.pdf (Katsottu 21.4.2018)

Euroopan parlamentti ja neuvosto. Direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta. Saatavissa: http://eur-lex.europa.eu/legal-content/fi/TXT/PDF/?uri=CELEX:32016L0680&from=EN (Katsottu 21.2.2018).

Euroopan komissio. 2000/520/EY: Komission päätös, tehty 26 päivänä heinäkuuta 2000, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa

koskevien Safe Harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä. Saatavissa: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:FI:HTML (Katsottu 24.4.2018).

Euroopan komissio. Täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä (tiedoksiannettu numerolla C (2016) 4176). Saatavissa: http://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2016/07-11/C_2016_4176_F1_COMMISSION_IMPLEMENTING_DECISION_FI.pdf (Katsottu 22.1.2018).

Euroopan komissio. COM (2013) 846 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle: Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon. Saatavissa: http://ec.europa.eu/transparency/regdoc/rep/1/2013/FI/1-2013-846-FI-F1-1.Pdf (Katsottu 22.1.2018).

Euroopan komissio. COM (2017) 611 final. Komission kertomus Euroopan parlamentille ja neuvostolle EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toiminnan ensimmäisestä vuosittaisesta tarkastelusta. Saatavissa: http://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017DC0611&from=FI (Katsottu 22.1.2018).

Euroopan komissio. COM (2017) 10 final. Ehdotus Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017PC0010&from=EN (Katsottu 24.4.2018).

Euroopan komissio. COM (2013) 846 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle. Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon. Saatavissa: http://ec.europa.eu/transparency/regdoc/rep/1/2013/FI/1-2013-846-FI-F1-1.Pdf (Katsottu 24.4.2018).

Euroopan komissio. COM (2013) 847 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle: Safe Harbor-järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta. Saatavissa: http://www.europarl.europa.eu/meetdocs/2014_2019/documents/com/com_com(2013)0847_/com_com(2013)0847_fi.pdf (Katsottu 24.4.2018).

Euroopan komissio. COM (2015) 566 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle direktiiviin 95/46/EY perustuvasta henkilötietojen siirtämisestä EU:sta Yhdysvaltoihin unionin tuomioistuimen asiassa C-362/14 (Schrems) antaman tuomion johdosta. Saatavissa: http://ec.europa.eu/transparency/regdoc/rep/1/2015/FI/1-2015-566-FI-F1-1.PDF (Katsottu 22.4.2018).

Euroopan komissio. COM (2016) 117 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle. Transatlanttiset tietovirrat: luottamuksen palauttaminen vahvoilla suojatoimilla. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52016DC0117&from=EN (Katsottu 14.4.2018).

Commission of the European Communities. Commission Staff Working Paper. The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. 13.02.2002 SEC (2002) 196. Saatavissa: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/05_2002-196ecstaff_wp_/05_2002-196ecstaff_wp_en.pdf (Katsottu 24.4.2018).

Commission of the European Communities. Commission Staff Working Document. The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. Brussels 20.10.2004 SEC (2004) 1323. Saatavissa: http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/06_2004-1323ecstaff_report_/06_2004-1323ecstaff_report_en.pdf (Katsottu 24.4.2018).

European Commission. Commission Staff Working Document. (Accompanying the document) Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield. SWD (2017) 344 final. Saatavissa: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=605619 (Katsottu 24.4.2018).

European Commission. Statement 15/5782, Strasbourg 6.10.2015. Saatavissa: http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm (Katsottu 23.4.2018).

Euroopan komissio. Lehdistötiedote 10.1.2017. Komissio ehdottaa korkeatasoisen yksityisyydensuojan varmistavia sääntöjä kaikkeen sähköiseen viestintään ja päivittää EU:n toimielimiä koskevia tietosuojasääntöjä. Saatavissa: http://europa.eu/rapid/press-release_IP-17-16_fi.htm (Katsottu 22.4.2018).

European Commission. Press release. EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield. Strasbourg, 2 February 2016. Saatavissa: http://europa.eu/rapid/press-release_IP-16-216_en.htm (Katsottu 14.4.2018).

Euroopan komissio. Lehdistötiedote 12.7.2016. Euroopan komissio ottaa käyttöön EU:n ja Yhdysvaltojen välisen Privacy Shield-järjestelyn: vahvempi suoja transatlanttisille tietovirroille.

Euroopan parlamentti. Päätöslauselma Yhdysvaltojen kansallisen turvallisuusviraston valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa, 12.3. 2014. (2013/2188(INI) Saatavissa: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P7-TA-2014-0230+0+DOC+XML+V0//FI (Katsottu 20.3.2018).

Euroopan parlamentti. Päätöslauselma transatlanttisista tietovirroista, 26.5.2016. (P8_TA (2016)0233). Saatavissa: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2016-0233+0+DOC+PDF+V0//FI (Katsottu 14.4.2018).

Euroopan parlamentti. Päätöslauselma EU:n ja Yhdysvaltojen Privacy Shield-järjestelyn tarjoaman suojan riittävyydestä, 6.4.2017. (2016/3018(RSP). Saatavissa: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P8-TA-2017-0131+0+DOC+PDF+V0//FI (Katsottu 24.4.2018).

Article 29 Working Party. Working Document on Functioning of the Safe Harbor Agreement. 11194/02/EN WP 62. Saatavissa: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2002/wp62_en.pdf (Katsottu 21.4.2018).

Article 29 Working Party. Statement on the Implementation of the Judgment of the Court of Justice of the European Union of 6 October 2015 in the Maximillian Schrems v Data Protection Commissioner case (C-362-14). Brussels, 16 October 2015. Saatavissa: http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (Katsottu 24.4.2018).

Article 29 Working Party. Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision (16/EN WP 238) 13.4.2016. Saatavissa: http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf (Katsottu 14.4.2018).

Article 29 Working Party. Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, 26.7.2016. Saatavissa: http://ec.europa.eu/justice/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf (Katsottu 24.4.2018).

Article 29 Working Party. 17/EN WP 255. EU – U.S. Privacy Shield – First annual Joint Review. Saatavissa: https://iapp.org/media/pdf/resource_center/Privacy_Shield_Report-WP29pdf.pdf (Katsottu 24.4.2018).

Article 29 Working Party. Press release 11.4.2018. Sorry is not enough – WP29 establishes a Social Media Working Group. https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf (Katsottu 30.4.2018).

Euroopan unionin perusoikeusvirasto ja Euroopan neuvosto. Käsikirja Euroopan tietosuojaoikeudesta 2014. Saatavissa: https://rm.coe.int/16806ae651 (Katsottu 24.4.2018).

Yhdysvaltojen lainsäädäntö ja virallislähteet

The Constitution of the United States. Saatavissa: https://constitution.findlaw.com/ (Katsottu 18.4.2018).

Federal Trade Commission Act. [Chapter 311, 38 Stat. 717, September 26, 1914] [As Amended Through Public Law 111–203, Enacted July 21, 2010].

https://legcounsel.house.gov/Comps/Federal%20Trade%20Commission%20Act.pdf (Katsottu 24.4.2018).

USA Freedom Act of 2015. Public Law No. 114-23. Saatavissa: https://www.congress.gov/bill/114th-congress/house-bill/2048/text (Katsottu 24.4.2018).

Foreign Intelligence Surveillance Act of 1978. 1 [Public Law 95–511; 92 Stat. 1783; approved October 25, 1978] [As Amended Through P.L. 115–118, Enacted January 19, 2018] Saatavissa: https://legcounsel.house.gov/Comps/Foreign%20Intelligence%20Surveillance%20Act%20Of%201978.pdf (Katsottu 25.4.2018).

Children's Online Privacy Protection Act of 1998. Saatavissa: http://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title15-section6501&edition=prelim (Katsottu 15.4.2018).

Civil Code Sec. 1798.82. The California Security Breach Information Act. Senate Bill No. 1386. Saatavissa: https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=200120020SB1386 (Katsottu 15.4.2018).

Online Privacy Protection Act of 2003. California Business and Professions Code. Saatavissa: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=8.&chapter=22.&lawCode=BPC (Katsottu 24.4.2018).

Civil Code 1798.83. Saatavissa: https://codes.findlaw.com/ca/civil-code/civ-sect-1798-83.html (Katsottu 15.4.2018).

The Massachusetts Data Security Regulation. Saatavissa: http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf (Katsottu 15.4.2018).

United States Foreign Intelligence Surveillance Court. Secondary Order. https://assets.documentcloud.org/documents/709012/verizon.pdf (Katsottu 12.4.2018).

EU-U.S. Privacy Shield Framework Principles. Saatavissa: https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf (Katsottu 14.4.2018).

US White House. A Framework for Global Electronic Commerce, 1997. Saatavissa: http://clinton4.nara.gov/WH/New/Commerce (Katsottu 11.4.2018).

Federal Trade Commission. Privacy & Data Security. Update: 2017. Saatavissa: https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2017-overview-commissions-enforcement-policy-initiatives-consumer/privacy_and_data_security_update_2017.pdf (Katsottu 24.4.2018).

Euroopan unionin tuomioistuin

Euroopan unionin tuomioistuin. Julkisasiamies Yves Bot: Ratkaisuehdotus 23.9.2015 asiassa C-362/14 Maximillian Schrems vastaan Data Protection Commissioner. Saatavissa: http://curia.europa.eu/juris/celex.jsf?celex=62014CC0362&lang1=en&type=TXT&ancre= (Katsottu 13.2.2018).

Euroopan unionin tuomioistuin. Lehdistötiedote 117/15. Saatavissa: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf (Katsottu 18.1.2018).

Oikeuskäytäntö

Euroopan unionin tuomioistuin. Tuomio asiassa C-362/14. Saatavissa: http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=FI (Katsottu 22.1.2018).

Euroopan unionin tuomioistuin. Tuomio asiassa C-131/12. Saatavissa: https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:62012CJ0131&from=FI (Katsottu 24.4.2018).

Euroopan unionin tuomioistuin. Tuomio asiassa C-293/12 ja C-594/12. Saatavissa: http://curia.europa.eu/juris/document/document.jsf?text=&docid=150642&pageIndex=0&doclang=fi&mode=lst&dir=&occ=first&part=1&cid=360741 (Katsottu 24.4.2018).

Euroopan unionin tuomioistuimen asiat

Digital Rights Ireland v Commission. Case T-670/16. http://curia.europa.eu/juris/liste.jsf?language=en&jur=C%2CT%2CF&num=T-670%252F16 (Katsottu 24.4.2018).

La Quadrature du Net and Others v Commission. Case T-738/16. http://eur-lex.europa.eu/legal-content/en/TXT/PDF/?uri=uriserv%3AOJ.C_.2017.006.01.0039.01.ENG (Katsottu 24.4.2018).

Lehtiartikkelit

Kaivola, Tuomas. Artikkeleita eurooppaoikeudesta: Euroopan unionin tuomioistuimen viimeaikainen oikeuskäytäntö ja uudistuva tietosuojalainsäädäntö, Defensor Legis 5/2016, s. 862 – 872.

Kuner, Christopher. Reality and Illusion in EU Data Transfer Regulation Post Schrems. German Law Journal Vol. 18 No. 04, 2017.

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

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

Reidenberg, Joel R. The Simplification of International Data Privacy Rules, 29 Fordham Int'l L.J. 1128 (2005-2006). Fordham University School of Law.

Reidenberg, Joel R. E-Commerce and Trans-Atlantic Privacy, 38 Hous. L. Rev. 717 (2001-2002). Fordham University School of Law.

Saarenpää Ahti. Verkkoyhteiskunnan oikeutta - johdatusta aiheeseen. Oikeus 1/ 2000, s. 3-14.

Schaffer, Gregory. Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards. Yale Journal of International Law 2000.

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.

Swire, Peter. Elephants and Mice Revisited: Law and Choice of Law on the Internet. University of Pennsylvania Law Review 2005.

Walkila, Sonya. Artikkeleita eurooppaoikeudesta – Perusoikeuksien turvaaminen Euroopan unionissa – Tasapainoilua tavoitteiden ja keinojen ristiaallokossa. Defensor Legis N:o 4/2015. s. 791 – 807.

Kansainväliset sopimukset

Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (108/1981). Saatavissa: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680078b37 (Katsottu 24.4.2018).

Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data 23.8.1980. Päivitetyt ohjeet saatavissa: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm (Katsottu 9.3.2018).

Kansalais- ja poliittisia oikeuksia koskeva yleissopimus. http://www.globalis.fi/view/content/3655/full/1/2245 (Katsottu 8.3.2018).

Muut lähteet ja artikkelit

Bygrave, Lee A. Transatlantic Tensions on Data Privacy. Transworld Working Paper 19/April 2013. Saatavissa: http://iaitestnew.asw.bz/sites/default/files/TW_WP_19.pdf (Katsottu 18.4.2018).

Connolly, Chris. The US Safe Harbor – Fact or Fiction, 2008. Saatavissa: http://www.galexia.com/public/research/assets/safe_harbor_fact_or_fiction_2008/safe_harbor_fact_or_fiction.pdf (Katsottu 19.4.2018).

Ieuan, Jolly. US Privacy and Data Security Law: Overview, 2016. Saatavissa: https://blog.richmond.edu/lawe759/files/2016/08/US-Privacy-and-Data-Security-Law-Overview.pdf (Katsottu 24.4.2018).

Meltzer, Joshua P. Brookings. Global Economy and Development Working Paper 79/2014. The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment. Saatavissa: https://www.brookings.edu/wp-content/uploads/2016/06/internet-transatlantic-data-flows-version-2.pdf (Katsottu 20.4.2018).

Schrems, Maximillian. Initial Response October 6th 2015. Saatavissa: http://www.europe-v-facebook.org/CJEU_IR.pdf (Katsottu 14.4.2018).

Council of Europe. Committee of Ministers. Resolution 95 (37) on Observer Status for the United States of America with the Council of Europe. Saatavissa: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016804c8c35 (Katsottu 24.4.2018).

Internet-lähteet

European Commission. EU Position in World Trade. http://ec.europa.eu/trade/policy/eu-position-in-world-trade/ (Katsottu 22.1.2018).

Euroopan komissio. Tietosuoja EU:ssa. https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi (Katsottu 30.4.2018).

Council of Europe. Member States. https://www.coe.int/en/web/about-us/our-member-states (Katsottu 8.3.2018)

Statista. European Union: Total Population from 2007 to 2017. https://www.statista.com/statistics/253372/total-population-of-the-european-union-eu/ (Katsottu 30.4.2018).

Statista. Facebook's monthly Active Users in Europe from 4th quarter 2012 to 4th quarter 2017. https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ (Katsottu 15.4.2018).

Statista. LinkedIn: Registered Members Worldwide as of 1st quarter 2016. https://www.statista.com/statistics/272783/linkedins-membership-worldwide-by-country/ (Katsottu 22.1.2018).

Eurostat. International Trade in Goods. http://ec.europa.eu/eurostat/news/themes-in-the-spotlight/trade-in-goods-2016 (Katsottu 15.1.2018).

The U.S. – EU Safe Harbor List. https://www.export.gov/safeharbor_eu (Katsottu 14.1.2018).

Privacy Shield Framework. Privacy Shield List. https://www.privacyshield.gov/list (Katsottu 15.4.2018).

Privacy Shield Framework. Facebook, Inc. https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC&status=Active (Katsottu 20.4.2018).

Facebook. Yrityksen tiedot. https://www.facebook.com/pg/facebook/about/?ref=page_internal (Katsottu 18.1.2018).

Facebook. Legal Terms. https://www.facebook.com/legal/terms/update (Katsottu 19.1.2018).

The New York Times 4.4.2018. Cambridge Analytica and Facebook: The Scandal and the Fallout so far. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html (Katsottu 15.4.2018).

The New York Times 17.3.2018. How Trump Consultants Exploited the Facebook Data of Millions. https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

The Guardian 7.6.2013. NSA Prism Program Taps in to User Data of Apple, Google and others. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (Katsottu 12.4.2018).

The Guardian 31.7.2013. XKeyscore: NSA tool collects ”nearly everything a user does on the Internet. https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (Katsottu 12.4.2018).

The Guardian 26.11.2013. NSA Surveillance: Europe threatens to freeze US data-sharing arrangements. https://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing (Katsottu 15.4.2018).

The Guardian 9.10.2015. Tech companies like Facebook not above the law, says Max Schrems. https://www.theguardian.com/technology/2015/oct/09/facebook-data-privacy-max-schrems-european-court-of-justice (Katsottu 14.4.2018).

EU Observer 22.7.2013. EU questions decade-old US data agreement. https://euobserver.com/justice/120919 (Katsottu 15.4.2018).

EU Observer 13.7.2016. Privacy Shield will not survive legal challenge, says Schrems. https://euobserver.com/digital/134322 (Katsottu 24.4.2018).

EU Observer 8.9.2016. Snowden: Privacy Shield won’t stop US mass surveillance https://euobserver.com/justice/134958 (Katsottu 24.4.2018).

BBC 20.3.2018. Cambridge Analytica: Facebook being investigated by FTC. http://www.bbc.com/news/world-us-canada-43476594

Electronic Frontier Foundation. Commentary 3.3.2016: The Privacy Shield is Riddled with Surveillance Holes. https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes (Katsottu 21.4.2018).

Civil Society Coalition. Letter 16.3.2016. https://edri.org/wp-content/uploads/2016/03/PrivacyShield_Letter_Coalition_March2016.pdf (Katsottu 24.4.2018).

Electronic Privacy Information Center 18.1.2018. Congress Renews Controversial Surveillance Measure, EU Impacted. https://epic.org/2018/01/congress-renews-controversial-.html (Katsottu 21.4.2018).

LYHENTEET

CIA	Central Intelligence Agency
EFF	Electronic Frontier Foundation
EIS	Euroopan neuvoston ihmisoikeussopimus
EN	Euroopan neuvosto
EPIC	Electronic Privacy Information Center
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
FBI	Federal Bureau of Investigation
FISA	Foreign Intelligence Surveillance Act
FTC	Federal Trade Commission
HE	Hallituksen esitys
KP-sopimus	Kansalais- ja poliittisia oikeuksia koskeva yleissopimus
NSA	National Security Agency
NSL	National Security Letter
OECD	The Organisation for Economic Cooperation and Development
PeVL	Perustuslakivaliokunnan lausunto
PL	Perustuslaki
SEU	Sopimus Euroopan unionista
SEUT	Sopimus Euroopan unionin toiminnasta
WP	Working party, direktiivin 95/46/EY 29 artiklalla perustettu tietosuojatyöryhmä
WWW	World Wide Web

1 JOHDANTO

1.1. Henkilötietojen muuttunut käsittely-ympäristö

Viime vuosikymmenten aikana teknologian kehitys on ollut nopeaa ja nykyään merkittävä osa työstämme, yhteydenpidostamme muihin ihmisiin ja päivittäisten asioiden hoitamisestamme tapahtuu tietoverkkoja hyödyntäen. Käytämme tietoverkkoja monien elämämme tärkeiden toimintojen tekemiseen: haemme työ- ja opiskelupaikkoja, maksamme laskuja ja teemme muuttoilmoituksia. Avointen tietoverkkojen hyödyntäminen on elämisen arkipäivää jo suuressa osassa maailmaa.[1] Tiedon siirtäminen on helppoa ja tietoverkon hyödyntäminen on nopeuttanut elämäämme merkittävästi. Yhteiskuntamme näyttää pikkuhiljaa rakentuneen tietotekniikan varaan.

Erilaisten tiedostojen, viestien ja muun informaation lisäksi jaamme verkossa henkilötietojamme. Verkkoyhteiskunnan muodostuminen on luonut aivan uudenlaisen ympäristön henkilötietojen käsittelylle ja säilyttämiselle, kun tietojamme on erilaisilla alustoilla, palvelimilla ja tietojärjestelmissä. On tavallista, että tilatessamme tavaroita verkkokaupasta laskulla, verkkokauppa vaatii muiden henkilötietojen ohella myös henkilötunnuksemme. Kun luomme tilin sosiaalisen median palveluun, palvelu vaatii kirjautumisvaiheessa henkilötiedoiksi luokiteltavia tietoja itsestämme. Myös valokuva luokitellaan henkilötiedoksi silloin, kun se voidaan tunnistaa tiettyä luonnollista henkilöä koskevaksi.[2] Mitä laajemmin toimimme verkossa, sitä enemmän tietoa meistä muodostuu sen syövereihin.

Teknologian kehitys tuo eteemme jatkuvasti uusia henkilötietojen suojaa säätelevän tietosuojalainsäädännön sääntelyn ja tulkinnan ongelmia.[3] Euroopan unioni (EU) on ollut tietosuojan sääntelyssä edistyksellinen ja henkilötietojen suoja on yksi Euroopan unionin perusoikeuskirjassa määritellyistä perusoikeuksista. Unionin tietosuojasäädökset luovat yksityisyyden suojan perustan valtavan suurelle ihmisjoukolle. Euroopan unioni on maailman suurin talous.[4]

[1] Saarenpää 2008, s. 135.
[2] Ks. Pitkänen, Tiilikka, Warma 2013, s. 44.
[3] Saarenpää 2016, s. 76.
[4] http://ec.europa.eu/trade/policy/eu-position-in-world-trade/

Henkilötietodirektiivi (95/46/EY) on toiminut perustana unionin jäsenvaltioiden kansalaisten henkilötietojen suojelulle pitkään, mutta toukokuussa 2018 tulee sovellettavaksi EU:n uusi henkilötietodirektiivin korvaava tietosuoja-asetus[5]. Tietosuoja-asetuksen myötä unionin tietosuojasääntely tarkentuu huomattavasti, sillä uudessa asetuksessa on kolminkertainen määrä artikloja tietosuojadirektiiviin verrattuna.[6]

1.2. Sähköisen liiketoiminnan kansainvälinen kasvu

Sähköinen liiketoiminta on kasvanut merkittävästi viimeisen parinkymmenen vuoden aikana. Verkkoyhteiskunnan kehittyminen on mahdollistanut ja helpottanut yritysten monikansallistumista ja kansainvälisen kaupan kasvua. Perinteiset kivijalkayritykset ovat laajentaneet toimintaansa tietoverkkoon ja valtava määrä yrityksiä toimii ainoastaan verkossa. Verkossa toimiessaan yrityksille ja niiden käyttämille palvelimille kertyy valtavat tietovarannot, joiden joukossa on myös asiakastietoja. Liiketoiminta ei ole mahdollista ilman omien ja toisten tietojen käsittelyä ja käyttöä.[7]

Henkilötietoja siirretään paljon Euroopan ulkopuolelle, sillä Googlen ja Facebookin kaltaiset amerikkalaiset yritykset ovat markkinajohtajia digitaalisissa palveluissa.[8] Esimerkiksi verkkoyhteisöpalvelu LinkedIn:llä (LinkedIn Corporation), joka on rekisteröity Yhdysvaltoihin, oli vuoden 2016 alussa 11 miljoonaa rekisteröitynyttä käyttäjää Ranskassa, 8 miljoonaa Espanjassa ja 2 miljoonaa Ruotsissa.[9] Euroopan komissio on todennut henkilötietojen siirron olevan olennainen osa Atlantin yli käytävää kauppaa, jonka yhteydessä siirretään suuria tietomääriä EU:sta Yhdysvaltoihin.[10]

[5] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta. EU:n yleistä tietosuoja-asetusta (General Data Protection Regulation) sovelletaan 25.5.2018 alkaen kaikissa Euroopan unionin jäsenmaissa.
[6] Kaivola 2016, s. 863. Henkilötietodirektiivistä (95/46/EY) on käytetty myös nimeä tietosuojadirektiivi.
[7] Pesonen 2012, s. 14.
[8] Kaivola 2016, s. 864.
[9] https://www.statista.com/statistics/272783/linkedins-membership-worldwide-by-country/
[10] COM (2013) 846 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle: Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon, s. 2.

Sähköisen liiketoiminnan kehittyminen ja kansainvälistyminen ovat asiakkaiden henkilötietojen suojan osalta nostaneet esiin uudenlaisia sääntelytarpeita, kun on ollut tarpeen aikaansaada sääntelyä palvelimien ja tietojärjestelmien tietosuojavaatimuksista ja samalla luoda sääntelystä kansainvälisesti sitovaa. Verkkoyhteiskunnassa maantieteellisten rajojen fyysinen vaikutus vähenee, mutta rajojen oikeudellinen ylittäminen voi olla haastavaa etenkin ylitettäessä Euroopan unionin rajat.[11]

1.3. Henkilötietojen siirto Euroopan unionista Yhdysvaltoihin

Yhdysvallat on Euroopan unionin merkittävin kauppakumppani.[12] Yhdysvalloissa ei ole yleistä tietosuojalainsäädäntöä, vaan siellä käytetään alakohtaista lähestymistapaa, jossa yhdistyvät lainsäädäntö, sääntely ja itsesääntely.[13] Euroopan unionissa on informaatioteknologian kehittyessä nähty ongelmallisena henkilötietojen suojan mahdollinen riittämättömyys silloin, kun yhdysvaltalaiset yritykset vastaanottavat, käsittelevät, säilyttävät ja siirtävät unionin kansalaisten henkilötietoja tietojärjestelmissään. Yhdysvalloissa ei ole sellaista lainsäädäntöä, jonka nojalla Euroopan komissio olisi katsonut, että lainsäädäntö turvaisi tietosuojan riittävän tason vaatimuksen ja tietojen siirto EU:n jäsenvaltiosta olisi siten mahdollista.[14] Euroopan unionissa henkilötietojen suojalla on perusoikeuden asema.

Euroopan komissio antoi vuonna 2000 päätöksen 2000/520/EY yksityisyyden suojaa koskevien Safe Harbor-periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä.[15] Päätöksessä määritettiin henkilötietojen suojan käsittelylle oikeudelliset reunaehdot silloin, kun yhteisöstä siirretään henkilötietoja Yhdysvaltoihin sijoittuneille organisaatioille. Reunaehtoja

[11] Ks. Saarenpää 2016, s. 78-79.
[12] http://ec.europa.eu/eurostat/news/themes-in-the-spotlight/trade-in-goods-2016
[13] Komission päätös 2000/520/EY liite 1: Yhdysvaltojen kauppaministeriön 21 päivänä heinäkuuta 2000 antamat Safe Harbor-periaatteet.
[14] Pitkänen, Tiilikka, Warma 2013, s. 185.
[15] 2000/520/EY: Komission päätös, tehty 26 päivänä heinäkuuta 2000, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien Safe Harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä (tiedoksiannettu numerolla K (2000) 2441).

kutsuttiin Safe Harbor-periaatteiksi ja niitä sovellettiin Euroopan unionista Yhdysvaltoihin siirrettyjen henkilötietojen käsittelyssä vuoteen 2015 asti. Safe Harbor-järjestelyssä mukana olleista yhdysvaltalaisista, kansainvälisesti merkittävistä yrityksistä voidaan mainita esimerkiksi Pfizer, Facebook, Microsoft, Google, Apple ja Nike.[16]

Euroopan unionin tuomioistuin (EUT) totesi lokakuussa 2015 tekemässään ratkaisussa C-362/14 Safe Harbor-periaatteet pätemättömiksi.[17] Ratkaisu aiheutti hetkellisen sääntelyaukon henkilötietojen siirrossa unionista Yhdysvaltoihin niiden yhdysvaltalaisten yritysten osalta, jotka siirsivät henkilötietoja Safe Harbor-periaatteiden mukaisesti. Tuon sääntelyaukon täyttämiseksi Euroopan komissio hyväksyi EU:n ja Yhdysvaltojen välisen Privacy Shield-järjestelyn heinäkuussa 2016.[18] Privacy Shield pyrkii turvaamaan Euroopan unionin alueella asuvan henkilön tietosuojaperusoikeudet silloin, kun tämän henkilötietoja siirretään Yhdysvaltoihin. Lokakuussa 2017 järjestelystä annettiin ensimmäinen vuosiraportti.[19]

1.4. Tutkielman rakenne

Esittelen tutkielman aiheen, Privacy Shield-järjestelyn luvussa 2. Samassa luvussa käyn läpi maisteritutkielmani aihevalintaan vaikuttaneet tekijät ja tutkielman tavoitteet. Esittelen myös tutkielman lainopillisen metodin ja käyn läpi oikeusinformatiikan tutkimusalaa.

Tutkielman kannalta oleellisimmat käsitteet esittelen luvussa 3. Esitetyt käsitteet ovat yleisiä tietosuojaan, yksityisyyden suojaan ja henkilötietojen suojaan liittyviä, tutkielman kannalta relevantteja käsitteitä. Unionin uusi tietosuoja-asetus tulee sovellettavaksi toukokuussa 2018, jolloin henkilötietodirektiivin soveltaminen lakkaa. Tutkielmani valmistuu keväällä 2018, joten olen katsonut tarkoituksenmukaisemmaksi esitellä käsitteet,

[16] https://www.export.gov/safeharbor_eu
[17] Euroopan unionin tuomioistuin: Tuomio asiassa C-362/14.
[18] Komission täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä (tiedoksiannettu numerolla C (2016) 4176).
[19] COM (2017) 611 final. Komission kertomus Euroopan parlamentille ja neuvostolle EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toiminnan ensimmäisestä vuosittaisesta tarkastelusta.

joiden sisältö määritellään tietosuoja-asetuksessa, uuden asetuksen mukaisesti. Luvussa 4 käsittelen henkilötietojen suojan sääntelyä niin kansallisesti kuin Euroopan unionin oikeudessa. Luvussa tarkastelen myös ylikansallisia tietosuojan sääntelykeinoja, kuten OECD:n antamia tietosuojasuosituksia.

Tutkielman luvussa 5 esittelen tietosuojasääntelyn rakennetta Yhdysvalloissa. Jotta voidaan ymmärtää Euroopan unionin ja Yhdysvaltojen välinen konflikti henkilötietojen suojan sääntelyssä, on perehdyttävä siihen, millä tavoin henkilötietojen suojaa ja yksityisyyttä säädellään Yhdysvaltain lainsäädännössä. Luku 6 käsittelee henkilötietojen siirtoa Euroopan unionista Yhdysvaltoihin vuosina 2000–2015 säännellyttä Safe Harbor-järjestelyä. Luvussa 7 esittelen Euroopan unionin tuomioistuimen ratkaisun C-362/14, jossa tuomioistuin totesi Safe Harbor-periaatteet pätemättömiksi.

Luvussa 8 tarkastelen voimassa olevaa Privacy Shield-järjestelyä ja sen eroja Safe Harbor-järjestelyyn. Luvussa käyn myös läpi lokakuussa 2017 julkaistun ensimmäisen Privacy Shield-järjestelyn vuosiraportin. Tarkastelen lisäksi Privacy Shield-sopimusjärjestelyn sekä uuden tietosuoja-asetuksen välistä keskinäistä suhdetta. Luvussa 9 esittelen henkilötietojen suojan transatlanttisen sääntelyn tulevaisuuden näkymiä ja tutkielman johtopäätökset.

2 TUTKIMUSAIHEEN ESITTELY

2.1. Tutkimuksen kohde

Euroopan unionin tietosuojan sääntely on viime aikoina uudistunut ja tulee lähiaikoina uudistumaan huomattavasti. Vaikuttaa siltä, että samalla, kun informaatioteknologinen kehitys on otettu avosylin vastaan, tietosuoja-asioiden sääntely yksilön näkökulmasta ja yksilön oikeuksien kunnioittamisen kautta on vähitellen otettu jopa ensiarvoiseksi tavoitteeksi sääntelyn kehittämisessä ainakin EU:n toimesta. Yhä useammista informaatioon, tietojenkäsittelyyn ja viestintään liittyvistä, ihmistä koskevista asioista on säädettävä laissa ja tuo sääntely tapahtuu enenevässä määrin yksilön oikeuksien näkökulmasta.[20]

Unionin alueella asuvien ihmisten henkilötietojen suojaa turvaava Privacy Shield-järjestely on ollut voimassa pian kahden vuoden ajan ja EU:n uusi tietosuoja-asetus tulee sovellettavaksi vuonna 2018. Tietosuoja-asetuksen tarkoituksena on ajantasaistaa tietosuojaa koskevaa sääntelyä, jotta voidaan vastata teknologian kehitykseen ja globalisaatioon liittyviin henkilötietojen suojaa koskeviin haasteisiin.[21]

Privacy Shield valikoitui tutkielmani aiheeksi ensinnäkin sen ajankohtaisuuden vuoksi. Edelliset henkilötietojen siirtoa unionista Yhdysvaltoihin säännelleet Safe Harbor-periaatteet julistettiin pätemättömiksi vasta pari vuotta sitten, lokakuussa 2015. Sääntelyaukko saatiin täytettyä verrattain nopeasti, kun Privacy Shield-järjestely tuli voimaan heinäkuussa 2016.

Privacy Shield on alusta alkaen saanut osakseen myös paljon kritiikkiä, eikä sen tehokkuudesta ole vallinnut yksimielisyyttä edes Euroopan unionin toimielinten sisällä.[22] Se ei myöskään ole ainut henkilötietodirektiivin tai tietosuoja-asetuksen mahdollistama menetelmä henkilötietojen siirtämiselle Yhdysvaltoihin. Privacy Shield on kuitenkin se oikeudellinen perusta, jonka

[20] Saarenpää 2016, s. 80.
[21] Oikeusministeriö, Tietosuojavaltuutetun toimisto. Selvityksiä ja ohjeita 4/2017, s. 9.
[22] Euroopan unionin toimielinten toisistaan poikkeavia näkemyksiä Privacy Shield-järjestelyn tehokkuudesta käsitellään luvussa 8.

nojalla miljoonien eurooppalaisten henkilötietoja siirretään yhdysvaltalaisille yrityksille, joten sen vaikutus on valtava.[23] Järjestelyyn sitoutuneita yrityksiä ovat esimerkiksi Microsoft ja Facebook.[24]

Toinen syy sille, miksi haluan tarkastella Privacy Shield-järjestelyä, on Euroopan unionin koko ajan kehittyvä ja tarkentuva tietosuojasääntely. Teknologian kehittyessä henkilötietojen suojan sääntelyn tarve kasvaa koko ajan ja Euroopan unioni on pyrkinyt vastaamaan siihen käynnissä olevalla tietosuojauudistuksella. Valitsin aiheekseni Privacy Shield-järjestelyn, koska se määrittelee henkilötietojen siirtoa Yhdysvaltoihin. Yhdysvallat on valtio, joihin tietoja siirretään unionista kaikista eniten.[25] Samalla se on valtio, jossa tietosuoja-asioista säädetään hyvin erilaisista lähtökohdista kuin Euroopan unionissa. Erilaiset näkemykset henkilötietojen suojan sääntelystä ovat jo pitkään aiheuttaneet konflikteja unionin ja Yhdysvaltojen välille ja viime vuosien suuret, henkilötietojen suojan loukkaamiseen liittyvät paljastukset, kuten Edward Snowdenin esiin tuoma Yhdysvaltain suorittama massavalvonta tai Facebookin Cambridge Analytica-kohu, ovat liittyneet juuri Yhdysvaltain viranomaisiin tai yhdysvaltalaisiin yrityksiin.[26]

Privacy Shield-sopimusjärjestelyn linkittyminen Euroopan unionin oikeuteen ja Yhdysvaltojen tietosuojasääntelyyn ja käsityksiin yksityisyyden suojasta sekä järjestelyn erityinen perusoikeudellinen näkökulma tekevät siitä tutkimuskohteena kiinnostavan. Uuden tietosuoja-asetuksen astuessa voimaan on tarpeen määritellä myös asetuksen ja Privacy Shield-järjestelyn keskinäistä suhdetta.

Tutkielmani tavoitteena on selvittää, kuinka Privacy Shield toimii ja turvaa henkilötietojen suojaa. Lisäksi pyrin selvittämään ja jäsentelemään unionista Yhdysvaltoihin siirrettävien henkilötietojen sääntelyn taustoja ja lähtökohtia ja siksi perehdyn myös Safe Harbor-järjestelyyn. Tarkastelen Safe Harbor-periaatteiden ja Privacy Shield-järjestelyn eroavaisuuksia ja pyrin

[23] https://www.statista.com/statistics/253372/total-population-of-the-european-union-eu/ Vuoden 2017 lopussa Euroopan unionin väestöluku oli 511,81 miljoonaa. https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ Pelkästään Facebookilla oli vuoden 2017 loppuneljänneksellä 370 miljoonaa kuukausittain aktiivista käyttäjää Euroopassa.
[24] https://www.privacyshield.gov/list
[25] Meltzer 2014, s. 1. Yhdysvaltojen ja Euroopan unionin välinen rajat ylittävä tiedonsiirron määrä on maailman korkein.
[26] https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

selvittämään, onko järjestelyn ero Safe Harbor-periaatteisiin niin merkittävä, että siitä voi muodostua pysyvä ja pitkäaikainen ratkaisu henkilötietojen siirtoon unionista Yhdysvaltoihin. Tarkastelen lisäksi sitä, mitä vaatimuksia uusi tietosuoja-asetus asettaa henkilötietojen siirrolle kolmansiin maihin ja kuinka nuo vaatimukset vaikuttavat Privacy Shield-sopimusjärjestelyn soveltamiseen.

Tutkimuksen näkökulma on eurooppaoikeudellinen ja henkilötietojen suojan sääntelyä Euroopan unionin kansalaisen näkökulmasta tutkiva. Haasteensa tälle tutkimukselle asettaa se, että järjestelmän uutuudesta johtuen sen tehokkuudesta saadut kokemukset ovat vähäisiä. Sen takia koen tarpeelliseksi perehtyä siihen, kuinka järjestely toimii, millä tavoin Privacy Shield-periaatteet sääntelevät henkilötietojen siirtoa Yhdysvaltoihin ja miten järjestelyyn on suhtauduttu Atlantin molemmin puolin.

Tässä tutkielmassa oma roolinsa on Euroopan unionin tuomioistuimen ratkaisulla C-362/14, koska se toimi merkittävänä sysäyksenä Privacy Shield-järjestelyn alkuun saattamiselle. Tapaus itsessään ei kuitenkaan ole tutkimukseni kohteena. Käyn tapausta läpi sen verran kuin on tarpeen sen selvittämiseksi, mitkä seikat vaikuttivat siihen, että Safe Harbor-järjestely julistettiin pätemättömäksi ja mikä tapauksesta teki niin merkittävän yksityishenkilön henkilötietojen suojan kannalta.

2.2. Tutkimuksen metodi ja lähteet

Tässä maisteritutkielmassa ensisijaisena tutkimuksen kohteena on Euroopan unionin ja Yhdysvaltojen välinen Privacy Shield-järjestely, jonka perustana on Euroopan komission täytäntöönpanopäätös 2016/1250. Tutkielmassa käytetään lähteinä voimassa olevaa lainsäädäntöä, lakien esitöitä, kotimaisia ja ulkomaisia virallislähteitä, kansainvälisiä tietosuojasuosituksia, oikeuskäytäntöä sekä oikeuskirjallisuutta.

Tutkimusmetodini on pääasiallisesti oikeusdogmaattinen eli lainopillinen. Lainoppi tutkii sitä, mikä on voimassaolevaa oikeutta ja mikä merkitys laista ja muista oikeuslähteistä löytyvällä materiaalilla on.[27] Itse sopimusjärjestelyä

[27] Hirvonen 2011, s. 23.

koskevan päätöksen lisäksi tarkasteltavana ovat Suomen kansallinen henkilötietojen suojaa koskeva lainsäädäntö sekä Euroopan unionin oikeuden henkilötietojen suojaa koskevat osat, joihin kuuluvat muun muassa uusi tietosuoja-asetus, Euroopan unionin perusoikeuskirja, väistyvä henkilötietodirektiivi sekä muita Euroopan unionin oikeuteen sisältyviä päätöksiä.

Suomen liittyminen Euroopan unionin jäseneksi vuonna 1995 on kasvattanut merkittävästi Suomea koskevien ja Suomessa sovellettavien oikeussääntöjen ja oikeuslähteiden kirjoa. Toki myös ennen unionin jäsenvaltion asemaa Suomi oli osapuolena lukuisissa kansainvälisissä sopimuksissa. *Saarenpää* huomauttaa, ettei Euroopan unionin merkittävää yleisempää vaikutusta oikeustieteemme kansainvälistymiseen voida sivuuttaa ja itse asiassa oikeuslähdeaineiston kansainvälistyminen on muuttamassa oikeustieteen kokonaisuudessaan enenevässä määrin kansainväliseksi.[28]

Lainopilla on perinteisesti katsottu olevan kaksi tehtävää: oikeudellisten käsitteiden konstruointi ja oikeussäännösten systematisointi näiden käsitteiden avulla sekä oikeussäännösten sisällön selvittäminen eli tulkinta ja niiden ajateltu soveltaminen.[29] Tarkastellessani sitä, minkälaisia toimintavelvoitteita Privacy Shield-sopimusjärjestely tuottaa ja kuinka velvoitteiden noudattaminen tapahtuu, tutkimukseni lähentelee metodiltaan käytännöllistä ja lainoppia ja *Aarnion* esittelemää säännösten toiminnan tarkastelua.[30] Oikeusnormilause antaa informaatiota oikeusnormin

[28] Ks. Saarenpää 2016, s. 86-87.

[29] Aarnio 1978, s. 52-53. Aarnion mukaan oikeustutkimuksen on katsottu tulleen ainakin liian suppeasti, ellei peräti väärin määritellyksi, jos siihen sisällytetään vain systematisointi ja säännösten tulkitseminen. Hänen mukaansa oikeudellisen tutkimuksen piiriin on haluttu lukea myös kolme muuta, itsenäiseksi käsitettyä tehtäväaluetta: *oikeussäännösten toiminnan tarkastelu, voimassa olevien säännösten ja instituutioiden arviointi ja lainlaadintaan liittyvien ongelmien tarkastelu eli oikeuspoliittinen tutkimus*. Aarnio 1978 s. 54 mukaan säännösten toiminnan tarkastelu on merkittävä oikeustutkimukseen kuuluva tehtävä. Tärkeys tulee näkyviin monella tavalla ja monissa eri kysymyksissä. Joskus on pidetty tärkeänä tutkia esimerkiksi sitä, keihin säännökset kohdistuvat (kohderyhmätutkimukset), millä tavoin säännökset rasittavat eri kohderyhmiä (rasitusvertailu) ja kuinka tehokkaasti jotakin säännöstä noudatetaan käytännössä (tehokkuustutkimus). Aarnio 1997, s. 37 jakaa lainopin teoreettiseen ja käytännölliseen lainoppiin, joilla kummallakin on oma metodinsa kuitenkin niin, että ne ovat vuorovaikutussuhteessa toisiinsa. Aarnio 1997 s. 43 mukaan teoreettinen lainoppi erittelee käsitteistöä ja jäsentää käsitteitä uudelleen, se siis systematisoi oikeussäännöksiä. Hirvonen 2011. s. 25 mukaan tulkintaa on pidetty lainopin praktisena ulottuvuutena ja tulkintalainoppia on yleensä kutsuttu käytännölliseksi lainopiksi. Myös oikeusperiaatteiden punninta ja tasapainottaminen kuuluvat ensisijaisesti käytännölliseen lainoppiin.

[30] Ks. Aarnio 1978, s. 54.

ajatussisällöstä, jota lainoppi tulkinnallaan pyrkii selvittämään, selventämään, täsmentämään ja ilmaisemaan.[31]

Laissa olevan oikeussäännön muoto on usein yleisluonteinen. Toisaalta säännös tulee jättää tietyllä tavalla avoimeksi, jotta se ei liian yksityiskohtaisella muotoilulla sulje pois sellaisia oikeudellisia tilanteita, joihin säännöksen on kuitenkin tarkoitettu soveltuvan. Jos säännös taas on liian yleisluonteinen, sen soveltumista juuri tietynlaiseen tilanteeseen voi olla hankala perustella. Yleensä lainvalmisteluaineistosta löytyy tarkempi perustelu siihen, mitä kyseisellä säännöksellä on tarkoitettu säätää. Lainoppi pyrkii siten löytämään vastauksen siihen, mitä tarkasteltavana oleva säännös merkitsee, mihin oikeudellisiin tilanteisiin se soveltuu ja mitä se lopulta säätelee. Yhtä tärkeää on selvittää, mitä jää säännöksen soveltuvuuden ulkopuolelle.

Oikeuslähteitä, kuten lainsäädäntöä, oikeuskäytäntöä ja oikeuskirjallisuutta syntyy koko ajan lisää. Toisaalta lainsäädännön muuttuessa ja esimerkiksi oikeuskäytännön kehittyessä jotkut oikeuslähteet menettävät merkitystään ja kumoutuvat uusien tullessa tilalle. Oikeuden käytössä on oltava selvillä ensinnäkin siitä, mitkä oikeuslähteet ovat ajantasaisia ja kyseiseen tilanteeseen sovellettavissa olevia. Oikeuden tulkitsijan on muodostettava käsitys siitä oikeuslähdekokoelmasta, jota hän voi perustellusti soveltaa. Toiseksi on osattava asettaa oikeuslähteet oikein niiden keskinäiseen järjestykseen. Kaikki oikeuslähteet eivät ole saman tasoisia ja mahdollisessa ristiriitatilanteessa on tiedettävä, kumpi oikeuslähde on velvoittavampi ja kumpaa on sovellettava. Oikeuslähteiden välityksellä tuomioistuimet, hallintoviranomaiset ja kansalaiset tunnistavat sen, mikä on oikeutta.[32]

Oikeuslähdeoppi on syntynyt tarpeesta luoda yleinen oppirakennelma, jonka avulla voidaan konkreettisessa soveltamis- ja tulkintatilanteessa ottaa rationaalisesti kantaa eri normilähteiden keskinäisiin suhteisiin ja määrittää

[31] Hirvonen 2011, s. 37. Hirvonen 2011 s. 38 – 40 jakaa tulkintaa määräävät periaatteet 1) sanamuodon mukaiseen tulkintaan 2) systemaattiseen tulkintaan 3) historialliseen tulkintaan 4) vertailevaan tulkintaan 5) supistavaan ja laajentavaan tulkintaan 6) analogiseen tulkintaan 7) teleologiseen eli tarkoitusperäopilliseen tulkintaan 8) arvoperusteiseen tulkintaan ja 9) objektiiviseen tulkintaan. Tulkintanormien etusijajärjestyksestä ei ole yleistä normia, mutta EU-oikeudessa on korostettu tarkoitusperäopillista tulkintaa ja perus- ja ihmisoikeusmyönteisessä lainopissa arvoperusteista tulkintaa.

[32] Myrsky 2010, s. 50.

niiden painoarvoja.[33] Oikeuslähteet on Aarnion oppia mukaillen tavattu jakaa vahvasti velvoittaviin, heikosti velvoittaviin ja sallittuihin oikeuslähteisiin.[34] Kun vahvasti velvoittaviksi oikeuslähteiksi luetaan muun muassa Eurooppaoikeuden sitovat osat ja kansallisen oikeuden osaksi saatetut kansainväliset sopimukset, tutkielmani pääasiallisen tarkastelun kohteena olevaa Euroopan komission täytäntöönpanopäätöstä Privacy Shield-sopimusjärjestelyn noudattamisesta voidaan pitää vahvasti velvoittavana oikeuslähteenä.

Eurooppaoikeuden oikeusjärjestys koostuu tavoitteista, periaatteista, politiikoista ja säännöistä, jotka edistävät integraatiota.[35] Oikeuden kansainvälistyessä ja Euroopan unionin oikeusjärjestyksen laajentuessa on tunnettava sekä Euroopan yhteisön oikeuden ja kansallisen lainsäädännön keskinäinen suhde, että eurooppaoikeudellisten lähteiden keskinäinen suhde. EU:n oikeus jakautuu primaarilainsäädäntöön ja sekundaarilainsäädäntöön. Primaarilainsäädäntö eli primaarioikeus koostuu unionin perussopimuksista ja niihin rinnastettavista sopimuksista. Keskeisiä primaarisopimuksia ovat Sopimus Euroopan unionista[36] (SEU) ja Sopimus Euroopan unionin toiminnasta[37] (SEUT). SEU 6 artiklan mukaan myös Euroopan unionin perusoikeuskirjalla on sama oikeudellinen arvo kuin perussopimuksilla.

Johdettuun oikeuteen eli sekundaarioikeuteen kuuluvat direktiivit, asetukset ja päätökset. Sekundaarinormit konkretisoivat primaarinormeissa esitettyjä periaatteita ja politiikkoja.[38] SEUT 288 artiklassa määritetään sekundaarioikeuden velvoittavuus; *asetukset* pätevät yleisesti, ovat kaikilta osiltaan velvoittavia ja niitä sovelletaan sellaisinaan kaikissa jäsenvaltioissa. *Direktiivi* velvoittaa saavutettavaan tulokseen nähden jokaista jäsenvaltiota,

[33] Nuotio 2004, s.1268.
[34] Aarnio 2011, s. 68. Aarnion mukaan oikeuslähteet voidaan jakaa eri kategorioihin sen mukaan, mikä on niiden velvoittavuuden aste. Vahvasti velvoittavia oikeuslähteitä ovat Aarnion mukaan 1) Kansallisen oikeuden ulkopuoliset normistot (Eurooppaoikeuden sitovat osat, Euroopan ihmisoikeussopimuksen normit, EY-tuomioistuimen tietyt prejudikaatit, Euroopan ihmisoikeustuomioistuimen tietyt prejudikaatit) 2) Kansallisen oikeuden normistot (Suomen perustuslain perusoikeudet, lait ja lakien nojalla annetut alemman asteiset normit, kansallisen oikeuden osaksi saatetut kansainväliset sopimukset, systeemiperusteet), 3) maan tapa. Aarnio 2011, s. 69 mukaan heikosti velvoittavia oikeuslähteitä ovat lainsäätäjän tarkoitus ja ennakkoratkaisut ja sallittuja oikeuslähteitä käytännölliset argumentit, eettiset ja moraaliset perusteet, yleiset oikeusperiaatteet, oikeustiede (vallitseva mielipide), vertailevat argumentit sekä muut.
[35] Raitio 2016, s. 195.
[36] Konsolidoitu toisinto EUVL 2016/C 202/01.
[37] Konsolidoitu toisinto EUVL 2016/C 202/01.
[38] Raitio 2016, s. 203.

jolle se on osoitettu, mutta jättää kansallisen viranomaisen valittavaksi muodon ja keinot. *Päätös* on kaikilta osiltaan velvoittava. Jos siinä nimetään ne, joille se on osoitettu, se velvoittaa ainoastaan niitä.

Tarkastellessa Euroopan unionin oikeuden ja jäsenvaltioiden kansallisen lainsäädännön keskinäistä suhdetta ja normihierarkiaa, etusijaperiaatteella on keskeinen merkitys. Etusijaperiaate tarkoittaa sitä, että ristiriitatilanteissa etusija on yleisesti annettava Euroopan yhteisön oikeudelle.[39] Periaate syntyi EU-tuomioistuimen ennakkoratkaisukäytännön myötä ja Lissabonin sopimuksen[40] yhteyteen on liitetty erillinen julistus Euroopan unionin oikeuden ensisijaisuudesta.[41]

2.3. Tutkimuksen ala

Maisteritutkielmani sijoittuu oikeusinformatiikan alalle, mutta se kytkeytyy kiinteästi myös persoonallisuusoikeuteen henkilötietojen suojan ollessa osa persoonallisuusoikeutta. Tutkielmassa on myös perusoikeudellinen näkökulma, sillä henkilötietojen suojalla on Euroopan unionin oikeudessa perusoikeusasema. Henkilötietojen suojaa järjestävä tietosuojalainsäädäntö on vakiintuneimpia oikeusinformatiikan lainopillisia tutkimusaiheita.[42] Henkilötietojen suoja kytkeytyy niin oikeusinformatiikan, persoonallisuusoikeuden, julkisoikeuden kuin hallinto-oikeuden aloihin.[43]

Oikeusinformatiikan oikeudenala on kehittynyt verraten rinnakkain teknologian kehityksen kanssa, joka on vain kiihtynyt viime vuosikymmenien aikana. Saarenpää on määritellyt oikeusinformatiikan oikeudenalaksi, jonka puitteissa tutkitaan ja opetetaan oikeuden ja informaation sekä oikeuden ja

[39] Tolonen 2003, s. 111.
[40] Lissabonin sopimus Euroopan unionista tehdyn sopimuksen ja Euroopan yhteisön perustamissopimuksen muuttamisesta (2007/C 306/01).
[41] Ks. Raitio 2016, s. 223-224. Lissabonin sopimukseen liitetyn 17. Julistus Euroopan unionin oikeuden ensisijaisuudesta mukaan Euroopan unionin tuomioistuimen vakiintuneen oikeuskäytännön mukaan perussopimukset ja unionin niiden nojalla antama lainsäädäntö ovat ensisijaisia jäsenvaltioiden oikeuteen nähden mainitussa oikeuskäytännössä määriteltyjen edellytysten mukaisesti.
[42] Saarenpää 2016, s. 75.
[43] Ks. Saarenpää 2016, s. 75-76. Saarenpää 2008, s. 144 huomauttaa henkilötietojen suojan olevan oikeuden ja tietojenkäsittelyn suhteeseen liittyvänä osa oikeusinformatiikkaa, yksilön itsemääräämisoikeuteen liittyvänä osa persoonallisuusoikeuttaja informaatioon liittyvänä osa modernia informaatio-oikeutta.

tietotekniikan välisiä suhteita yleisesti eri muodoissaan samoin kuin niiden yhteydessä ilmeneviä oikeudellisia sääntely- ja tulkintakysymyksiä.[44]

Oikeusinformatiikka tarkastelee kysymyksiä, jotka ovat etenkin eurooppalaisen yhteiskunnan kehityksessä, mutta nyttemmin myös enenevässä määrin maailmanlaajuisesti nousseet viime aikoina entistä merkittävämpään asemaan. Kehittyneestä tietosuojalainsäädännöstä on tullut yksi kansainvälisen kaupan kehittymisen perusedellytyksistä.[45] Privacy Shield-sopimusjärjestely määrittää nimenomaan henkilötietojen käsittelyn tietosuojan vaatimustasoa kansainvälisen kaupan yhteydessä siinä tilanteessa, jossa henkilötietojen siirretään Euroopan unionin alueelta yhdysvaltalaisille yrityksille.

Oikeusinformatiikalla on tänä päivänä välttämätön yhteys teknologiaan, tietokoneisiin ja tietojärjestelmiin, sillä verkkoyhteiskunnan kehittyminen on johtanut meidät tilanteeseen, jossa yhä suurempi osa yhteiskunnan toiminnoista järjestetään tietoverkoissa tai tietoverkkoja hyödyntäen. Voidaan puhua tietokannoista, tietopankeista, tietovarastoista ja tietojärjestelmistä, joihin tietoa ja informaatiota tallennetaan.[46] Alusta – *template* – on yksi digitaalisen oikeusvaltion avainsanoista.[47] Alustaa koskeva sääntely on myös Privacy Shield-järjestelyn ydinaluetta, sillä henkilötiedot tallennetaan erilaisille tietoverkossa oleville alustoille ja näiden alustojen tietosuojan tasoa Privacy Shield määrittää.

Tutkielman oikeusvertaileva näkökulma näyttäytyy Euroopan unionin ja Yhdysvaltojen tietosuojalainsäädännön lähtökohtien, rakenteiden ja tason vertailussa. Oikeusvertailun tavoitteena on hankkia informaatiota siitä, mikä tarkasteltavia oikeusjärjestelmiä erottaa ja mikä niitä yhdistää, sekä selittää tai arvioida, mistä erot tai yhtäläisyydet johtuvat.[48]

[44] Saarenpää 2016, s. 67.
[45] Saarenpää 2016, s. 78.
[46] Ks. Korhonen 2003, s. 18.
[47] Saarenpää 2016, s. 82.
[48] Husa 2013, s. 43.

3 KESKEISET KÄSITTEET

Tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan *henkilötiedolla* tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, liittyviä tietoja; tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella. Henkilöä kuvaava ominaisuus voi olla esimerkiksi ruumiinrakenteen kuvaus ja ominaisuuksia kuvaava tieto röntgenkuva.[49] Henkilötietoja ovat esimerkiksi henkilötunnus, tietokoneen IP-osoite ja sormenjälki.

Henkilötietoja tarvitaan esimerkiksi hyvinvointivaltiollisten palvelujen tarjoamiseen ja väestön hallinnointiin. Yhteiskunnan toimien tehostaminen, palveluiden käyttäminen ja tehokas toiminta markkinoilla edellyttävät, että yksilö luopuu osasta yksityisyyttään.[50] Henkilötiedon määritelmää voi kuvata melko avoimeksi.[51] Tämä kertoo osaltaan siitä, kuinka laaja-alaisesti henkilötietojen suojaa on katsottu tarpeelliseksi turvata.

Privacy Shield-järjestelyssä määrätään käytänteistä siinä tilanteessa, kun henkilötietoja siirretään yhdysvaltalaiselle yritykselle. Henkilötietoja ovat yrityksen eri tiedostoissa ja palvelimella olevat asiakkaan yhteystiedot, valvontakamerassa oleva asiakkaan kuva ja nauhoitteeseen tallentunut asiakkaan ääni sekä muu asiakkaalta jollakin muulla tavalla kerätty tieto. Tieto voi olla talletettu tietokantaan, www-palvelimelle, sähköpostiin, valvontakameran nauhalle tai ääninauhalle tai tietokoneen muistiin. [52]

[49] Voutilainen 2012, s. 246.
[50] Neuvonen 2014, s. 60.
[51] Ks. Vanto 2011, s. 22. Pitkänen, Tiilikka ja Warma 2013, s. 40 huomauttavat, että teknologian kehittyminen on tuonut mukanaan sellaisia tilanteita ja toimintatapoja, joita ei lakia säädettäessä ole osattu ajatella. Näissä tilanteissa on perusteltua tulkita henkilötiedon ja henkilörekisterin käsitteitä pikemmin laajasti kuin suppeasti. Pitkänen, Tiilikka ja Warma 2013, s. 47 huomauttavat lisäksi, että laajan määritelmän soveltamista puoltaa henkilötietolain tarkoituksena oleva yksityiselämän ja yksityisyyden suojaaminen ja hyvän tietojenkäsittelytavan edistäminen.
[52] Pesonen 2012, s. 17.

Henkilötietojen suojaa ja sen sääntelyä käydään tässä tutkielmassa läpi omassa luvussaan, mutta käsitteenä sen on muun muassa määritelty sisältävän persoonallisuuden ja siihen on yhdistetty tiedollinen itsemääräämisoikeus, joka tarkoittaa sitä, että henkilöllä tulisi olla mahdollisimman suuri mahdollisuus vaikuttaa siihen, kuka, miten ja missä käsittelee hänen henkilötietojaan.[53] Verkkoyhteiskunnan kehittymisen myötä henkilötiedoille on muodostunut uusi käsittelyalusta, kun henkilötietojamme on yhä enemmän tietoverkossa eri palvelimilla ja tietojärjestelmissä.

Yrityksen käsitellessä asiakkaan henkilötietoja se vastaanottaa tiedon ja käsittelee sitä. Yritys myös säilyttää henkilötietoja, saattaa luovuttaa niitä eteenpäin ja lopulta poistaa tiedot. Sähköpostiosoitteen keräämisen tarkoitus voi olla esimerkiksi asiakkaan tilaamaan tavaraan liittyvä yhteydenpito.[54] Tietosuoja-asetuksen 4 artiklan 2 kohta määrittelee *henkilötietojen käsittelyn* tarkoittavan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti, kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. *Henkilötietojen käsittelijä* on tietosuoja-asetuksen 4 artiklan 8 kohdan mukaan luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

Henkilötietojen siirto on osa henkilötietojen käsittelyä. Siirrolla tarkoitetaan tietojen tosiasiallista siirtämistä toiselle oikeushenkilölle ja siirrosta on kyse myös tilanteessa, jossa kolmas osapuoli voi teknisen yhteyden avulla ulkopuolelta käsitellä henkilötietoja, vaikka tiedot tosiasiallisesti sijaitsevat koko ajan samassa organisaatiossa.[55] Vapaan liikkuvuuden periaate soveltuu myös henkilötietojen siirtämiseen Euroopan unionin maiden välillä ja tietoja

[53] Ks. Neuvonen 2014, s. 59.
[54] Vanto 2011, s. 42.
[55] Pitkänen, Tiilikka ja Warma 2013, s. 52.

saa siirtää jäsenmaiden välillä samoin perustein kuin yhden jäsenmaan sisällä.[56]

Tietosuoja-asetuksen 4 artiklan 6 kohdan mukaan *rekisterillä* tarkoitetaan mitä tahansa jäsenneltyä henkilötietoja sisältävää tietojoukkoa, josta tiedot ovat saatavilla tietyin perustein, oli tietojoukko sitten keskitetty, hajautettu tai toiminnallisin tai maantieteellisin perustein jaettu. Laajoja ja yksittäisen henkilön henkilötietojen osalta hyvinkin kokonaisvaltaisia henkilörekistereitä syntyy erityisesti yhteisöpalvelujen, kuten Facebookin tarjoajille. Sosiaalisen median käyttö perustuu käyttäjien henkilötietojen käsittelyyn ja palveluntarjoajan keräämät asiakastiedot muodostavat henkilörekisterin.[57]

Tietosuoja-asetus ei erikseen määrittele *rekisteröidyn* käsitettä, mutta 4 artiklan 1 kohdassa henkilötiedon käsitteen määrittelyssä puhutaan ”luonnollisesta henkilöstä, jäljempänä rekisteröidystä”. Henkilötietolain (523/1999) 3 § 5 kohdan mukaan rekisteröidyllä tarkoitettiin henkilöä, jota henkilötieto koskee. *Rekisterinpitäjällä* tarkoitetaan asetuksen 4 artiklan 7 kohdan mukaan luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot; jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti.

Henkilötietojen käsittely voi perustua esimerkiksi *rekisteröidyn suostumukseen.* Tietosuoja-asetuksen 4 artiklan 11 kohdan mukaan rekisteröidyn suostumuksella tarkoitetaan mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua, jolla rekisteröity hyväksyy henkilötietojensa käsittelyn antamalla suostumusta ilmaisevan lausuman tai toteuttamalla selkeästi suostumusta ilmaisevan toimen. Muun muassa sosiaalisen median palvelut keräävät käyttäjien henkilötietoja käyttöehtojen hyväksymisen yhteydessä annetun suostumuksen perusteella.[58]

[56] Ks. Salminen 2009, s. 83-84.
[57] Pesonen 2013, s. 91.
[58] Pesonen 2013, s. 96.

Tietoturvan[59] käsitettä on määritelty tietoyhteiskuntakaaren[60] (917/2014) 3 §:n 28 kohdassa, jonka mukaan tietoturvalla tarkoitetaan hallinnollisia ja teknisiä toimia, joilla varmistetaan se, että tiedot ovat vain niiden käyttöön oikeutettujen saatavilla, että tietoja eivät voi muuttaa muut kuin siihen oikeutetut sekä että tiedot ja tietojärjestelmät ovat niiden käyttöön oikeutettujen hyödynnettävissä. Tietoturvan rinnalla voidaan puhua myös *tietoturvallisuudesta*. Säädöstasolla käsitteet vastaavat toisiaan ja niillä tarkoitetaan tietoon liittyvien ominaisuuksien hallintaa ja tiedon laadun säilyttämistä sekä tietojenkäsittelyn turvaamista.[61] Uuden tietosuoja-asetuksen johdanto-osan 49 kohdassa puhutaan verkko- ja tietoturvallisuudesta ja sillä tarkoitetaan verkon tai tietojärjestelmän kykyä suojautua tietyllä suojatasolla onnettomuuksilta tai laittomilta taikka ilkivaltaisilta toimilta, jotka vaarantavat tallennettujen tai siirrettävien henkilötietojen saatavuuden, aitouden, eheyden ja luottamuksellisuuden ja niihin liittyvien, verkoissa ja tietojärjestelmissä tarjottujen tai välitettävien palvelujen turvallisuuden.

Korhonen määrittelee *verkkoyhteiskunnan* yhteiskunnaksi, jonka merkittävät toiminnot ja prosessit ovat järjestäytyneet erilaisten toisiinsa liittyneiden verkkojen muotoon.[62] *Pöysti* katsoo verkkoyhteiskunnalle ominaisia piirteitä olevan verkostojen hyödyntäminen organisaatiomuotona liiketoiminnassa, politiikassa ja kansalaisyhteiskunnan toiminnoissa.[63] Saarenpää katsoi jo vuonna 2000 olevan aiheellista puhua *oikeudellisesta verkkoyhteiskunnasta,* sillä tietoverkoista ja niiden käytöstä oli tullut oikeudellisesti tärkeä asia.

---

[59] Suomen lainsäädännössä sähköisen viestinnän tietosuojan osalta tietoturvasta säädetään tietoyhteiskuntakaaressa. Euroopan komissio julkaisi tammikuussa 2017 ehdotuksen COM (2017) 10 final Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). Uusi asetus kumoaisi vuonna 2002 säädetyn sähköisen viestinnän tietosuojadirektiivin, jonka pohjalta tietoyhteiskuntakaaremme on säädetty. Pitkänen, Korpisaari ja Korhonen 2017 s. 8 toteavat, että eurooppalainen ja kansallinen tietosuojalainsäädäntö ovat voimakkaan muutoksen alla ja nähtäväksi jää muun muassa se, millaisia muutoksia tullaan tarvitsemaan varsin tuoreeseen tietoyhteiskuntakaareen.

[60] Tietoyhteiskuntakaaren nimike on muutettu lailla tietoyhteiskuntakaaren muuttamisesta (68/2018) ja se tulee voimaan 1.6.2018. Lain uusi nimike on laki sähköisen viestinnän palveluista. Muutosta koskevan hallituksen esityksen (HE 82/2017 vp) johdannossa todettiin, että tietoyhteiskuntakaari on muutospaineiden alaisena EU:n käynnissä olevista lainsäädäntöhankkeista johtuen ja että muutokset kansalliseen lainsäädäntöön tehdään, kun EU-lainsäädännön muutokset on hyväksytty. Lain nimikkeen muutoksesta eduskunnan perustuslakivaliokunta totesi, että se pitää säädöksen vanhahtavaa nimikettä epäonnistuneena ja että laintasoisen säädöksen nimikkeessä olisi syytä esiintyä sana ”laki” (PeVL 40/2017 vp).

[61] Voutilainen 2012, s. 117-118.

[62] Korhonen 2003, s. 15.

[63] Pöysti 2002, s. 36.

Lainsäädäntö ja viestintätavat uudistuivat ja informaatiota käytettiin uusin tavoin.[64]

[64] Saarenpää 2000, s. 5-6.

4 HENKILÖTIETOJEN SUOJA

4.1. Henkilötietojen suojaamisen tarve

Henkilötietojen suojan sääntelyllä pyritään turvaamaan luonnollisen henkilön henkilötietojen keräämisen ja käsittelyn asianmukaisuus. Henkilötietojen suojan on katsottu liittyvän tiedolliseen itsemääräämisoikeuteen ja tietosuojan tarkoituksena on nähty pyrkimys siihen, että yritykset ja yhteisöt toimivat asianmukaisesti kansalaisia koskevaa informaatiota kerätessään ja säilyttäessään.[65] Teknologian kehittyessä lainsäädännön on pystyttävä vastaamaan tietojen muuttuvaan käsittely-ympäristöön ja asettamaan käsittelylle oikeudelliset rajansa. Niin henkilötietojen suojan sääntelyn kuin tietosuojalainsäädännön syntymisen ylipäätään on nähty liittyvän kiinteästi informaatio- ja viestintäteknologioiden vauhdikkaaseen kehittymiseen.[66]

Henkilötietojen suojan sääntelyn merkitys on erityisesti Euroopan unionissa huomattu jo verkkoyhteiskuntakehityksen varhaisessa vaiheessa. EU:n henkilötietodirektiivi tuli voimaan vuonna 1998, jolloin verkkoyhteiskuntamme oli hyvin erilainen kuin nykyään. Tietojen suojaamisen tarve automaattisessa tietojenkäsittelyssä oli kuitenkin tuolloin jo tunnustettu.[67] 2010-luvulla henkilötietojen suoja on ollut esillä erityisen näkyvästi. Euroopan unionin tuomioistuin on antanut useita ratkaisuja[68], jotka ovat vahvistaneet sekä yksityiselämän että henkilötietojen suojan asemaa perusoikeutena.

[65] Pesonen 2013, s. 73.
[66] Ks. Salminen 2009, s. 19.
[67] Henkilötietodirektiivin 3 artiklan 1 kohdan mukaan direktiiviä sovelletaan osittain tai kokonaan automatisoituun tietojenkäsittelyyn sekä sellaisten henkilötietojen manuaaliseen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.
[68] Euroopan unionin tuomioistuimen asiassa C-362/14, eli niin sanotussa Schrems-tapauksessa, jota tässä tutkielmassa käsitellään perusteellisesti, unionin tuomioistuin otti kantaa henkilötietojen suojan ja yksityiselämän suojan perusoikeuksien kautta siihen, täyttikö komission päätös 2000/520/EY henkilötietodirektiivin vaatimukset henkilötietojen suojasta. Asiassa C-131/12, joka tunnetaan Google Spain-tapauksena, tuomioistuin vahvisti perusoikeuskirjan 7 ja 8 artikloihin perustuen, että henkilö voi halutessaan pyytää hakukoneyhtiötä poistamaan häntä koskevia tietoja. Kyse on oikeudesta tulla unohdetuksi. Digital Rights Ireland-ratkaisussa eli asiassa C-293/12 tuomioistuin totesi teletunnistetietojen säilyttämistä edellyttävän direktiivin 2006/2454 merkitsevän puuttumista perusoikeuskirjan 7 ja 8 artiklassa taattujen yksityiselämän ja henkilötietojen suojaan.

Henkilötietojen suojassa luonnollisen henkilön vastinparina on usein yritys tai muu yhteisö, joka syystä tai toisesta käsittelee yksityishenkilön henkilötietoja. Privacy Shield-järjestelmän osalta kysymys on nimenomaan yksityisen henkilön henkilötiedon tietosuojan turvaamisesta silloin, kun henkilötietoja käsitellään yhdysvaltalaisen yrityksen järjestelmissä. Tietoverkossa toimivien yritysten palvelutarjonta on valtava ja ihmiset käyttävät tietoverkkoa tuotteiden ja palveluiden hankkimiseen yhä enemmän. Sähköisen liiketoiminnan konsepteissa, joissa asiakas tunnistetaan ja hänen tietojaan tarvitaan palvelun tuottamisessa, henkilötietojen käsittely on erottamaton osa yrityksen ydinliiketoimintaa.[69]

4.2. Henkilötietojen suojan sääntely Suomessa

Henkilötietojen suojan sääntely Suomessa lähtee perustuslaista. Perustuslain (731/1999) 10.1 §:n mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. PL 10.1 § turvaa neljää oikeushyvää: yksityiselämää, kunniaa, kotirauhaa ja henkilötietoja. Perustuslaki ilmaisee ainoastaan henkilötietojen suojan perusoikeudellisuuden ohjaten sääntelyn alemman tasoiseen lainsäädäntöön, mutta kuitenkin tunnustetaan henkilötietojen suojan perusoikeudellinen asema. Säännös viittaa tarpeeseen lainsäädännöllisesti turvata yksilön oikeusturva ja yksityisyyden suoja henkilötietojen käsittelyssä, rekisteröinnissä ja käyttämisessä.[70]

Suomen lainsäädännössä henkilötietojen suojasta säädetään henkilötietolaissa, tietoyhteiskuntakaaressa ja laissa yksityisyyden suojasta työelämässä (759/2004). Säännöksiä löytyy myös muista laeista. Aivan ensimmäinen tietosuojaa koskeva pääsäädös Suomen lainsäädännössä oli henkilörekisterilaki, joka tuli voimaan vuonna 1988. Sen korvasi vuonna 1999 voimaan tullut henkilötietolaki, joka merkitsi unionin henkilötietodirektiivin implementointia Suomen lainsäädäntöön.[71] *Pitkänen*, *Korpisaari* ja Korhonen toteavat henkilötietojen suojan sääntelyn Suomessa

[69] Salminen 2009, s. 19.
[70] Saraviita 2005, s. 370.
[71] Ks. Korhonen 2003, s. 114-117.

olevan sirpaleista, sillä voimassa olevassa lainsäädännössä on henkilötietolain lisäksi paljon muita henkilötietojen käsittelyä koskevia lakeja ja yksittäisiä säännöksiä, joita on valmisteltu eri hallinnonaloilla.[72]

Käynnissä olevan Euroopan unionin tietosuojalainsäädännön uudistuksen myötä myös Suomen kansallinen henkilötietojen suojaa koskeva lainsäädäntö tulee muuttumaan. Uuden tietosuoja-asetuksen soveltaminen alkaa 25.5.2018 ja asetus on jäsenvaltioissa suoraan sovellettavaa oikeutta. Euroopan unionin etusijaperiaatteen mukainen kansallinen lainsäädäntö ei voi olla asetuksen kanssa ristiriidassa, joten siltä osin kuin kansallinen lainsäädäntö ei jo vastaa tietosuoja-asetuksen määräyksiä, se tulee muuttaa vastaamaan niitä. Tietosuoja-asetuksen edellyttämää kansallisen lainsäädännön muutostarvetta on selvitetty ja kansallisen lainsäädännön on suurelta osin todettu olevan tietosuoja-asetuksen mukaista. Muutostarpeita on huomattu olevan lähinnä yksittäisten lakien yksittäisissä säännöksissä.[73]

4.2.1. Sähköisen viestinnän tietosuoja-asetus

Suhteellisen uusi, vuodesta 2015 lähtien sovellettavana ollut tietoyhteiskuntakaari on joutumassa muutosten alaiseksi. Lain nimike muuttuu 1.6.2018 alkaen laiksi sähköisen viestinnän palveluista ja samalla lain yksittäisiä säännöksiä muutetaan ja puretaan. EU-tasolla tietoyhteiskuntakaaren taustalla olevaa sähköisen viestinnän tietosuojadirektiiviä (2002/58 EY) esitetään kumottavaksi ja korvattavaksi sähköisen viestinnän tietosuoja-asetuksella.[74] Asetus olisi suhteessa yleiseen tietosuoja-asetukseen erityissäädös ja sillä täsmennettäisiin ja täydennettäisiin yleistä tietosuoja-asetusta henkilötiedoiksi luokiteltavien sähköisen viestinnän tietojen osalta. Kaikki henkilötietojen käsittelyyn

[72] Pitkänen, Korpisaari, Korhonen 2017, s. 4.

[73] Pitkänen, O. (toim.) Tietosuojasäädösten muutostarve. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017. Muutostarpeen arvioinnissa ongelmalliseksi osoittautui erityisesti arkaluonteisten tietojen käsittelyn perusteiden kansallinen liikkumavara yleisen tietosuoja-asetuksen 9 artiklassa, jossa määritetään erityisiä henkilötietoryhmiä koskevaa käsittelyä. Kansallista lainsäädäntöämme voi olla vaikea sovittaa 9 artiklassa määriteltyihin perusteisiin käsittelyn tarpeellisuudesta. Selvityksessä ei käyty läpi henkilötietolakia, sillä sen muutostarve on ollut erikseen arvioitavana.

[74] Komission ehdotus COM (2017) 10 final. Euroopan parlamentin ja neuvoston asetus yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus).

liittyvät kysymykset, joita ehdotus ei nimenomaisesti kata, kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan.[75] Asetuksen myötä tuleva merkittävin muutos olisi se, että asetus koskisi kaikkia viestintäpalveluiden tarjoajia ja kaikkea sähköistä viestintää. Näin myös viime vuosina yleistyneet kuluttajien väliset viestintäpalvelut, kuten Snapchat ja Whatsapp, olisivat asetuksen sovellusalan piirissä.

4.2.2. Tietosuojalaki

Unionin yleinen tietosuoja-asetus kumoaa henkilötietodirektiivin, jonka määräykset on Suomessa pantu täytäntöön henkilötietolailla. Tietosuoja-asetus korvaa siten myös henkilötietolain säännökset siltä laajuudelta, kuin henkilötietojen käsittely kuuluu uuden asetuksen soveltamisalaan. Henkilötietolain mahdollisia muutostarpeita selvittämään asetettiin vuonna 2016 Oikeusministeriön toimesta täytäntöönpanotyöryhmä, jonka tehtävänä oli myös arvioida henkilötietolain kaltaisen yleislain tarvetta ja tehdä siitä tarvittaessa ehdotus.[76]

Työryhmä päätyi mietinnössään esittämään uuden yleisen tietosuojalain säätämistä. Laki täydentäisi yleistä tietosuoja-asetusta ja se voimaan tullessaan kumoaisi henkilötietolain, lain tietosuojalautakunnasta ja tietosuojavaltuutetusta (389/1994) sekä asetuksen tietosuojalautakunnasta ja tietosuojavaltuutetusta (432/1994).[77] Tietosuojalaista annettiin hallituksen esitys (HE 9/2018 vp)[78] 1.3.2018 ja lain on tarkoitus tulla voimaan 25.5.2018.

Ehdotettu laki olisi henkilötietojen käsittelyyn sovellettava yleislaki, jota sovellettaisiin rinnakkain tietosuoja-asetuksen kanssa. Samoin sitä tulisi myös lukea rinnakkain tietosuoja-asetuksen kanssa. Laki ei siten muodostaisi itsenäistä sääntelykokonaisuutta, vaan se täydentäisi ja täsmentäisi tietosuoja-asetusta, sillä henkilötietojen suojaa koskevan lainsäädännön aineellinen sisältö tulee pääasiallisesti tietosuoja-asetuksesta. Tilanne on eri kuin henkilötietolakia säädettäessä eli pantaessa täytäntöön

[75] COM (2017) 10 final, s. 2-3.
[76] Oikeusministeriö. Mietintöjä ja lausuntoja 35/2017. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö.
[77] OM. EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän mietintö 35/2017, s. 70.
[78] Hallituksen esitys HE 9/2018 vp.

henkilötietodirektiiviä, sillä tietosuoja-asetuksen mahdollistama kansallinen liikkumavara ei anna mahdollisuutta kokonaisvaltaisen lain säätämiseen, jollainen henkilötietolaki on ollut.[79]

Tietosuoja-asetuksen kattavuuden ja yksityiskohtaisuuden vuoksi ei ole tarpeen säätää tietynlaista henkilötietolain toisintoa, vaan tietosuojalain tehtävä olisi olla täydentävä yleislaki. Kattavan yleislain säätäminen ei olisi edes mahdollista, sillä yleinen tietosuoja-asetus on nimenomaan asetus ja siten jäsenvaltioissa sellaisenaan ja suoraan sovellettavaa oikeutta, joten sen kanssa päällekkäisen lainsäädännön säätäminen ei olisi perusteltavaa. On huomioitava, että henkilötietolain pohjana oli henkilötietodirektiivi, jolloin kansallisen lainsäätäjän valittavana oli direktiivin implementoinnin muoto. Henkilötietodirektiivin ja tietosuoja-asetuksen eurooppaoikeudelliset oikeuslähdepohjat ovat erilaisia ja tämä ero vaikuttaa siten merkittävästi kansalliseen lainsäädäntöön.

4.3. Yksityisyyden suojaa koskeva kansainvälinen perusoikeussäännöstö

Perus- ja ihmisoikeudet ymmärretään perustavaa laatua olevien arvojen ilmaisuina.[80] Yksityisyyden suoja on ollut perus- ja ihmisoikeuksina suojattavien oikeushyvien joukossa jo ensimmäisistä perus- ja ihmisoikeussopimuksista lähtien. Vuonna 1953 voimaan tulleen Euroopan neuvoston ihmisoikeussopimuksen (EIS) 8 artiklassa säädetään oikeudesta nauttia yksityis- ja perhe-elämän kunnioitusta.

> Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, tai epäjärjestyksen tai rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi, tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

Euroopan ihmisoikeustuomioistuin on useissa ratkaisuissaan todennut henkilötietojen suojan olevan olennainen osa EIS 8 artiklan takaamaa

[79] Ks. HE 9/2018 vp, 1 Johdanto.
[80] Ojanen 2015, s. 10.

yksityis- ja perhe-elämän suojaa.[81] Euroopan neuvosto (EN) on aina pysynyt yhteisöstä ja myöhemmin unionista erillisenä toimielimenä. Sen perustamisen on katsottu aloittaneen eurooppalaisen yhteistyön erityisesti ihmisoikeuksien, demokratian ja oikeusvaltioperiaatteen aloilla.[82] Neuvoston kaikki 47 jäsenvaltiota ovat Euroopan ihmisoikeussopimuksen osapuolia, joten sopimuksen vaikutusvallan alaisena on satoja miljoonia ihmisiä.[83] Yhdysvallat ei ole Euroopan ihmisoikeussopimuksen osapuoli, mutta sille myönnettiin tarkkailijan asema vuonna 1995.[84]

Yhdistyneiden kansakuntien kansalais- ja poliittisia oikeuksia koskeva yleissopimus (KP-sopimus), joka tuli voimaan vuonna 1976, sisältää myös yksityisyyden suojaa koskevan artiklan 17. Lähes kaikki maailman valtiot ovat KP-sopimuksen osapuolia.[85]

> 1. Kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä suorittaa hänen kunniaansa ja mainettaan loukkaavia hyökkäyksiä.
> 2. Jokaisella on oikeus lain suojaan tällaista puuttumista tai tällaisia hyökkäyksiä vastaan.

4.3.1. Euroopan unionin perusoikeuskirja

Merkittävä Euroopan unionin perus- ja ihmisoikeuksien turvaamiseksi luotu instrumentti on Euroopan unionin perusoikeuskirja (2012/C326/02), joka allekirjoitettiin vuonna 2000. Perusoikeuskirja[86] määrittelee perusoikeudet, joita unionin tulee kaikessa toiminnassaan noudattaa. Perusoikeuskirjasta tuli oikeudellisesti sitova Lissabonin sopimuksen yhteydessä vuonna 2009.[87]

---

[81] Pitkänen, Tiilikka, Warma 2013, s. 18.
[82] Ks. Ojanen 2016, s. 9.
[83] https://www.coe.int/en/web/about-us/our-member-states
[84] Council of Europe. Committee of Ministers. Resolution 95 (37) on Observer Status for the United States of America with the Council of Europe.
[85] http://www.globalis.fi/view/content/3655/full/1/2245 Muun muassa Malesia, Etelä-Sudan ja Saudi-Arabia eivät ole ratifioineet sopimusta.
[86] Euroopan unionin perusoikeuskirja (2012/C326/02).
[87] SEU 6 (1) artikla. SEU 6 (3) artiklassa määritetään unionin oikeuden suhdetta Euroopan ihmisoikeussopimukseen: ”Ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä eurooppalaisessa yleissopimuksessa taatut ja jäsenvaltioiden yhteisestä valtiosääntöperinteestä johtuvat perusoikeudet ovat yleisinä periaatteina osa unionin oikeutta.” Euroopan unioni, joka itsenäisenä oikeushenkilönä ei ainakaan toistaiseksi ole Euroopan ihmisoikeussopimuksen osapuoli, on erityisesti perusoikeuskirjassa luonut EU:n ja EIS:n välille selkeän siteen. Perusoikeuskirjan johdanto-osassa todetaan perusoikeuskirjassa vahvistettavan unionin toimivallan ja tehtävien sekä toissijaisuusperiaatteen mukaisesti oikeudet, jotka perustuvat erityisesti jäsenvaltioille yhteisiin

Perusoikeuskirjassa henkilötietojen suoja on saanut itsenäisen perusoikeuden aseman, sillä se ei ole siinä osa yksityiselämän suojaa turvaavaa perusoikeutta. Henkilötietojen suojan voi kuitenkin katsoa kuuluvan myös 7 artiklan alaisuuteen, koska henkilötietojen suoja on historiallisesti ollut ja on edelleen yksityisyyden suojan osa-alue. 8 artiklassa vahvistetun itsenäisen perusoikeusaseman voikin arvioida olevan osittain seurausta verkkoyhteiskunnan kehittymisestä ja henkilötietojen suojan tärkeyden korostumisesta yhteiskunnan toimintojen siirtyessä yhä vahvemmin tietoverkkoihin. *Neuvosen* mukaan henkilötietojen suojan perusoikeutta on toteutettu enemmän tavallisessa lainsäädännössä, josta se tulkintojen ja muun muassa perusoikeuskirjan seurauksena on saanut tunnustetun perus- ja ihmisoikeusulottuvuutensa.[88]

Perusoikeuskirjan 7 artiklassa säädetään yksityis- ja perhe-elämän kunnioittamisesta:

> Jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan.

8 artiklan määräys henkilötietojen suojan perusoikeudesta koostuu kolmesta erillisestä kohdasta:

> 1. Jokaisella on oikeus henkilötietojensa suojaan.
> 2. Tällaisten tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi.

valtiosääntöperinteisiin ja kansainvälisiin velvoitteisiin, ihmisoikeuksien ja perusvapauksien suojaamiseksi tehtyyn yleissopimukseen, unionin ja Euroopan neuvoston hyväksymiin sosiaalisiin peruskirjoihin sekä Euroopan unionin tuomioistuimen ja Euroopan ihmisoikeustuomioistuimen oikeuskäytäntöön. Perusoikeuskirjan 52 (3) artiklan mukaan ”siltä osin kuin perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamiseksi tehdyssä yleissopimuksessa taattuja oikeuksia, niiden merkitys ja ulottuvuus ovat samat kuin mainitussa yleissopimuksessa.”

[88] Neuvonen 2014, s. 73.

3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.

Unionin oman perusoikeuden merkitys kasvaa tilanteissa, joissa on kyse unionin toimivaltaan kuuluvasta asiasta ja esimerkiksi tietojenvaihdosta unionin ulkopuolelle.[89] EU:n kansalaisten henkilötietojen siirrossa yhdysvaltalaisten yritysten palvelimille on kyse tällaisesta tilanteesta, joten perusoikeuskirja määrittää tällaisen tiedonsiirron oikeudellisia reunaehtoja keskeisesti.[90]

4.3.2. Perusoikeuskirja unionin tuomioistuimen oikeuskäytännössä

Perusoikeudet, joiden säätämisellä halutaan turvata tärkeimmiksi katsottuja arvoja, kuten esimerkiksi oikeutta elämään ja oikeutta turvallisuuteen, olisivat pelkkää perusoikeussäännöstöä lukemalla ja tulkitsemalla kovin abstrakteja. Perusoikeudet ja niiden sääntelyn merkitys näkyvät todellisuudessa vasta sitten, kun tuomioistuimet oikeudenkäytössään soveltavat ja tulkitsevat niitä sekä käyttävät niitä tuomioidensa perustelemiseen. Tuomioistuimet herättävät abstraktit perusoikeussäännökset eloon ja tuovat ne lähelle tavallisen ihmisen elämää koskevia oikeudellisia kysymyksiä. Tilanne on tietyllä tapaa vastavuoroinen, sillä esimerkiksi perusoikeuskirja perustuu osaksi unionin tuomioistuimen perusoikeuksia kehittäneelle oikeuskäytännölle.[91]

Kun Euroopan unionin perusoikeuskirjasta tuli oikeudellisesti sitova Lissabonin sopimuksen myötä vuonna 2009, oikeudellistuminen on alkanut näkyä unionin tuomioistuimen ratkaisukäytännössä. EUT on antanut useita ratkaisuja, joissa perusoikeuskirjan säännöksiä on tulkittu perusteellisesti ja otettu tuomioiden perusteiksi. Tulkinnoillaan EUT ei ole vain selventänyt tietosuojadirektiivin (henkilötietodirektiivi) säännöksiä, vaan tuomiot vaikuttavat myös henkilötietojen suojan tulevaan sääntely-ympäristöön.[92]

[89] Neuvonen 2014, s. 56.
[90] Euroopan unionin tuomioistuin perusti tuomionsa Maximillian Schremsin tapauksessa vahvasti perusoikeuskirjaan ja erityisesti sen 7, 8 ja 47 artikloihin.
[91] Ks. Walkila 2015, s. 793-794. EY-tuomioistuin, eli nykyinen EU-tuomioistuin, ryhtyi jo 1970-luvun vaihteesta lähtien arvioimaan perusoikeuksien toteutumista oikeuskäytännössään muotoilemalla ne ”yleisiksi oikeusperiaatteiksi”.
[92] Kaivola 2016, s. 864.

Ratkaisuja, joissa henkilötietojen suojaa koskevaa perusoikeutta on sovellettu, ovat esimerkiksi Digital Rights Ireland, Google Spain sekä Schrems-tapaus.[93] Schrems-ratkaisussa unionin tuomioistuin viittasi toistuvasti henkilötietojen suojaa koskevan perusoikeuteen ja totesi Safe Harbor-periaatteita koskevan komission päätöksen olevan pätemätön nimenomaan perusoikeuskirjan valossa katsottuna.[94] Tuomioistuinten roolia perusoikeuksien ja erityisesti henkilötietojen suojaa koskevan perusoikeuden tulkinnassa ja kehittämisessä ei tule väheksyä, sillä nimenomaan tuomioistuimet luovat tulkinnoillaan perusoikeuksille käytännön ilmentymiä.

4.4. Kansainvälinen henkilötietojen suojaa koskeva sääntely

Henkilötietojen suojaa on oikeudellisessa keskustelussa korostettu 1970-luvulta lähtien.[95] Vuosikymmenen kuluessa annettiin ensimmäisiä kansallisia tietosuojaa koskevia, lain tasoisia säädöksiä, kuten Ruotsin *Datalagen* ja Yhdysvaltojen *Fair Credit Reporting Act* sekä *Privacy Act*.[96] Teknologian ja verkkoyhteiskunnan kehittyessä kansainvälisten, tietosuojaa koskevien oikeudellisten reunaehtojen määrittämiselle alettiin nähdä yhä enemmän tarvetta.

Merkittävä tietosuojaa säätelevä instrumentti on ollut vuonna 1981 voimaan tullut Euroopan neuvoston tietosuojasopimus.[97] Kaikki Euroopan unionin jäsenvaltiot sekä EU itsenäisenä oikeushenkilönä ovat liittyneet yleissopimukseen, jolla katsotaan olevan sitova asema kansainvälisessä oikeudessa.[98] Euroopan neuvostossa on yleistä, vuonna 2018 sovellettavaksi tulevaa tietosuojauudistusta koskevien neuvottelujen yhteydessä laadittu

[93] Digital Rights Ireland-ratkaisussa sovellettavana olivat perusoikeuskirjan 7, 8, 11 ja 52 artiklat. Google Spain-tuomiossa EUT sovelsi perusoikeuskirjan 7 ja 8 artikloita ja Schrems-tapauksessa 7, 8 ja 47 artikloita.
[94] Euroopan unionin tuomioistuin: Tuomio asiassa C-362/14, kohdat 94, 95, 98 ja 104.
[95] Neuvonen 2014, s. 70.
[96] Bygrave 2014, s. 99. Ruotsin Datalagen hyväksyttiin vuonna 1973, USA:n the Fair Credit Reporting Act vuonna 1970 ja the Privacy Act vuonna 1974.
[97] Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (108/1981).
[98] Ks. Korhonen 2003, s. 93.

lisäpöytäkirjaluonnos, jonka tavoitteena on mukauttaa yleissopimus nykyisiin ja tuleviin tietosuojahaasteisiin.[99]

Tietosuojasopimusta sovelletaan henkilötietojen käsittelyyn sekä yksityisellä että julkisella sektorilla ja siinä muun muassa määritellään tietosuojan periaatteet, jotka osapuolet sitoutuvat toteuttamaan lainsäädännössään yksityisyyden suojaamiseksi henkilötietojen automaattisessa käsittelyssä. Yleissopimuksessa mahdollistetaan henkilötietojen vapaa siirto sopimuspuolena olevien jäsenvaltioiden välillä, mutta siinä myös asetetaan tiettyjä rajoituksia siirroille sellaisiin maihin, joissa ei ole vahvistettu säädöksillä riittävää suojaa. Vuonna 2001 hyväksyttiin yleissopimuksen 108 lisäpöytäkirja, jossa määrätään rajan yli tapahtuvasta tietojen siirrosta sopimuksen ulkopuolisiin, niin kutsuttuihin kolmansiin maihin.[100]

Taloudellisen yhteistyön ja kehityksen järjestö OECD[101] antoi vuonna 1980 ohjeet yksityisyyden suojaamiselle ja henkilötietojen rajojen ylittävälle siirrolle.[102] Valtioille suunnattu lainsäädäntösuositus sisältää henkilötietojen keräämistä ja laatua, rekisteröidyn tarkastusoikeutta, tietoturvaa ja kansainvälistä tiedonsiirtoa koskevia yleisperiaatteita.[103] OECD:n suositusten vaikutus on edelleen merkittävä ja niitä on uudistettu viimeksi vuonna 2013. Ohjeiden sisältämät perusperiaatteet omaksuttiin tietosuojadirektiiviin (henkilötietodirektiivi) vain muutamin muutoksin.[104] Suosituksiin on viitattu myös uudessa tietosuojalakia koskevassa hallituksen esityksessä.[105]

OECD:n tietosuojasuositukset ovat suosituksenluonteisia, eivätkä siten osapuolivaltioissa sitovaa oikeutta. Niillä on kuitenkin ollut suuri vaikutus tietosuojalainsäädännön voimaansaattamiseen ja sisältöön monien Euroopan alueen ulkopuolisten valtioiden oikeusjärjestyksissä, esimerkiksi Japanissa ja

[99] HE 9/2018, 2.2.1. Euroopan neuvosto.
[100] Ks. Korhonen 2003, s. 93 ja Euroopan unionin perusoikeusvirasto ja Euroopan neuvosto: Käsikirja Euroopan tietosuojaoikeudesta 2014, s. 15-17.
[101] The Organisation for Economic Co-operation and development.
[102] Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of the Personal Data 23.8.1980.
[103] Korhonen 2003, s. 93.
[104] Vanto 2011, s. 13-14.
[105] HE 9/2018, 2.2.3. OECD:n tietosuojasuositus.

Australiassa. Pohjois-Amerikassa lukuisat yritykset ovat virallisesti allekirjoittaneet suositukset.[106]

Ensimmäiset tietosuojasta säätävät oikeudelliset instrumentit Euroopassa eivät ole siis olleet unionin omia instrumentteja, vaan OECD:n ja Euroopan neuvoston.[107] Tarkasteltaessa EU:n ja Yhdysvaltojen suhdetta sekä ristiriitoja henkilötietojen suojan sääntelyssä, OECD:n suositukset ovat merkittävässä roolissa, sillä sekä suurin osa EU:n jäsenvaltioista, että Yhdysvallat ovat OECD:n jäseniä. Tietosuojasuositukset ovat ylikansallinen instrumentti, jonka periaatteet myös Yhdysvallat on hyväksynyt. Niiden voidaan siten katsoa määrittävän yhteisen tietosuojan perustason molemmille toimijoille.

4.5. Euroopan unionin henkilötietojen suojaa koskeva sääntely

Henkilötietojen suojaa säännellään sekä Euroopan unionin primaari- että sekundaarioikeudessa. Primaarioikeuden säännökset on kirjattu Sopimukseen Euroopan unionin toiminnasta. SEUT 16 artiklan 1 kohdan mukaan jokaisella on oikeus henkilötietojensa suojaan. Artiklan 2 kohdan mukaan Euroopan parlamentti ja neuvosto antavat tavallista lainsäätämisjärjestystä noudattaen luonnollisten henkilöiden suojaa koskevat säännöt, jotka koskevat unionin toimielinten, elinten ja laitosten sekä jäsenvaltioiden silloin, kun viimeksi mainitut toteuttavat unionin oikeuden soveltamisalaan kuuluvaa toimintaa, suorittamaa henkilötietojen käsittelyä, sekä säännöt, jotka koskevat näiden tietojen vapaata liikkuvuutta. Lisäksi yhteisen ulko- ja turvallisuuspolitiikan erityismääräyksiä käsittelevä Euroopan unionista tehdyn sopimuksen 2 luku sisältää henkilötietojen suojaa koskevan artiklan.[108]

Euroopan unionin sekundaarioikeuden henkilötietojen suojaa koskeva sääntely on pitkään pohjautunut henkilötietodirektiiviin, joka tuli voimaan vuonna 1995. Henkilötietodirektiivi sisältää määräyksiä muun muassa

[106] Bygrave 2002, s. 32-33.
[107] Boehm 2012, s. 4.
[108] Sopimus Euroopan unionista 39 artiklan mukaan neuvosto tekee päätöksen, jolla vahvistetaan Euroopan unionin toiminnasta tehdyn sopimuksen 16 artiklan mukaisesti ja sen 2 kohdasta poiketen luonnollisten henkilöiden suojaa koskevat säännöt, jotka koskevat jäsenvaltioiden tämän luvun soveltamisalaan kuuluvaa toimintaa toteuttaessaan suorittamaa henkilötietojen käsittelyä, sekä säännöt, jotka koskevat näiden tietojen vapaata liikkuvuutta. Sääntöjen noudattamista valvoo riippumaton viranomainen.

tietojen laatua koskevista periaatteista, rekisteröidyn tiedonsaantioikeudesta, valvontaviranomaisista ja henkilötietojen siirrosta kolmansiin maihin. Direktiiviä on sovellettu osittain tai kokonaan automatisoituun tietojenkäsittelyyn sekä sellaisten henkilötietojen manuaaliseen käsittelyyn, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.[109] Henkilötietodirektiivi on sääntelyalaltaan kattava ja sen vaikutukset ovat moniulotteisia. Saarenpää onkin todennut, että muun muassa kansainvälisten yritysten toiminta ja kansainvälinen kauppa ovat paljolti henkilötietodirektiivin asettamien vaatimusten välittömästi tai välillisesti ohjaamia.[110] Koska kyseessä on direktiivi, se on unionin jäsenvaltioissa saatettu voimaan kansallisilla laeilla, mutta sen toteuttamisen keinot ovat olleet jäsenvaltioiden itsensä päätettävissä. On katsottu, että muun muassa henkilötietojen käsittelytehtäviin liittyvät käytännön toimenpiteet saattavat vaihdella huomattavasti eri jäsenvaltioissa.[111]

Henkilötietojen käsittelystä määrätään myös Euroopan parlamentin ja neuvoston asetuksessa yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta. Asetus tulee sovellettavaksi silloin, kun henkilötietojen käsittelyä suorittavat yhteisöjen toimielimet ja elimet niissä tilanteissa, kun käsittely suoritetaan yhteisön oikeuden soveltamisalaan kokonaan tai osittain kuuluvien toimien toteuttamiseksi.[112] Sähköisen viestinnän tietosuojadirektiivi[113], joka on tarkoitus korvata sähköisen viestinnän tietosuoja-asetuksella, on säännellyt yksityisyyden suojaa käytännössä perinteisten teleoperaattoreiden toiminnassa. Yksityisyyttä suojaavia sääntöjä on uuden asetuksen myötä tarkoitus soveltaa myös uusiin sähköisiä viestintäpalveluja tarjoaviin toimijoihin, joita ovat esimerkiksi Whatsapp, Skype ja iMessage.[114]

[109] Henkilötietodirektiivi 3 artikla 1 kohta.
[110] Saarenpää 2016, s. 88.
[111] Pitkänen, Korpisaari, Korhonen 2017, s.1.
[112] Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, 3 artiklan 1 kohta.
[113] Euroopan parlamentin ja neuvoston direktiivi (2002/58/EY) henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla.
[114] Ks. Euroopan komissio: Lehdistötiedote 10.1.2017. Komissio ehdottaa korkeatasoisen yksityisyydensuojan varmistavia sääntöjä kaikkeen sähköiseen viestintään ja päivittää EU:n toimielimiä koskevia tietosuojasääntöjä.

Yksi Euroopan unionin tietosuojalainsäädännön uudistuksista on niin kutsuttu poliisidirektiivi[115], jota sovelletaan poliisin ja muiden viranomaisten suorittamaan henkilötietojen käsittelyyn rikosasioissa.[116] Direktiiviä aletaan soveltaa 6.5.2018 ja siihen mennessä se on implementoitava kansalliseen lainsäädäntöön. Suomessa direktiivi on tarkoitus saattaa voimaan lailla henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä.[117]

Yleisen tietosuoja-asetuksen ja muiden tietosuojalainsäädännön uudistusten myötä unionin tietosuojaa ja henkilötietojen suojaa koskeva sääntelykenttä uudistuu. Henkilötietodirektiiviä on sovellettu henkilötietojen käsittelyyn parinkymmenen vuoden ajan ja direktiiviä annettaessa vuonna 1995 verkkoympäristö oli hyvin erilainen. Nykymuotoinen World Wide Web (WWW) kehitettiin 1990-luvun alkuvuosina ja sen jälkeen tietoverkkojen tekninen toteutus ja tietojärjestelmät ovat kehittyneet huomattavasti.[118] Esimerkiksi tietosuojalakia koskevassa hallituksen esityksessä on todettu, että tietosuojauudistus on ollut tarpeellinen informaatioteknologian nopean kehityksen ja jäsenvaltioiden hajanaisten henkilötietojen suojaa koskevien säädösten ja niiden epäyhtenäisen soveltamisen vuoksi.[119] Lisäksi verkossa siirrettävien henkilötietojen määrä on sähköisen kaupankäynnin kasvun myötä lisääntynyt merkittävästi.

[115] Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta.
[116] Hallituksen esityksessä eduskunnalle laiksi henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä sekä eräiksi siihen liittyviksi laeiksi (HE 31/2018 vp) direktiivistä 2016/680 käytetään nimitystä ”rikosasioiden tietosuojadirektiivi”. Euroopan komissio on käyttänyt samasta direktiivistä nimitystä ”poliisidirektiivi” (https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_fi). Oikeusministeriön lainvalmisteluosaston lausunnossa 31.5.2016 eduskunnan hallintovaliokunnalle komission tiedonannosta: Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi (E 37/2016 vp) samasta direktiivistä käytetään nimityksiä ”EU:n tietosuojadirektiivi” ja ”poliisidirektiivi”.
[117] Oikeusministeriö. Mietintöjä ja lausuntoja 52/2017. Henkilötietojen suoja rikosasian käsittelyssä ja kansallista turvallisuutta ylläpidettäessä. Tietosuojadirektiivityöryhmän mietintö.
[118] World Wide Web-järjestelmän kehityksestä ks. Bygrave & Bing 2009, s. 38-42.
[119] HE 9/2018 1 Johdanto.

5 TIETOSUOJASÄÄNTELY YHDYSVALLOISSA

5.1. Tietosuojan sääntelyn rakenteesta

Yhdysvalloissa ei ole henkilötietojen käsittelyä koskevaa liittovaltiotason yleislakia eikä valtion tietosuojasääntelyn rakenne muutoinkaan ole verrattavissa esimerkiksi Euroopan unionin jäsenvaltioiden tai itse unionin tietosuojasääntelyyn. Yhdysvaltojen tietosuojasääntely koostuu liittovaltion tason tietosuojaa koskevista laeista, osavaltioiden omasta tietosuojalainsäädännöstä ja ohjesäännöistä sekä common law-periaatteista. Lisäksi valtion virastot ovat kehittäneet tietosuojaa koskevia ohjeita ja eri teollisuusaloilla on olemassa itsesääntelykäytäntöjä.[120]

Yhdysvalloissa henkilötietojen tai yksityisyyden suojaa ei erillisinä oikeuksina ole kirjattu perustuslakiin[121]. Vaikka henkilötietojen tai yksityisyyden suojaa ei ole turvattu perustuslaissa, eikä valtion tasolla olevaa tietosuojan yleislakia ole, Yhdysvalloissa on runsaasti henkilötietojen suojaa turvaavaa sääntelyä. Lainsäädäntö ei yleisesti ole niin tiukkaa ja kokonaisvaltaista kuin Euroopassa, mutta se muodostaa silti vankan säädöskokoelman.[122] Yleislain sijasta henkilötietojen suojasta on kehittynyt erityissääntelyä, joka määrittää tietojen käsittelyä yksittäisissä tapauksissa, sektorikohtaisesti tai esimerkiksi tietyillä teollisuuden aloilla.

Kun sääntely on hyvin pitkälti tapaus- ja alakohtaista, ongelmia voi syntyä erityisesti uusilla liiketoiminta-aloilla, kun niillä ei alan kehittyessä tietosuojasääntelyä ole välttämättä ollenkaan. Tämä voi antaa uusille yrityksille edullisemman aseman markkinoilla, kun ne voivat käsitellä henkilötietoja vapaammin. *Schwartz* on todennut, että uudet teknologiayhtiöt voivat hyödyntää henkilötietoja sellaisilla menetelmillä, jotka eivät ole sallittuja pidempään toimineille yhtiöille, joiden alalle on jo kehittynyt tietosuojasääntelyä.[123]

[120] Ks. Ieuan 2016, s. 1.
[121] The Constitution of the United States.
[122] Bygrave 2014, s. 108.
[123] Ks. Schwartz 2013, s. 1978 – 1979.

5.2. Tietosuojasääntely liittovaltiotasolla

Yhdysvalloissa ei ole virallista liittovaltiotason tietosuojaviranomaista, mutta liittovaltion kauppakomissiolla (Federal Trade Commission, FTC) on merkittävä rooli liittovaltiotason tietosuojasääntelyn kehittämisessä. FTC on itsenäinen viranomainen, jonka tehtävänä on kuluttajien suojaaminen ja kilpailun edistäminen talouden eri alueilla. Viraston oikeudellinen valtuutus tulee Federal Trade Commission-laista[124], joka kieltää epäreilut ja harhaanjohtavat käytännöt markkinoilla.[125]

FTC on yhdessä Yhdysvaltain kauppaministeriön kanssa edustanut Yhdysvaltoja kansainvälisesti sen neuvotellessa tietosuojasäännösten yhteensovittamisesta muiden valtioiden ja kansainvälisten toimijoiden, kuten Euroopan unionin kanssa. FTC myös neuvotteli EU:n kanssa sopimuksen ongelmakohdista ja kehittämisestä sen soveltamisaikana. *Bygrave* on todennut FTC:lla olevan todellisuudessa liittovaltion tietosuojaviranomaisen asema, joka on rinnastettavissa eurooppalaisten tietosuojaviranomaisten asemaan.[126]

Federal Trade Commission Act on liittovaltiotasoinen kuluttajansuojalaki, joka kieltää epäreilut tai harhaanjohtavat kaupalliset käytänteet. Kyseessä ei ole suoraan tietosuojaa säätelevä laki, mutta Yhdysvaltain kauppaministeriö on pitkään soveltanut sitä myös sellaisten liiketoimintojen harjoittamiseen, jotka vaikuttavat kuluttajien yksityisyyteen ja tietoturvaan. Lailla kielletään siten epäreilut tai harhaanjohtavat toimet, jotka eivät suojaa kuluttajan henkilötietoja.[127]

Children's Online Privacy Protection Act (COPPA) säätelee verkossa tapahtuvaa alle 13-vuotiaiden lasten henkilötietojen keräämistä ja se tulee sovellettavaksi silloin, kun kaupalliset verkkosivut tai viestintäpalvelut keräävät lasten henkilötietoja. COPPA määrittää lasten henkilötietoja olevan

[124] Federal Trade Commission Act. Chapter 311, 38 Stat. 717, September 26, 1914. As Amended Through Public Law 111–203, Enacted July 21, 2010.
[125] Federal Trade Commission. Privacy & Data Security. Update: 2017 s. 1.
[126] Bygrave 2014, s. 177-178 toteaa, että kauppaministeriötä pidetään *de facto* liittovaltiollisena tietosuojaviranomaisena. Vaikka sen toimivalta on rajatumpi kuin unionin tietosuojaviranomaisilla, sen tietosuojaa koskeva vastuualue on kasvanut huomattavasti 2000-luvulla. Ministeriön vahva rooli johtuu osittain siitä, ettei Yhdysvalloissa ole erillistä tietosuojaviranomaista.
[127] Ieuan 2016, s. 3.

esimerkiksi lapsen koko nimi, sosiaaliturvatunnus, puhelinnumero tai lasta esittävä kuva.[128] Sitä sovelletaan mihin tahansa verkkosivuun niin Yhdysvalloissa kuin sen ulkopuolella, joka kerää Yhdysvalloissa olevien lasten henkilötietoja.[129]

CAN-SPAM Act (Controlling the Assault of Non-Solicited Pornography and Marketing Act) sääntelee sähköpostiosoitteiden keräämistä ja käyttöä kaupallisiin tarkoituksiin ja kieltää kaupallisten sähköpostien lähettäjiä käyttämästä vääriä tai harhaanjohtavia otsikkotietoja tai sähköpostin aihetunnisteita. Lähettäjien on myös tuotava viesteissä selkeästi esiin tieto siitä, että kyseessä on mainos ja ilmoitus siitä, että vastaanottajalla on mahdollisuus vastaisuudessa kieltäytyä vastaanottamasta kyseiseltä lähettäjältä tulevia sähköpostiviestejä.[130]

5.3. Osavaltioiden tietosuojalainsäädäntö

Osavaltiotasolla Yhdysvalloissa on satoja yksityisyyttä ja tietoturvaa koskevia lakeja, jotka sääntelevät henkilötietojen keräämistä, käyttöä, käsittelyä ja suojaamista. Monien osavaltioiden omaksuma lainsäädäntö koskee esimerkiksi sosiaaliturvatunnusten käsittelyä ja suojaamista sekä yritysten vastaanottamien ja käsittelemien henkilötietojen keräämistä ja suojaa.[131] Tietosuojalainsäädännön kattavuus on kuitenkin osavaltiokohtaista ja niiden välillä on huomattavia eroja sääntelyn määrässä ja kehittymisessä.

Kalifornian osavaltio on ollut edelläkävijä yhdysvaltalaisen tietosuojalainsäädännön kehittämisessä. Se oli ensimmäinen osavaltio, jossa hyväksyttiin tietoturvallisuuden rikkomista käsittelevä laki[132] ja se voimaantulonsa jälkeen vuodesta 2003 lähtien on muuttanut merkittävästi yksityisyyden asemaa koko Yhdysvalloissa. Osavaltion tietosuojasääntely on kokonaisvaltaista ja sen on todettu muistuttavan tiukempaa ja kattavampaa eurooppalaista lähestymistapaa yksityisyyden suojaan.[133]

[128] Children's Online Privacy Protection Act of 1998. Section 1302 Definitions. (8) Personal Information.
[129] Kuner 2013, s. 127.
[130] Ieuan 2016, s. 18.
[131] Ieuan 2016, s. 19.
[132] Civil Code Sec. 1798.82. (The California Security Breach Information Act). Senate Bill No. 1386.
[133] Ieuan 2016, s. 19-20.

California Online Privacy Protection Act of 2003 (CalOPPA) säätää muun ohella, että sellaisen kaupallisen verkkosivun operaattorin, joka kerää henkilötiedoiksi luokiteltuja tietoja yksityisistä henkilöistä, jotka asuvat Kaliforniassa ja käyttävät kyseistä sivua tai vierailevat sillä, tulee näkyvästi julkaista tietosuojakäytänteensä verkkosivullaan. Laki määrittelee henkilötiedoiksi esimerkiksi henkilön nimen ja sähköpostiosoitteen.[134] *California Shine the Light Law (Civil Code 1798.83)* edellyttää yritysten kirjeitse tai sähköpostitse ilmoittavan asiakkailleen muun muassa sen, mitä heidän henkilötietojaan on jaettu kolmansille osapuolille suoriin markkinointitarkoituksiin ja mitkä ovat ne osapuolet, joille henkilötietoja on luovutettu.[135]

Toinen kattavasti tietosuojasta säännellyt osavaltio on Massachusetts, jonka *Data Security Regulation*[136] soveltuu kaikkiin liiketoimintoihin, jotka toimintansa yhteydessä omistavat, lisensoivat, varastoivat tai ylläpitävät osavaltion asukkaiden henkilötietoja siitä riippumatta, sijaitseeko liiketoiminta osavaltiossa tai sen ulkopuolella. Kaikkien tällaisten henkilöiden tai yritysten on kehitettävä ja otettava käyttöön kattava ja kirjallinen tietoturvaohjelma sekä ylläpidettävä sitä. Näiden tahojen on lisäksi varmistettava, että mitkä tahansa kolmannet osapuolet, joilla on pääsy yksityishenkilöiden henkilötietoihin, voivat suojata tuota informaatiota.[137]

5.4. Yhdysvaltojen ja EU:n tietosuojasääntelyn erot

Tietosuojan sääntelyllä on sekä Euroopassa että Yhdysvalloissa pitkä historia aina 1970-luvulta asti, mutta sääntelyn voi arvioida kehittyneen molemmilla alueilla niiden omien oikeusperinteidensä ja -kulttuuriensa mukaisesti.[138] *Heisenberg* huomauttaa, että unioni on lähtenyt kehittämään tietosuojasääntelyä hyvin erilaisesta lähtökohdasta kuin Yhdysvallat. EU:ssa

[134] Online Privacy Protection Act of 2003. California Business and Professions Code. Division 8. Special Business Regulations. Chapter 22. Internet Privacy Requirements 22575 & 22577.
[135] Civil Code. Division 3. Obligations. Part 4. Obligations arising from particular transactions. Title 1.81. Customer Records 1798.83. A (1) & A (2).
[136] The Massachusetts Data Security Regulation. Mass. Regs. Code tit. 201 § 17.01-17.05.
[137] Ieuan 2016, s. 24-25.
[138] Bygrave 2014, s. 108 huomauttaa, että Yhdysvallat oli yksi ensimmäisistä valtioista, jotka laativat tietosuojasääntelyä.

perusajatus on ollut, että ylimääräistä tietoa ei saa kerätä ja että sitä ei saa käyttää muihin tarkoituksiin kuin niihin, mihin se on kerätty. Yhdysvalloissa on lähdetty siitä, että tiedon kerääminen on lähtökohtaisesti sallittua ja yrityksille on annettu suhteellisen vapaat kädet kokeilla uusia tietojen käsittelymenetelmiä.[139]

EU:n ja Yhdysvaltojen oikeuden perustavanlaatuisena erona tietosuojan osalta voidaan pitää sitä, ettei henkilötietojen tai yksityisyyden suojalla ole Yhdysvalloissa perusoikeuden asemaa. Niissä oikeusjärjestelmissä, joissa yksityisyydellä tai henkilötietojen suojalla ei ole perusoikeuden asemaa, sitä on usein määritelty tiettyyn tapausta tai tilannetta koskevissa oikeuslähteissä, jotka voivat löytyä esimerkiksi oikeuskäytännöstä tai osavaltion laista.[140] Yhdysvalloissa tietosuojaa säätelevät oikeuslähteet ovat löydettävissä juuri näistä lähteistä ja vaikka valtion tietosuojalainsäädännön rakenne on perusteiltaan unionin lainsäädännöstä poikkeava, Yhdysvalloissa on runsaasti yksityishenkilöiden henkilötietoja suojaavaa lainsäädäntöä.

Ei-neuvoteltavissa olevan tietosuojan rajan on yhdysvaltalaisessa lainsäädännössä tai oikeuskäytännössä katsottu olevan matalampi kuin Euroopassa.[141] Tämän voi todeta johtuvan suurelta osin siitä, että henkilötietojen tai yksityisyyden suojalla ei ole Yhdysvalloissa perusoikeusasemaa ja osittain Yhdysvaltojen liittovaltiojärjestelmästä. Osavaltiot päättävät hyvin pitkälle omasta lainsäädännöstään ja niiden intresseistä riippuen tiettyä asiaa koskeva sääntely voi olla hyvin kattavaa tai sitä vastoin vähäistäkin. Bygrave on todennut, että yleisesti tietosuojan toteutumisen valvonta ja toimeenpanojärjestelmät eivät ole niin kehittyneitä kuin Euroopassa.[142]

Merkittävänä erona nimenomaan henkilötietojen siirron kannalta on pidetty sitä, ettei Yhdysvallat rajoita tiedon siirtämistä toisiin maihin.[143] Tämä ei tarkoita sitä, etteikö USA:n ulkopuolelle siirrettäviä henkilötietoja turvattaisi. Yhdysvaltojen lainsäädäntöä sovelletaan henkilötietoihin myös silloin, kun

[139] Ks. Heisenberg 2005, s. 14. & Schwartz 2013, s. 1978.
[140] Ks. Kuner 2013, s. 62.
[141] Bygrave 2014, s. 110.
[142] Bygrave 2014, s. 110-111.
[143] Schwartz 2013, s. 1977.

ne on siirretty yli Yhdysvaltojen rajojen. Yritykset, jotka ovat käsitelleet tietoja Yhdysvalloissa ja siirtäneet ne eteenpäin esimerkiksi alihankkijoilleen, ovat edelleen vastuussa tietojen käsittelystä ja niiden tulisi käyttää samoja suojausmenetelmiä riippumatta siitä, ovatko henkilötiedot sijoitettu Yhdysvaltoihin vai sen rajojen ulkopuolelle.[144]

Euroopan unionin tietosuojalainsäädännöllä on ollut suuri vaikutus alan lainsäädännön kehittymiselle myös muualla maailmassa, mutta Schwartz arvioi, että sen sijaan, että EU:n tietosuojalainsäädäntö asetettaisiin sellaisenaan malliksi myös muualla maailmassa, muotoutumassa on vastavuoroista sopeutumista ja yhdessä kehitettävää lainsäädäntöä korostava lainsäädännön kehittämismalli ja esimerkiksi Safe Harbor-sopimus on yksi osoitus tästä kehityksestä.[145]

Kun useampi kansainvälinen toimija lähtee kehittämään yhteistä lainsäädäntöä, taustalla vaikuttavat valtioiden tai alueiden omat lainsäädäntöperinteet. Tietosuojan kannalta haasteena on ollut lisäksi, että unioni ja Yhdysvallat ovat alun perin lähteneet kehittämään tietosuojasääntelyään hyvin erilaisista lähtökohdista. Molempien osapuolten kannalta on kuitenkin ollut ehdottoman tärkeää, että sellaisista säännöksistä, joilla on vaikutusta esimerkiksi kansainväliseen kauppaan, päästään sellaiseen lopputulokseen, johon sekä EU että Yhdysvallat voivat sitoutua.

[144] Ks. Ieuan 2016, s. 27.
[145] Schwartz 2013, s. 1979.

6 SAFE HARBOR

6.1. Sopimuksen taustat

Safe Harbor-sopimusjärjestely perustui Euroopan komission heinäkuussa 2000 tekemään päätökseen Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien Safe Harbor-periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista tavallisimmista kysymyksistä.[146] Sopimuksen osapuolia olivat Euroopan komissio ja Yhdysvaltain kauppaministeriö ja se antoi yhdysvaltalaisille yrityksille mahdollisuuden liittyä niin kutsuttuun Safe Harbor-listaan[147], joka toimi osoituksena siitä, että yritys noudattaa Yhdysvaltain kauppaministeriön julkaisemia periaatteita unionin kansalaisten henkilötietoja käsitellessään. Sopimus edusti siten yhtä Euroopan unionin henkilötietodirektiivin mukaista menetelmää henkilötietojen siirtämiselle kolmansiin maihin. Safe Harbor-järjestely kumottiin Euroopan unionin tuomioistuimen päätöksellä vuonna 2015.[148]

Sopimusta ei tule arvioida vain yksittäisenä, kahden kansainvälisen toimijan välisenä sopimuksena, vaan sen tarkoitus ja lähtökohdat ymmärtääkseen tulee perehtyä laajemmin sekä 1990-luvun lopun kansainväliseen ilmapiiriin tietosuoja-asioissa, että vuosituhannen vaihteessa koko ajan kasvaneeseen kansainväliseen kauppaan. Safe Harbor ei ollut sinänsä yksittäinen unionin ja Yhdysvaltojen välisiin suhteisiin vaikuttava sopimusjärjestely, sillä samoihin aikoihin solmittiin muitakin transatlanttisia sopimuksia, jotka helpottivat kaupankäyntiä ja poistivat kaupan rajoituksia.[149]

Euroopan unioni hyväksyi henkilötietodirektiivin vuonna 1995 ja sitä alettiin soveltaa vuonna 1998. Yhdysvaltojen kannalta direktiivin voimaantulo tarkoitti sitä, että henkilötietoja voitiin vastedes siirtää Euroopasta ainoastaan, mikäli tietosuojan taso Yhdysvalloissa on riittävä. Heti direktiivin

[146] Komission päätös 2000/520/EY.
[147] https://www.export.gov/safeharbor_eu
[148] Tuomio asiassa C-362/14.
[149] Petersmann & Pollack 2003, s. 92-93. Muita sopimuksia olivat esimerkiksi EU/US Positive Comity Agreement (1998), EU/US Agreement on Mutual Recognition of Certificates of Conformity for Marine Equipment (2001) ja EU/US Guidelines on Regulatory Co-operation and Transparency (2002).

hyväksymisen jälkeen Yhdysvaltoja yritettiin saada aloittamaan valmistelut direktiivin tulevien vaikutusten johdosta, mutta niin maan lukuisat yritykset kuin poliittiset päättäjätkin pitivät epätodennäköisenä, että EU asettaisi kansainväliset markkinat tiedonsiirron mahdollisen keskeyttämisen myötä riskin alaiseksi.[150]

Yhdysvaltojen reagointia henkilötietodirektiivin todellisiin vaikutuksiin voidaan pitää verkkaisena. Vaikka useilla unionin jäsenvaltioilla oli jo ennen direktiivin voimaantuloa kansallista lainsäädäntöä, joka antoi niille mahdollisuuden estää tiedonsiirrot maihin, joissa tietosuojan tasoa ei katsottu riittäväksi, *Schaffer* on arvioinut Yhdysvaltojen kokeneen tiedonsiirron lopettamisen luoman uhan todelliseksi vasta sitten, kun sen eston mahdollisuus oli osa unionin oikeutta.[151] Kun henkilötietodirektiiviä oli sovellettu noin kuukauden verran, Yhdysvaltain kauppaministeriö julkaisi ehdotuksen henkilötietojen suojaa itsesääntelyn keinoin turvaavista Safe Harbor-periaatteista ja vuonna 1999 uuden version luonnoksesta, mutta EU ei pitänyt niitä riittävinä.[152]

Presidentti Bill Clintonin hallinto oli vuonna 1997 julkaissut ohjelman koskien globaalia sähköistä kauppaa. Ohjelman mukaan hallitusten tulisi muodostaa ennakoitava ja yksinkertainen oikeudellinen ympäristö, joka perustuisi hajautettuun, sopimuksen mukaiseen lainsäädäntömalliin eikä yhteen, ylhäältä johdettuun säännökseen. Yhdysvallat lupasi jatkaa neuvotteluja unionin kanssa, jotta unionissa ymmärrettäisiin paremmin yhdysvaltalaista lähestymistapaa tietosuojaan ja yksityisyyteen yleensä.[153] Ohjelman ilmaisuista voi todeta käyvän ilmi, että Yhdysvallat oli täysin ajan tasalla henkilötietodirektiivin seurauksista, mutta halukkuus mukautua sen säännöksiin oli epävarmaa.

Juuri kansainvälisen kaupan kehittymisen varmistamiseksi ja markkinoiden turvaamiseksi henkilötietojen suojaamisesta oli välttämätöntä päästä sopimukseen. Kuten aiemmin tässä tutkielmassa on todettu, Euroopan

[150] Ks. Heisenberg 2005, s. 78-79. Heisenberg 2005, s. 2. mukaan vuonna 1998 USA:n ja EU:n välille noussut tietosuojakonflikti oli tärkeämpi kuin niiden välillä aiemmin olleet taloudelliset konfliktit, sillä riskin alaisena olevien markkinoiden suuruudeksi arvioitiin 120 miljardia dollaria.
[151] Schaffer 2000, s. 83.
[152] Schaffer 2000, s. 59-62.
[153] US White House (1997). A Framework for Global Electronic Commerce.

unionin ja Yhdysvaltojen lähtökohdat tietosuojasääntelylle ovat poikenneet toisistaan huomattavasti. Tietosuojajärjestelyn luomiseksi käytiin erilaisia neuvotteluja vuosien 1998-1999 aikana ja Yhdysvaltain kauppaministeriön maaliskuussa 2000 antama ehdotus Safe Harbor-periaatteista hyväksyttiin komission jäsenvaltioedustajien toimesta. Safe Harbor tuli voimaan marraskuussa 2000.[154]

Henkilötietodirektiivi aiheutti merkittävän transatlanttisen kiistan, ja Bygrave on kuvannut Yhdysvaltojen ja EU:n välisiä neuvotteluja kireiksi kummankin osapuolen väittäessä, että toinen yritti määritellä sopimukseen toisen osapuolen kannalta ehtoja, jotka olivat mahdottomia hyväksyä.[155] Tilanne ei ollut kitkaton myöskään Euroopassa, sillä Euroopan parlamentti vastusti Safe Harborin hyväksymistä, samoin kuin artiklan 29 mukainen tietosuojatyöryhmä (the Article 29 Working Party). Niillä ei kuitenkaan ollut toimivaltaa estää komissiota hyväksymästä sopimusta.[156]

Safe Harbor-periaatteilla oli väistämätön vaikutus yhdysvaltalaisten yritysten toimintaan, sillä niiden tuli ottaa käyttöön kaksi erilaista tietosuojastandardia, toinen eurooppalaisille asiakkaille ja toinen Yhdysvaltojen kansalaisille. Kun toisen asiakasryhmän henkilötietoja suojattaisiin tiukemmin, sen katsottiin voivan vaikuttaa yrityksen imagoon.[157] Safe Harborin alkutaival Yhdysvalloissa vaati yrityksiltä uudenlaista sopeutumista.

6.2. Henkilötietodirektiivin vaatimukset henkilötietojen siirtämiselle

Henkilötietodirektiivin johdanto-osassa todetaan muun ohella, että henkilötietojen kansainvälinen siirto on tarpeen kansainvälisen kaupan kehittämiseksi ja että direktiivillä taattava yksilöiden tietosuoja ei estä henkilötietojen siirtoa kolmansiin maihin, jotka voivat turvata tietosuojan riittävän tason. Edelleen todetaan, että jos tietosuojan taso kolmannessa

[154] Ks. Heisenberg 2005, s. 86-93.
[155] Petersmann & Pollack 2003, s. 99. Ks. Bygrave 2013, s. 9-10.
[156] Ks. Heisenberg 2005, s. 8.
[157] Ks. Schaffer 2000, s. 78.

maassa ei ole riittävä, henkilötietojen siirto kyseiseen maahan on kiellettävä.[158]

Direktiivin IV luvussa määrätään henkilötietojen siirrosta kolmansiin maihin. 25 artiklan 1 kohdan mukaan jäsenvaltioiden on säädettävä siitä, että käsiteltävien tai siirron jälkeen käsiteltäväksi tarkoitettujen henkilötietojen siirto kolmanteen maahan voidaan suorittaa ainoastaan, jos kyseisessä kolmannessa maassa taataan tietosuojan riittävä taso, jollei tämän direktiivin muiden säännösten mukaisesti säädetyistä kansallisista säännöksistä muuta johdu. Saman artiklan 2 kohdan mukaan kolmannessa maassa taattavan tietosuojan tason riittävyyttä on arvioitava kaikkien tiettyyn siirtoon tai siirtojen ryhmään liittyvien olosuhteiden osalta. Säännöksessä määritettyjä erityisiä olosuhteita ovat muun muassa tietojen luonne, suunnitellun käsittelyn tarkoitus ja kestoaika, kyseisessä kolmannessa maassa voimassa olevat yleiset tai alakohtaiset oikeussäännöt sekä ammattisäännöt ja tässä maassa noudatettavat turvatoimet.

25 artiklan 6 kohdan mukaisesti komissio voi todeta, että tietyssä kolmannessa maassa taataan tietosuojan riittävä taso, mikä johtuu kyseisen maan sisäisestä lainsäädännöstä tai kansainvälisistä sitoumuksista. Safe Harbor-päätös tehtiin juuri edellä mainitun kohdan valtuutuksen mukaisesti. Henkilötietodirektiivin IV luvun 25 artiklan 3 kohdan mukaan jäsenvaltioiden ja komission on informoitava toisiaan, jos ne arvioivat, että tietosuojan taso ei jossain maassa ole riittävä.

Henkilötietodirektiivin IV luvun 26 artiklassa määrätään poikkeuksista 25 artiklan säännöksiin eli niistä tilanteista, joissa henkilötietojen siirto sellaiseen kolmanteen maahan, jossa ei taata 25 artiklan 2 kohdassa tarkoitettua tietosuojan riittävää tasoa, voidaan suorittaa tietyin edellytyksin. Edellytyksiä ovat esimerkiksi rekisteröidyn yksiselitteinen suostumus siirtoon, siirron tarpeellisuus rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöön panemiseksi, siirron tarpeellisuus tärkeän yleisen edun turvaamiseksi tai rekisteröidyn elintärkeän edun suojaamiseksi.

[158] Henkilötietodirektiivin johdanto-osa, kohdat 56 ja 57.

6.3. Päätöksen sisältö

Safe Harbor-päätöksen artikla 1 sisältää määräyksen siitä, että Safe Harbor-periaatteet, joita sovelletaan Yhdysvaltain kauppaministeriön julkaisemien tavallisimpien kysymysten (Frequently Asked Questions, FAQ) ohjauksen mukaisesti, varmistavat unionista Yhdysvaltoihin sijoittautuneille organisaatioille siirrettyjen henkilötietojen riittävän suojelun tason. Artiklassa 3 annetaan jäsenvaltioiden tietosuojaviranomaisille valtuudet keskeyttää henkilötietojen siirto organisaatiolle, joka on ilmoittanut noudattavansa FAQ:n mukaisesti sovellettavia periaatteita, jos Yhdysvaltojen valtiollinen elin tai riippumaton valitusmenettelyjärjestely on todennut, että organisaatio loukkaa kyseisiä periaatteita. Tietojen siirto voidaan keskeyttää myös, jos on huomattavan todennäköistä, että periaatteita loukataan, täytäntöönpano-organisaatio ei ole ryhtynyt riittäviin toimenpiteisiin asian ratkaisemiseksi, tietojen siirron jatkaminen aiheuttaisi välittömän vakavan haitan vaaran rekisteröidyille ja jos jäsenvaltion viranomaiset ovat kohtuullisessa määrin pyrkineet antamaan organisaatiolle ilmoituksen ja tilaisuuden vastata siihen.[159]

Safe Harbor-päätöksen tärkein sisältö on päätöksen liitteessä I, joka sisältää Yhdysvaltain kauppaministeriön antamat seitsemän periaatetta henkilötietojen siirtämiseen Euroopasta Yhdysvaltoihin. *Ilmoitus-periaatteen* sisältöön kuuluu muun muassa organisaation velvollisuus ilmoittaa yksityishenkilöille, mihin tarkoitukseen se kerää ja käyttää heitä koskevia tietoja ja minkälaisille kolmansille osapuolille se antaa tietoja. Ilmoituksen on oltava selkeä. *Valinta-periaatteen* mukaisesti organisaation on tarjottava rekisteröidyille mahdollisuus valita (opt out), voiko heidän henkilötietojaan antaa kolmannelle osapuolelle tai käyttää tarkoitukseen, joka ei vastaa tietojen keruun alkuperäistä tarkoitusta. Rekisteröidyille on annettava helposti käytettävissä olevat ja kustannuksiltaan kohtuulliset keinot valintamahdollisuuden käyttämiseen.

Periaatteen, joka määrittää *tiedon siirtämistä edelleen*, mukaan organisaatio voi antaa tietoja kolmannelle osapuolelle ainoastaan ilmoitus- ja valintaperiaatteiden mukaisesti. Organisaatio voi halutessaan antaa tietoja

[159] Komission päätös 2000/520/EY, 1 ja 3 artiklat.

kolmannelle osapuolelle, joka toimii kyseisen organisaation puolesta, jos se ensin varmistaa, että kolmas osapuoli noudattaa Safe Harbor -periaatteita tai on direktiivin tai muun tietosuojan riittävyyden takaavan säädöksen alainen, taikka jos organisaatio tekee kolmannen osapuolen kanssa kirjallisen sopimuksen, jossa vaaditaan, että kolmas osapuoli tarjoaa vähintään saman tasoisen suojan kuin vastaavilla Safe Harbor -periaatteilla taataan. *Turvallisuus-periaatteen* mukaan organisaatioiden on toteutettava riittävät varotoimet muun muassa tietojen katoamisen, vääriin käsiin joutumisen ja hävittämisen ehkäisemiseksi.

Tietojen koskemattomuuden periaate turvaa sen, että henkilötietojen on liityttävä siihen tarkoitukseen, johon niitä on määrä käyttää. Organisaatio ei saa käsitellä henkilötietoja tavalla, joka ei sovi niiden alkuperäiseen käyttötarkoitukseen tai johon kyseinen henkilö ei ole antanut suostumustaan. *Tiedonsaanti-periaatteeseen* kuuluu henkilön oikeus saada itseään koskevat tiedot organisaatiolta. Henkilön on voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä. *Täytäntöönpano-periaatteen* mukaisesti tehokkaaseen tietosuojaan on sisällyttävä menettelyt, joilla varmistetaan tietosuojaperiaatteiden noudattaminen ja organisaatiolle koituvat seuraamukset niiden noudattamatta jättämisestä. Menettelyihin on kuuluttava ainakin valitusmenettely, seurantamenettely ja organisaatiolle asetettava velvoite korjata ongelmat, jotka johtuvat siitä, että ne eivät noudata periaatteita ilmoittamallaan tavalla. Seuraamusten on oltava riittävän vakavat, jotta niillä voidaan varmistaa, että organisaatiot noudattavat periaatteita.[160]

Liitteessä II, joka sisältää Yhdysvaltain kauppaministeriön julkaisemat tavallisimmat kysymykset, määritetään muun muassa periaatteiden tarkempaa sisältöä ja soveltamisalaa ja FTC:n toimivaltuuksia Safe Harborin soveltamisessa. FTC tutkii, onko toiminnassa rikottu FTC Act-lain 5 pykälää, jossa kielletään sopimattomat ja harhaanjohtavat toimet ja käytännöt kaupan alalla. Se voi hakea hallinnollista kieltomääräystä, jolla estetään kyseiset toimet, tai nostaa kanteen liittovaltion piirioikeudessa (Federal District Court).[161] Liitteessä III kuvataan Safe Harbor-järjestelmän täytäntöönpanoa

[160] Komission päätös 2000/520/EY. Liite I. Yhdysvaltojen kauppaministeriön 21 päivänä heinäkuuta 2000 antamat Safe Harbor-periaatteet.
[161] Komission päätös 2000/520/EY. Liite II. Tavallisimmat kysymykset (FAQ).

ja FTC:n toimivaltaa sopimattomien tai harhaanjohtavien käytäntöjen suhteen.[162]

6.4. Safe Harbor-sopimusjärjestelyn toiminta

Safe Harborin toimintaa ja tehokkuutta arvioitiin järjestelyn voimaantulon jälkeen niin Euroopan unionin toimielinten, Yhdysvaltain viranomaisten kuin lukuisten oikeustieteilijöiden toimesta. Järjestelyyn esitettiin lisäksi useita parannusehdotuksia. Vallitseva mielipide oli, että Safe Harbor-järjestelyssä ja sen noudattamisessa oli useita vakavia puutteita, jotka tulisi korjata, jotta järjestelyn mukainen henkilötietojen suojan turvaaminen olisi oikeasti tehokasta. Vuonna 2005 *Reidenberg* totesi järjestelyn olevan sekä laadullisesti että määrällisesti jopa häpeällisen heikko.[163]

Euroopan komissio antoi vuonna 2002 ensimmäisen arviointikertomuksensa Safe Harborin toiminnasta. Se totesi FTC:n luoneen järjestelyn ja ylläpitävän sitä sovitusti. Huomattava määrä niistä yrityksistä, jotka olivat sitoutuneet periaatteisiin, ei täyttänyt niiden vaatimaa läpinäkyvyyttä siitä, mihin tietosuojakäytäntöjä yritys noudattaa ja mikä niiden sisältö on. Ongelmaksi osoittautui myös se, etteivät useat yritykset olleet ilmoittaneet kuulumisestaan Safe Harbor-järjestelyyn.[164]

Samana vuonna arvionsa Safe Harborin toiminnasta antoi myös artiklan 29 mukainen tietosuojatyöryhmä. Se pyysi itselleen toimitettavaksi selvitykset muun muassa siitä, onko mahdollista ottaa käyttöön ylimääräistä tarkistusmenettelyä periaatteisiin sitoutumisen varmistamiseksi. Työryhmä halusi tietoonsa myös sen, aiheuttivatko saman toimijan soveltamat useat

[162] Komission päätös 2000/520/EY. Liite III. Yleiskatsaus Safe Harbor-järjestelmän täytäntöönpanoon.
[163] Reidenberg 2005, s. 1133. Jo vuonna 2001 Reidenberg huomautti Safe Harborin olevan ainoastaan heikko ja virheellinen ratkaisu henkilötietojen siirrolle. Hänen mukaansa sopimus on molempien osapuolten kannalta toimimaton, eikä se todellisuudessa lievitä Yhdysvaltain heikon tietosuojasääntelyn ongelmia (Reidenberg 2001, s. 719 ja 739).
[164] Commission of the European Communities. Commission Staff Working Paper. The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. 13.02.2002 SEC (2002) 196, s. 2 ja 8.

tietosuojakäytännöt vaikeuksia. Se toivoi lisäksi tietoa mahdollisuudesta laatia erillinen Safe Harbor-ohjekirja.[165]

Toisen arviointikertomuksensa komissio antoi vuonna 2004, kun Safe Harbor-periaatteet olivat olleet sovellettavana noin kolmen vuoden ajan. Periaatteisiin oli tuolloin sitoutunut yli 400 yhdysvaltalaista yritystä ja määrä oli kasvanut joka vuosi. Ongelmat olivat osittain samoja kuin aiemmassa arviointikertomuksessa: yritysten verkkosivuilta ei ollut löydettävissä julkista ilmoitusta sitoutumisesta Safe Harbor-periaatteisiin. Komissio katsoi, että merkittävällä osalla yrityksiä tuntui olevan vaikeuksia sovittaa periaatteita omiin tietojenkäsittelymenetelmiinsä ja ilmaisi huolensa siitä, että suhteellisen harva organisaatio julkaisi sellaisia tietosuojaselosteita, jotka kuvasivat kaikkia seitsemää periaatetta.[166]

Komissio huomautti, että kauppaministeriön tulisi tuoda Safe Harbor-järjestelyä aktiivisemmin esiin ja alkaa konkreettisiin toimiin taatakseen sen, että periaatteisiin sitoutuneet yritykset julkaisevat sovitunlaiset tietosuojaselosteet. Komission mukaan FTC:n tulisi aktiivisemmin valvoa organisaatioiden sitoutumista periaateisiin ja tarvittaessa aloittaa selvitys, mikäli periaatteiden noudattaminen osoittautuu kyseenalaiseksi.[167]

Vuonna 2008 australialainen konsulttiyritys *Galexia* julkaisi tutkimuksen Safe Harbor-periaatteiden noudattamisesta ja tuloksia voi kutsua kriittisiksi. Tutkimus osoitti muun muassa, että yhteensä 206 yritystä, jotka väittivät olevansa Safe Harbor-järjestelyyn sitoutuneita, eivät sitä olleet.[168] Galexia totesi virheellisten tietojen periaatteisiin sitoutumisesta aiheuttavan merkittävän riskin siitä, että eurooppalaiset kuluttajat ja yritykset tulevat johdetuksi harhaan väärien väitteiden myötä. Tutkimuksessa ehdotettiin, että unionin tulisi harkita uusia neuvotteluja Safe Harborin tehokkuuden parantamiseksi muun muassa siten, että kaikkien järjestelyyn sitoutuneiden yritysten tietosuojaselosteet tulisi olla saatavissa julkisella verkkosivulla.

[165] Article 29 Data Protection Working Party. Working Document on Functioning of the Safe Harbor Agreement. 11194/02/EN WP 62, s. 3 – 4.
[166] Commission of the European Communities. Commission Staff Working Document. The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce. Brussels 20.10.2004 SEC (2004) 1323, s. 5 – 8.
[167] Commission Staff Working Document SEC (2004) 1323, s. 5 - 8.
[168] Connolly 2008, s. 6. Safe Harbor-listassa oli vuonna 2008 noin 1700 yhdysvaltalaista yritystä.

Lopputulemana tutkimuksessa todettiin, että komission vuosien 2002 ja 2004 arviointikertomusten jälkeen järjestelyyn tehdyt parannukset ovat olleet vähäisiä.[169]

Vaikka Safe Harborin saama kritiikki oli voimakasta, järjestely nähtiin joiltain osin myös onnistuneena. Yhdysvalloissa järjestelyä on viranomaisten toimesta pidetty menestyksenä.[170] Sen avulla katsottiin myös vältetyn transatlanttisen kauppasodan ja sen todettiin tarjoavan kohtuullisen perustan tietosuojalle rajat ylittävissä toiminnoissa.[171]

6.5. Safe Harbor 2010-luvulla

Jos Safe Harbor oli jo aiemmin ollut merkittävän kritiikin kohteena, tilanne ei ainakaan helpottunut 2010-luvulla. Kesäkuussa 2013 tiedusteluasiantuntijana CIA:lla (Central Intelligence Agency) ja NSA:n (National Security Agency) alihankkijalla työskennellyt Yhdysvaltain kansalainen Edward Snowden toi julkisuuteen tietoja useista vakoiluohjelmista, jotka mahdollistivat ihmisten massavalvonnan. Ensin paljastettiin, että Yhdysvaltain hallitus oli oikeuden määräyksellä velvoittanut yhdysvaltalaisen puhelinyhtiö Verizonin toimittamaan NSA:lle kaikki puhelutietonsa riippumatta siitä, soitettiinko puhelut Yhdysvalloissa vai maan rajojen ulkopuolelle.[172]

Seuraava paljastus koski salaista PRISM-ohjelmaa, jonka avulla Yhdysvallat pystyi keräämään muun muassa Googlen, Facebookin ja Applen palvelimilta tietoja muun muassa henkilöiden hakuhistoriasta, sähköpostien sisällöistä, chat-keskusteluista ja kuvista.[173] NSA:n käyttämä XKeyScore-ohjelma mahdollisti muun muassa yksityishenkilöiden sähköpostien ja chat-keskusteluiden seuraamisen reaaliaikaisesti. Ohjelman hakukoneen avulla tietoja voitiin etsiä nimen, puhelinnumeron tai IP-osoitteen perusteella.[174]

[169] Connolly 2008, s. 8 ja 16.
[170] Ks. Connolly 2008, s. 5.
[171] Ks. Swire 2005, s. 1987.
[172] https://assets.documentcloud.org/documents/709012/verizon.pdf
[173] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data
[174] https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data

Snowdenin paljastukset aiheuttivat uuden henkilötietojen suojaa koskevan transatlanttisen kriisin ja julkitulleiden tietojen myötä Safe Harbor-järjestelyn kautta siirrettyjen henkilötietojen suoja asettui vakavasti kyseenalaiseksi. Euroopan komissiossa heräsi kesällä 2013 epäilyksiä siitä, ettei Safe Harbor ole niin turvallinen, kuin on oletettu.[175] Saman vuoden marraskuussa Euroopan komission perus- ja ihmisoikeuskomissaari Viviane Reding ilmoitti, ettei komissio pidä Safe Harboria turvallisena.[176]

Komissio julkaisi Snowdenin paljastuksiin liittyen kaksi tiedonantoa marraskuun lopussa 2013. Toinen tiedonannoista koski luottamuksen palauttamista EU:n ja Yhdysvaltojen väliseen tietojen siirtoon. Komissio totesi Yhdysvaltojen käyttämien ohjelmien laajamittaiseen tiedustelutietojen keruuseen loukkaavan eurooppalaisten perusoikeuksia ja erityisesti heidän oikeuttaan yksityisyyteen ja henkilötietojen suojaan. Tiedonannossa huomautettiin, että vaikka Safe Harbor sallii tietosuojasääntöjen rajoitukset, jos ne ovat tarpeen kansalliseen turvallisuuteen perustuvista syistä, siinä kyseenalaistettiin Yhdysvaltojen suorittaman henkilötietojen laajamittaisen keruun tarpeellisuus ja oikeasuhtaisuus kansallisen turvallisuuden kannalta. Tiedonannossa esitettiin huoli siitä, että Safe Harbor -järjestelmää voidaan käyttää EU:n kansalaisten henkilötietojen siirtämiseen EU:sta Yhdysvaltoihin myös silloin, kun Yhdysvaltojen tiedusteluviranomaiset velvoittavat yritykset luovuttamaan tietoja tiedustelutietojen keruuohjelmien puitteissa.[177]

Komission toinen tiedonanto[178] koski Safe Harbor-järjestelmän toimintaa EU:n kansalaisten ja unioniin sijoittautuneiden yritysten näkökulmasta. Tiedonannon mukaan Safe Harbor-järjestelmän perustaa on arvioitava uudessa valossa muun muassa sen takia, että tietovirrat ovat kasvaneet räjähdysmäisesti ja niillä on ratkaiseva merkitys erityisesti transatlanttisen talouden kannalta. Komissio totesi, että Googlen, Facebookin ja Microsoftin kaltaisilla verkkoyhtiöillä on Euroopassa satoja miljoonia asiakkaita ja ne

[175] https://euobserver.com/justice/120919
[176] https://www.theguardian.com/world/2013/nov/26/nsa-surveillance-europe-threatens-freeze-us-data-sharing
[177] COM (2013) 846 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle. Luottamuksen palauttaminen EU:n ja Yhdysvaltojen väliseen tietojen siirtoon, s. 3, 4 ja 7.
[178] COM (2013) 847 final. Komission tiedonanto Euroopan parlamentille ja neuvostolle: Safe Harbor-järjestelmän toiminnasta EU:n kansalaisten ja EU:hun sijoittautuneiden yritysten näkökulmasta.

siirtävät Yhdysvaltoihin käsiteltäväksi niin valtavia määriä henkilötietoja, ettei sitä voinut kuvitella vuonna 2000, kun Safe Harbor-järjestelmä luotiin. Päätöstä hyväksyttäessä ei myöskään voitu ennakoida, että tiedustelupalvelut pääsisivät käsiksi valtaviin määriin Yhdysvaltoihin kaupallisten liiketoimien yhteydessä siirrettyjä tietoja.[179]

Komission mukaan kaikki yritykset, jotka osallistuvat PRISM-ohjelmaan ja jotka sallivat Yhdysvaltojen viranomaisten pääsyn Yhdysvalloissa tallennettuihin ja käsiteltyihin tietoihin, näyttivät kuuluvan Safe Harbor -järjestelmään. Järjestelmästä oli tullut yksi väylistä, joiden kautta Yhdysvaltojen tiedusteluviranomaiset pääsivät keräämään alun perin EU:ssa käsiteltyjä henkilötietoja.[180] Safe Harbor-järjestelmä, joka oli laadittu unionin kansalaisten henkilötietojen suojaamiseksi, näytti mahdollistavan henkilötietojen tarkkailun epäasianmukaisessa tarkoituksessa.

Euroopan parlamentti antoi maaliskuussa 2014 päätöslauselman[181], jossa se käsitteli muun muassa Safe Harboria ja NSA:n valvontaohjelmaa. Päätöslauselmasta käy ilmi parlamentin turhautuminen Safe Harbor-sopimuksen rikkomuksiin ja komission toimien puuttumiseen järjestelyn parantamiseksi. Parlamentti totesi, että jo vuonna 2000 antamassaan päätöslauselmassa se esitti epäilyksiä ja ilmaisi huolensa periaatteiden riittävyydestä ja kehotti komissiota tarkastelemaan päätöstä uudelleen hyvissä ajoin saatujen kokemusten ja mahdollisen lainsäädännössä tapahtuneen kehityksen valossa. Parlamentin mukaan yhtäkään komission toisessa arviointikertomuksessa esitettyä puutetta ei oltu korjattu vuoteen 2013 mennessä ja uudessa tiedonannossa[182] komissio oli nimennyt vielä uusia merkittäviä puutteita periaatteiden täytäntöönpanossa. Se totesi lisäksi, että komissio ei ollut toteuttanut toimia korjatakseen periaatteiden tämänhetkiseen täytäntöönpanoon liittyviä tiedossa olevia puutteita.[183]

[179] COM (2013) 847 final, s. 3 ja 17-19.
[180] COM (2013) 847 final, s. 17.
[181] Euroopan parlamentti. Päätöslauselma 12. maaliskuuta 2014 Yhdysvaltojen kansallisen turvallisuusviraston valvontaohjelmasta, eri jäsenvaltioiden valvontaelimistä ja niiden vaikutuksesta EU:n kansalaisten perusoikeuksiin ja transatlanttiseen yhteistyöhön oikeus- ja sisäasioissa (2013/2188(INI).
[182] COM (2013) 847 final.
[183] Päätöslauselma (2013/2188(INI), kohta 39.

Parlamentti katsoi, että Yhdysvaltojen tiedustelupalvelujen laaja pääsy tietoihin on heikentänyt vakavalla tavalla transatlanttista luottamusta ja heikentänyt EU:ssa toimivia yhdysvaltalaisia organisaatioita kohtaan tunnettua luottamusta ja kehotti Yhdysvaltojen viranomaisia esittämään uutta kehystä henkilötietojen siirroille. Tuon kehyksen tulisi täyttää unionin lainsäädännön tietosuojavaatimukset ja siinä tulisi varmistaa vaadittava tietosuojan riittävä taso. Parlamentin mukaan järjestelyn soveltaminen tulisi keskeyttää, kunnes henkilötietojen suojan turvaaminen on varmistettu.[184]

Safe Harbor oli voimakkaan kritiikin ja erilaisten kiistojen kohteena koko 15 vuoden ajan. Järjestelyn perustaminen alkoi transatlanttisesta henkilötietojen suojaa koskevasta kiistasta ja sellainen väritti myös järjestelyn viimeisiä voimassaolovuosia. Lisäksi Safe Harbor aiheutti alusta alkaen erimielisyyttä myös unionin sisällä. Merkittävistä puutteista huolimatta järjestelyn ei missään nimessä voi arvioida olleen täysin tehoton. Safe Harbor-periaatteiden voimassaoloaikana FTC suoritti yhteensä 39 toimenpidettä sellaisia yrityksiä vastaan, jotka rikkoivat sopimusta. Näiden yritysten joukossa ovat muun muassa Google ja Facebook.[185] Vuonna 2012 FTC määräsi Googlen maksamaan 22,5 miljoonan Yhdysvaltain dollarin sakot sovintomääräyksen rikkomisesta johtuen.[186]

Ottaen huomioon Euroopan unionin elinten erimielisyys sopimuksen hyväksymisestä, oikeustieteilijöiden esittämä jatkuva kritiikki, teknologian kehitys ja sen myötä uudistuva lainsäädäntö ja se, että sopimuksen noudattaminen oli lukuisien yhdysvaltalaisten yritysten osalta kyseenalaista, Safe Harborin voi todeta olleen voimassa jopa yllättävän pitkään.

[184] Päätöslauselma (2013/2188(INI), kohdat AQ ja 40.
[185] Federal Trade Commission. Privacy & Data Security. Update: 2017 s. 6. Schwartz 2013, s. 1992 on pitänyt FTC:n suorittamia täytäntöönpanotoimia mielenkiintoisena esimerkkinä EU:n ja Yhdysvaltojen yhteistyössä luodusta lainsäädännöstä, joka on perustunut kahden erilaisen oikeudellisen järjestelmän yhdessä kehittämiin normeihin, ja jonka täytäntöönpanoa toinen osapuoli on suorittanut.
[186] COM (2013) 847 final, s. 11.

7 EUROOPAN UNIONIN TUOMIOISTUIMEN ASIA C-362/14

7.1. Tapauksen taustat

Facebook Inc. (jäljempänä Facebook) on yhdysvaltalainen, vuonna 2004 perustettu, Kalifornian osavaltioon rekisteröity internetissä toimiva yhteisöpalvelu.[187] Palvelussa voi luoda profiilin yksityishenkilönä, yrityksen tai yhteisön nimissä ja palvelun käyttäminen mahdollistaa esimerkiksi omien päivitysten jakamisen, yhteydenpidon ystäviin ja liittymisen erilaisiin yhteisöihin. Rekisteröitymisen ehtoja ovat muun muassa 13 vuoden ikä ja oikeiden henkilötietojen antaminen.[188]

Facebook on vuonna 2008 perustanut tytäryhtiö Facebook Ireland Ltd:n (jäljempänä Facebook Ireland) Irlantiin. Yhtiö jakaa oikeus- ja vastuulausekkeessaan palvelun käyttäjät Yhdysvalloissa tai Kanadassa asuviin käyttäjiin ja muihin käyttäjiin: jos yksityishenkilö asuu Yhdysvalloissa tai Kanadassa tai jos yhteisön pääasiallinen liiketoimintapaikka on noissa valtioissa, oikeus- ja vastuulausekkeen toinen sopimuspuoli on Facebook USA. Muissa tapauksissa kyseisen lausekkeen toinen sopimuspuoli on Facebook Ireland.[189] Facebook on käyttänyt Safe Harbor -järjestelyä siirtäessään palvelunsa käyttäjien tietoja Yhdysvaltoihin.[190]

Itävallan kansalainen Maximillian Schrems oli käyttänyt Facebookia vuodesta 2008.[191] Kesäkuussa 2013 Schrems teki Irlannin valvontaviranomaisille kantelun, jossa hän katsoi, että Yhdysvaltojen oikeus ja käytännöt eivät tarjoa riittävää suojaa viranomaisten harjoittamalta tähän maahan siirrettyjen tietojen tarkkailulta. Schremsin mukaan erityistä huolta aiheuttivat Edward Snowdenin vuonna 2013 tekemät paljastukset viranomaisten kansalaisiin kohdistuvasta verkkovalvonnasta. Euroopan

[187] https://www.facebook.com/pg/facebook/about/?ref=page_internal (Katsottu 18.1.2018).
[188] https://www.facebook.com/legal/terms/update (Katsottu 18.1.2018).
[189] https://www.facebook.com/legal/terms/update (Katsottu 19.1.2018).
[190] https://www.export.gov/safeharbor_eu Facebook Inc. oli Safe Harbor-järjestelyn osapuoli ja sen tiedoissa olevalla listalla ”Relevant Countries from which Personal Information Received” Irlanti on yksi maista, josta henkilötietoja siirrettiin.
[191] Euroopan unionin tuomioistuin: Lehdistötiedote 117/15.

unionin kansalaisten ja unionin alueella asuvien käyttäjien Facebookille antamat tiedot siirretään kokonaan tai osittain Facebookin irlantilaisesta tytäryhtiöstä Yhdysvaltojen alueella sijaitseville palvelimille käsiteltäviksi. Kantelussa Schrems vaati Irlannin tietosuojavaltuutettua käyttämään lakisääteistä toimivaltaansa ja kieltämään Facebook Irelandia siirtämästä hänen henkilötietojaan Yhdysvaltoihin.[192]

Irlannin tietosuojavaltuutettu hylkäsi kantelun perusteettomana katsoen, ettei se ollut velvollinen tutkimaan Schremsin kanteessaan esittämiä seikkoja. Viranomaisen mukaan ei ollut olemassa näyttöä siitä, että NSA olisi päässyt Schremsin henkilötietoihin. Lisäksi Irlannin tietosuojavaltuutettu totesi, ettei Schremsin kantelussaan esittämiä väitteitä voida pitää tehokkaina, koska kaikki kysymykset henkilötietojen suojan riittävyydestä Yhdysvalloissa on ratkaistava päätöksen 2000/520 mukaisesti (Safe Harbor-päätös) ja tässä päätöksessä komissio on todennut Yhdysvaltojen takaavan tietosuojan riittävän tason.[193] Tietosuojavaltuutettu totesi myös, että jo päätöksen luonne ja olemassaolo estivät häntä tutkimasta kysymystä.[194]

7.2. Asian käsittely Irlannin High Court-tuomioistuimessa

Maximillian Schrems nosti tietosuojavaltuutetun päätöksestä kanteen Irlannin High Court-tuomioistuimessa. Heinäkuussa 2014 tekemässään päätöksessä High Court totesi muun ohella, että henkilötietojen sähköinen tarkkailu ja sieppaaminen vastaavat yleisen edun mukaisia tarpeellisia ja välttämättömiä tavoitteita eli kansallisen turvallisuuden säilyttämistä ja vakavien rikosten estämistä. Tuomioistuin katsoi kuitenkin, että Snowdenin tekemät paljastukset ovat osoittaneet NSA:n ja muiden liittovaltion elimien ylittäneen hyväksyttävyyden rajat merkittävällä tavalla. High Court ei päätöksessään epäillyt Snowdenin paljastusten oikeellisuutta. Tuomioistuin lausui, että koska henkilötietoihin tutustumista koskevaan oikeuteen liittyvät päätökset tehdään Yhdysvaltojen oikeuden perusteella, unionin kansalaisilla

[192] Tuomio asiassa C-362/14, kohdat 27-28.
[193] Tuomio asiassa C-362/14, kohta 29.
[194] Julkisasiamies Yves Bot: Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohta 33.

ei ole mitään tosiasiallista oikeutta tulla kuulluiksi heidän tietojensa tarkkailua ja sieppaamista koskevasta kysymyksestä.[195]

High Court katsoi näytetyn todeksi, että kun henkilötietoja siirretään Yhdysvaltoihin, NSA sekä muut Yhdysvaltojen turvallisuusvirastot, kuten Federal Bureau of Investigation (FBI), voivat tutustua niihin tarkkaillessaan ja siepatessaan erottelemattomia massatietoja. Vaikka High Court totesi, että henkilötietojen sähköinen tarkkailu voi olla joissain tilanteissa hyväksyttävää, olisi silloin kuitenkin osoitettava, että määrätyt viestien sieppaamiset ja tiettyjen henkilöiden tai tiettyjen henkilöryhmien tarkkailu ovat objektiivisesti perusteltavissa kansallisen turvallisuuden ja rikollisuuden torjunnan nimissä. Noissa tilanteissa sähköisen viestinnän sieppaamista voitaisiin mahdollisesti pitää Irlannin perustuslain mukaisena.[196] Tuomioistuin katsoi, että koska oli olemassa vakava epäilys siitä, takaako Yhdysvallat henkilötietojen suojan riittävän tason, tietosuojavaltuutetun olisi pitänyt tutkia Schremsin kanne, mikäli asia olisi tullut ratkaista ainoastaan Irlannin lainsäädännön perusteella. Koska asia kuitenkin koski Euroopan unionin perusoikeuskirjan 51 artiklassa[197] tarkoitettua unionin oikeuden soveltamista, pääasiassa kyseessä olevan päätöksen laillisuutta olisi arvioitava unionin oikeuden kannalta.[198]

High Courtin mukaan olennainen kysymys asiassa koski sitä, sitooko komission Safe Harbor-päätöksessä vahvistama toteamus, joka liittyy henkilötietojen suojelua koskevan oikeuden ja käytäntöjen riittävyyteen Yhdysvalloissa, ehdottomasti tietosuojavaltuutettua unionin oikeuden perusteella, kun otetaan huomioon erityisesti myöhemmin voimaan tulleen perusoikeuskirjan 7 ja 8 artikla. Tuomioistuin lausui, että on vaikeaa nähdä, miten Safe Harbor-päätös voisi käytännössä täyttää perusoikeuskirjan 7 ja 8

[195] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohdat 34-36.
[196] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohdat 36 ja 38.
[197] Euroopan unionin perusoikeuskirjan artikla 51: 1. Tämän perusoikeuskirjan määräykset koskevat unionin toimielimiä ja laitoksia toissijaisuusperiaatteen mukaisesti sekä jäsenvaltioita ainoastaan silloin, kun ne soveltavat unionin oikeutta. Tämän vuoksi ne kunnioittavat tämän perusoikeuskirjan mukaisia oikeuksia, noudattavat sen sisältämiä periaatteita ja edistävät niiden soveltamista kukin toimivaltuuksiensa mukaisesti. 2. Tällä perusoikeuskirjalla ei luoda yhteisölle ja unionille uusia toimivaltuuksia.
[198] Tuomio asiassa C-362/14, kohdat 33-34.

artiklan vaatimukset.[199] High Court katsoi, että koska Schremsin kanteessa viitattiin siihen, että Safe Harbor-päätös saattaisi kaiken kaikkiaan olla ristiriidassa perusoikeuskirjan 7 ja 8 artiklan kanssa, EUT saattaisi arvioida, että on mahdollista tulkita henkilötietodirektiiviä ja erityisesti sen 25 artiklan 6 kohtaa sekä Safe Harbor-päätöstä siten, että siinä sallitaan kansallisten viranomaisten tekevän omia tutkimuksiaan selvittääkseen, täyttääkö henkilötietojen siirto kolmanteen maahan perusoikeuskirjan 7 ja 8 artiklasta johtuvat vaatimukset.[200] High Court päätti lykätä asian käsittelyä ja esitti Euroopan unionin tuomioistuimelle asiasta ennakkoratkaisupyynnön.

7.3. Asian käsittely Euroopan unionin tuomioistuimessa

7.3.1. Asian osapuolet ja ennakkoratkaisupyynnön sisältö

Euroopan unionin tuomioistuin vastaanotti High Court of Ireland-tuomioistuimen ennakkoratkaisupyynnön 25.7.2014. Pyyntö esitettiin asiassa, jonka vastapuolet olivat Maximillian Schrems ja Data Protection Commissioner (jäljempänä tietosuojavaltuutettu), Digital Rights Ireland Ltd:n osallistuessa käsittelyyn. Ennakkoratkaisupyyntö koski sitä, että tietosuojavaltuutettu oli kieltäytynyt tutkimasta kantelua, jonka Schrems oli tehnyt sen takia, että Facebook Ireland siirtää Yhdysvaltoihin käyttäjiensä henkilötietoja ja säilyttää niitä kyseisessä maassa sijaitsevilla palvelimilla.[201] Pyyntö koski henkilötietodirektiivin 25 artiklan 6 kohdan ja 28 artiklan tulkintaa Euroopan unionin perusoikeuskirjan 7, 8 ja 47 artiklan kannalta ja pääasiallisesti Safe Harbor-päätöksen pätevyyttä. Tuomio annettiin 6.10.2015.

[199] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohdat 43 ja 46.
[200] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohta 46.
[201] Tuomio asiassa C-362/14, johdanto-osan kohta 2.

7.3.2. Julkisasiamies Botin ratkaisuehdotus

Euroopan unionin tuomioistuimen julkisasiamies Yves Bot antoi oman ratkaisuehdotuksensa[202] 23.9.2015. Ehdotuksessaan julkiasiamies huomautti Maximillian Schremsin Irlannin tietosuojavaltuutetulle tekemän kantelun olevan kaksitahoinen, sillä siinä pyritään ensinnäkin riitauttamaan henkilötietojen siirto Facebook Irelandilta Facebook USA:lle. Toisekseen kantelussa riitautetaan yleisemmin suojan taso, joka tällaisille tiedoille taataan Safe Harbor-järjestelyn yhteydessä.[203]

Botin mukaan Euroopan komissio on väittänyt, että Schrems ei ole esittänyt erityisiä perusteluja, joiden mukaan voitaisiin ajatella, että olisi olemassa välitön vaara siitä, että hänelle aiheutuisi vakavia vahinkoja tietojen siirrosta Facebook Irelandin ja Facebook USA:n välillä ja väittänyt myös, että Schremsin Yhdysvaltojen turvallisuuspalvelun toteuttamista tarkkailuohjelmista esittämät huolet ovat abstrakteja.[204] Tässä yhteydessä on huomioitava, että vuoden 2013 tiedonannoissa[205] komissio ei kyseenalaistanut tarkkailuohjelmien käyttöä ja olemassaoloa, joten komission esittämä mielipide Schrems-asian käsittelyssä on erikoinen.

Botin mukaan High Courtin ennakkoratkaisupyynnön lähtökohtina oli kaksi tosiseikkoja koskevaa toteamusta: se, että NSA ja muut Yhdysvaltojen turvallisuusvirastot voivat tutustua henkilötietoihin, joita Facebook Irelandin kaltaiset yritykset siirtävät Yhdysvaltoihin sijoittautuneelle emoyhtiölleen massiivisten kohdentamattomien tarkkailu- ja sieppaustoimien aikana ja se, että unionin kansalaisilla ei ole mitään tosiasiallista oikeutta tulla kuulluksi siitä, tarkkailevatko ja sieppaavatko NSA ja muut Yhdysvaltojen turvallisuusvirastot heidän tietojaan.[206]

Bot totesi, ettei Safe Harbor-päätöksessä vahvisteta selviä ja täsmällisiä sääntöjä, jotka koskisivat perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin puuttumisen laajuutta. Tekemällä kyseisen päätöksen ja pitämällä sen myöhemmin voimassa Bot katsoi komission ylittäneen rajat,

[202] Julkisasiamies Yves Bot: Ratkaisuehdotus 23.9.2015 asiassa C-362/14.
[203] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohta 49.
[204] Ratkaisuehdotus 23.9.2015 asiassa C-362/15, kohta 59.
[205] COM (2013) 847 final, COM (2013) 846 final.
[206] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohta 155.

joita suhteellisuusperiaatteen noudattaminen edellyttää perusoikeuskirjan 7 ja 8 artiklan ja 52 artiklan 1 kohdan perusteella.[207] Ratkaisuehdotuksensa loppupäätelmänä unionin tuomioistuimen julkisasiamies Bot ehdotti tuomioistuimen ratkaisevan ennakkoratkaisukysymykset siten, että henkilötietodirektiivin 28 artiklaa luettuna unionin perusoikeuskirjan 7 ja 8 artiklan valossa on tulkittava siten, että se, että on olemassa henkilötietodirektiivin 25 artiklan 6 kohdan nojalla tehty komission päätös, ei estä kansallista valvontaviranomaista tutkimasta kantelua, jossa väitetään, että tietty kolmas maa ei takaa siirretyille henkilötiedoille tietosuojan riittävää tasoa ja tarvittaessa keskeyttämästä näiden tietojen siirtoa. Julkisasiamies totesi komission päätöksen 2000/520/EY olevan pätemätön.[208]

7.3.3. Euroopan unionin tuomioistuimen tuomio asiassa C-362/14

EUT muistutti tuomiossaan, että niitä direktiivin säännöksiä, joilla säännellään henkilötietojen käsittelyä, joka saattaa loukata perusvapauksia ja varsinkin oikeutta yksityisyyteen, on välttämättä tulkittava perusoikeuskirjassa taattujen perusoikeuksien valossa. Yksityiselämän kunnioitusta koskevan perusoikeuden, joka taataan perusoikeuskirjan 7 artiklassa ja henkilötietojen suojaa koskevan perusoikeuden, joka taataan perusoikeuskirjan 8 artiklassa, tärkeyttä korostetaan lisäksi unionin tuomioistuimen oikeuskäytännössä.[209]

Tuomioistuimen mukaan kansallisilla valvontaviranomaisilla on perusoikeuskirjan 8 artiklan 3 kohdan ja henkilötietodirektiivin 28 artiklan mukaisesti tehtävänä valvoa yksilöiden suojaa henkilötietojen käsittelyssä koskevien unionin sääntöjen noudattamista, joten kukin niistä on toimivaltainen selvittämään, onko henkilötietojen siirto kolmanteen maahan jäsenvaltiosta, johon kyseinen viranomainen kuuluu, direktiivissä säädettyjen vaatimusten mukaista. Niin kauan kuin unionin tuomioistuin ei ole todennut komission päätöstä pätemättömäksi, jäsenvaltiot ja niiden elimet, joihin niiden itsenäiset valvontaviranomaiset kuuluvat, eivät voi toteuttaa kyseisen

[207] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohdat 214 ja 215.
[208] Ratkaisuehdotus 23.9.2015 asiassa C-362/14, kohta 237.
[209] Tuomio asiassa C-362/14, kohdat 38 ja 39.

päätöksen vastaisia toimenpiteitä, kuten toimia, joilla olisi tarkoitus todeta sitovasti, ettei päätöksen kohteena oleva kolmas maa takaa tietosuojan riittävää tasoa.[210] Tuo päätös ei kuitenkaan voi estää henkilöitä, joiden henkilötietoja on siirretty tai voidaan siirtää kolmanteen maahan, saattamasta vaatimusta oikeuksiensa ja vapauksiensa suojelusta henkilötietojen käsittelyssä kansallisen viranomaisen käsiteltäväksi. [211] Jos näin ei olisi, niiltä henkilöiltä, joiden henkilötiedot on siirretty tai voitaisiin siirtää kolmanteen maahan, vietäisiin perusoikeuskirjan 8 artiklassa taattu oikeus saattaa kansallisten viranomaisten käsiteltäväksi vaatimus perusoikeuksiensa suojaamisesta.[212]

Tuomioistuin päätyi oikeudellisesti merkittävään arvioon katsoessaan, että koska Safe Harbor-periaatteet on niitä koskevan päätöksen liitteessä I olevan 2 kohdan mukaan tarkoitettu käytettäviksi yksinomaan yhdysvaltalaisissa yrityksissä, jotka saavat henkilötietoja unionista ja jotka käyttävät periaatteiden noudattamista keinona Safe Harbor-järjestelmään osallistumiselle asetettujen kelpoisuusvaatimusten täyttämiseksi ja sen luoman tietosuojan riittävyyden olettamuksen saavuttamiseksi, periaatteita sovelletaan vain oman varmennuksensa antaneisiin henkilötietoja unionista saaviin yhdysvaltalaisiin organisaatioihin, mutta vaatimuksena ei ole, että Yhdysvaltojen *viranomaiset* noudattaisivat kyseisiä periaatteita.[213]

Tuomioistuin huomautti, että Safe Harbor-päätöksen liitteessä IV olevassa B kohdassa korostetaan Safe Harbor-periaatteiden sovellettavuuden rajoituksista seuraavasti: on selvää, että jos Yhdysvaltojen lainsäädäntö asettaa yhdysvaltalaiselle organisaatiolle Safe Harbor-periaatteiden kanssa ristiriitaisen velvoitteen, organisaation on noudatettava lakia riippumatta siitä, kuuluuko se Safe Harbor-järjestelmään vai ei. Tuomioistuin katsoi siten, että Safe Harbor-päätöksessä vahvistetaan kansallisen turvallisuuden, yleisen edun ja lainsäädännön vaatimusten ensisijaisuus Safe Harbor-periaatteisiin nähden. EUT:n mukaan Euroopan komissio ei ole todennut Safe Harbor-

[210] Tuomio asiassa C-362/14, kohdat 47 ja 52.
[211] Henkilötietodirektiivin 28 artiklan 4 kohdan mukaan kuka tahansa henkilö tai häntä edustava yhdistys voi esittää valvontaviranomaiselle oikeuksiensa ja vapauksiensa suojelua henkilötietojen käsittelyn osalta koskevan vaateen. Rekisteröidylle ilmoitetaan vaateen seurauksista.
[212] Tuomio asiassa C-362/14, kohdat 53 ja 58.
[213] Tuomio asiassa C-362/14, kohta 82.

päätöksessä Yhdysvaltojen tosiasiallisesti takaavan tietosuojan riittävän tason sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta. Oli siten, luettuna perusoikeuskirjan valossa, katsottava, että päätöksen 1 artiklassa jätetään huomiotta vaatimukset, joista säädetään henkilötietodirektiivin 25 artiklan 6 kohdassa. Tuomioistuin totesi Safe Harbor-päätöksen 1 artiklan olevan pätemätön.[214]

Päätöksen 3 artiklassa ei EUT:n mukaan rajoiteta viranomaisten toimivaltaa toteuttaa toimenpiteitä henkilötietodirektiivin soveltamiseksi annettujen kansallisten säännösten noudattamisen varmistamiseksi, mutta siinä suljetaan pois kyseisten viranomaisten mahdollisuus toteuttaa toimenpiteitä saman direktiivin 25 artiklan noudattamisen varmistamiseksi.[215] Päätöksen 3 artiklan 1 kohdan ensimmäinen alakohta on ymmärrettävä siten, että se estää kansallisia valvontaviranomaisia käyttämästä valtuuksia, jotka niillä on henkilötietodirektiivin 28 artiklan nojalla, kun henkilö esittää tähän säännökseen perustuvan vaatimuksen yhteydessä seikkoja, jotka voivat kyseenalaistaa komission päätöksen, jossa on kyseisen direktiivin 25 artiklan 6 kohdan nojalla todettu kolmannen maan takaavan tietosuojan riittävän tason.[216]

Euroopan unionin tuomioistuimen mukaan oli todettava, että päätöksen 3 artiklalla komissio on ylittänyt toimivallan, joka sille annetaan henkilötietodirektiivin 25 artiklan 6 kohdassa, luettuna perusoikeuskirjan valossa, joten kyseinen 3 artikla oli pätemätön. Koska Safe Harbor-päätöksen 1 ja 3 artiklaa ei voida erottaa päätöksen 2 ja 4 artiklasta eikä päätöksen liitteistä, niiden pätemättömyys vaikuttaa koko päätöksen pätevyyteen. EUT katsoi, että ainoastaan sillä itsellään on oikeus todeta unionin toimen pätemättömyys, koska tuon toimivallan yksinomaisuuden tarkoituksena on taata oikeusvarmuus varmistamalla, että unionin oikeutta sovelletaan yhtenäisesti. Tuomioistuin totesi Safe-Harbor-päätöksen pätemättömäksi.[217]

[214] Tuomio asiassa C-362/14, kohdat 86, 97 ja 98.
[215] Ks. Päätös 2000/520/EY 3 artikla.
[216] Tuomio asiassa C-362/14, kohdat 100, 101, 102.
[217] Tuomio asiassa C-362/14, kohdat 60, 61, 104, 105 ja 106.

7.4. Reaktiot Safe Harborin pätemättömyyteen

Komissio antoi lausunnon EUT:n ratkaisun johdosta heti tuomion julkistamispäivänä. Se muistutti transatlanttisten tiedonsiirtojen tärkeydestä unionin taloudelle ja muista, henkilötietodirektiivin mahdollistamista vaihtoehtoisista mekanismeista tietojen siirrolle. Komissio toi esiin omat toimensa vuodelta 2013, kun se antoi Yhdysvalloille 13 suositusta siitä, kuinka Safe Harboria tulisi parantaa ja kertoi tehneensä vuodesta 2013 lähtien jatkuvaa yhteistyötä Yhdysvaltojen kanssa uudistetun järjestelyn luomiseksi.[218] Tiedonannossaan marraskuussa 2015 komissio katsoi olevan tärkeää saada aikaan uusi kehys henkilötietojen siirtämiselle Yhdysvaltoihin, sillä se on paras keino varmistaa unionin kansalaisten henkilötietojen suojelu niitä Yhdysvaltoihin siirrettäessä.[219]

29 artiklan mukainen tietosuojatyöryhmä totesi omassa lausunnossaan, että sellaiset valtiot, joissa viranomaisilla on tarpeenmukaista laajempi pääsy henkilötietoihin, eivät ole turvallisia kohdevaltioita tietojen siirroille. Mikäli henkilötietoja siirretään Safe Harborin nojalla vielä EUT:n tuomion jälkeen, nuo siirrot ovat laittomia. Työryhmä peräänkuulutti keskustelun avaamista ratkaisun löytämiseksi, jotta tietojen siirtoa voidaan jatkaa ja jotta se tehtäisiin perusoikeuksia kunnioittavalla tavalla.[220] Maximillian Schrems totesi ratkaisun olevan odotettu ja looginen tulos siitä, mihin hän on pyrkinyt.[221] Schremsin mukaan ratkaisu on valtava isku Yhdysvaltojen suorittamalle maailmanlaajuiselle massavalvonnalle, jota suoritetaan suurelta osin yrityksiltä saatujen tietojen kautta. Tuomio teki selväksi sen, ettei yhdysvaltalaisia yrityksiä voi käyttää apuna vakoilussa, jolla rikotaan eurooppalaisten perusoikeuksia.[222]

---

[218] European Commission. Statement 15/5782, Strasbourg 6.10.2015.
[219] Komission tiedonanto Euroopan parlamentille ja neuvostolle direktiiviin 95/46/EY perustuvasta henkilötietojen siirtämisestä EU:sta Yhdysvaltoihin unionin tuomioistuimen asiassa C-362/14 (Schrems) antaman tuomion johdosta. COM (2015) 566 final, s. 15.
[220] Article 29 Working Party. Statement on the implementation of the judgment of the Court of Justice of the European Union of 6 October 2015 in the Maximillian Schrems v Data Protection Commissioner case (C-362-14). Brussels, 16 October 2015.
[221] https://www.theguardian.com/technology/2015/oct/09/facebook-data-privacy-max-schrems-european-court-of-justice
[222] http://www.europe-v-facebook.org/CJEU_IR.pdf

8 PRIVACY SHIELD

8.1. Neuvottelut uudesta tietosuojajärjestelystä

Euroopan unionin tuomioistuimen päätös tarkoitti sitä, ettei henkilötietoja voitu enää siirtää Yhdysvaltoihin Safe Harborin nojalla. Vaikka henkilötietodirektiivi antoi edelleen mahdollisuuden tietojen siirtämiselle muilla menetelmillä, ratkaisu aiheutti järjestelyyn sitoutuneille yrityksille epävarmuutta, kun tietojen siirtäminen Safe Harborin mukaisesti oli julistettu laittomaksi ja käytännössä yritysten oli heti turvauduttava vaihtoehtoisiin tiedonsiirtomenetelmiin. Safe Harborissa oli vuonna 2015 mukana yli 4000 yhdysvaltalaista yritystä, joten tuomion vaikutus oli valtava. Muun muassa Microsoft, Google, Facebook, Apple ja LinkedIn siirsivät henkilötietoja Euroopasta Yhdysvaltoihin Safe Harborin nojalla.[223]

Artiklan 29 mukainen tietosuojatyöryhmä oli omassa EUT:n tuomiota koskevassa lausunnossaan asettanut uutta ja turvallisempaa järjestelyä koskevien neuvottelujen loppuunsaattamisen takarajaksi tammikuun lopun vuonna 2016.[224] 2.2.2016 Euroopan komissio ja Yhdysvallat ilmoittivat päässeensä sopimukseen uudesta Privacy Shield-sopimusjärjestelystä, joka vastasi niitä vaatimuksia, jotka unionin tuomioistuin oli Safe Harbor-sopimusjärjestelyn lakkauttavassa päätöksessään uudelle järjestelylle esittänyt.[225] 29.2.2016 julkistettiin Privacy Shield-järjestelyä koskeva sopimusluonnos ja uudet, Yhdysvaltain kauppaministeriön laatimat periaatteet, joiden mukaan henkilötietojen siirtoa alettaisiin järjestämään.[226]

Euroopan komissio pyysi tiedonannossaan[227] artiklan 29 mukaiselta tietosuojatyöryhmältä lausuntoa uuden järjestelyn tarjoamasta tietosuojan tasosta ja työryhmä julkaisi mielipiteensä vuoden 2016 huhtikuussa. Se totesi, että luonnoksesta löytyy huomattavia parannuksia ja että monet Safe

[223] https://www.export.gov/safeharbor_eu

[224] Article 29 Working Party. Statement on the implementation of the judgment of the Court of Justice of the European Union of 6 October 2015 in the Maximillian Schrems v Data Protection Commissioner case (C-362-14). Brussels, 16 October 2015.

[225] http://europa.eu/rapid/press-release_IP-16-216_en.htm

[226] https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu_us_privacy_shield_full_text.pdf.pdf

[227] Komission tiedonanto Euroopan parlamentille ja neuvostolle. Transatlanttiset tietovirrat: luottamuksen palauttaminen vahvoilla suojatoimilla. COM (2016) 117 final.

Harborin puutteet oli luonnoksessa korjattu. Työryhmä löysi luonnoksesta kuitenkin myös useita puutteita ja epäselvyyksiä, joita se toivoi ratkaistavaksi.[228]

Työryhmä esitti henkilötietodirektiivin 6 artiklaan viitaten huolensa siitä, ettei luonnoksesta löytynyt määräystä henkilötietojen poistamisesta sen jälkeen, kun niitä on käytetty siihen tarkoitukseen, mihin tietoja on kerätty. Myös määräykset henkilötietojen siirtämiselle Yhdysvaltojen ulkopuolelle olivat riittämättömät. Privacy Shield-järjestelyä oli tarkoitus soveltaa myös niihin tilanteisiin, kun tietoja siirrettiin jälleen Yhdysvalloista eteenpäin, ja työryhmän mukaan myös niissä siirroissa tuli kaikilta osin turvata yhtä vahva tietosuojataso kuin Privacy Shield-järjestelyssä. Tietosuojatyöryhmä huomautti myös, että Privacy Shield-sopimuksen tulisi sisältää varaus siitä, että se voidaan mukauttaa toukokuussa 2018 voimaan tuleviin, uuden tietosuoja-asetuksen mukaisiin tiukempiin tietosuojastandardeihin.[229]

Euroopan parlamentti totesi toukokuussa 2016 antamassaan päätöslauselmassa, että komission tulisi panna täysimääräisesti täytäntöön artiklan 29 mukaisen tietosuojatyöryhmän lausunnossaan esittämät suositukset. Se huomautti, että Privacy Shield-sopimusluonnoksen liitteessä on todettu, että muita kuin Yhdysvaltojen kansalaisia koskevien tietojen ja viestien valikoimaton kerääminen on edelleen sallittua tietyin edellytyksin. Valikoimattoman keräämisen olisi pelkästään oltava mahdollisimman räätälöityä ja kohtuullista, mikä ei parlamentin mukaan täytä perusoikeuskirjassa asetettuja tarpeellisuuden ja oikeasuhteisuuden kriteereitä. Päätöslauselmassa pidettiin myönteisenä jäsenvaltioiden tietosuojaviranomaisille annettua näkyvää roolia tutkittaessa perusoikeuskirjan mukaista yksityisyyden suojaamista koskevia väitteitä ja keskeytettäessä tietojen siirtäminen. Myös se, että Yhdysvaltojen ulkoministeriöön oli nimetty oikeusasiamies, jonka tehtävä oli riippumattomien viranomaisten kanssa vastata unionin valvontaviranomaisten välittämiin, valtion harjoittamaa valvontaa koskeviin

[228] Article 29 Data Protection Working Party. Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision (16/EN WP 238) 13.4.2016.
[229] Article 29 Data Protection Working Party. Opinion 01/2016 s. 2, 3 ja 7.

pyyntöihin, oli parlamentin mukaan myönteistä, mutta se ei pitänyt elintä riittävän riippumattomana eikä asianmukaista toimivaltaa omaavana.[230]

Euroopan komissio ilmoitti tehneensä järjestelyyn eräitä parannuksia ja hyväksyneensä Privacy Shield-sopimusjärjestelyn 12.7.2016. Järjestely tuli voimaan välittömästi ja 1.8.2016 alkaen yhdysvaltalaisilla yrityksillä oli mahdollisuus antaa kauppaministeriölle oma varmennuksensa sitoutumisesta järjestelyyn.[231]

8.2. Privacy Shield-järjestely

Privacy Shield-järjestely perustuu Euroopan komission täytäntöönpanopäätökseen EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä.[232] Itse täytäntöönpanopäätös sisältää johdanto-osan sekä kuusi (6) artiklaa. Päätökseen kuuluu lisäksi liitteitä, joihin sisältävät muun muassa Yhdysvaltojen kauppaministeriön hyväksymät EU:n ja Yhdysvaltojen Privacy Shield-järjestelyn periaatteet, Kansallisen tiedusteluviraston päälakimiehen kirjeen sekä EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn signaalitiedustelua koskeva oikeusasiamiesmekanismin.

Päätöksen 1 artiklan 1 kohdan mukaan komissio katsoo direktiivin 95/46/EY 25 artiklan 2 kohdan soveltamiseksi, että Yhdysvallat takaa riittävän suojan henkilötiedoille, jotka siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa unionista Yhdysvalloissa oleville organisaatioille. 1 artiklan 2 kohdan mukaisesti Privacy Shield -järjestely muodostuu Yhdysvaltojen kauppaministeriön 7 päivänä heinäkuuta 2016 antamista järjestelyn periaatteista ja virallisista lausumista ja sitoumuksista, jotka sisältyvät päätöksen liitteisiin. Saman artiklan 3 kohdan mukaan edellä olevan 1 kohdan soveltamiseksi henkilötietoja siirretään EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn puitteissa silloin, kun ne

[230] Euroopan parlamentti. Päätöslauselma transatlanttisista tietovirroista (P8_TA (2016)0233), kohdat 4, 8, 9 ja 12.
[231] Euroopan komissio: Lehdistötiedote. Euroopan komissio ottaa käyttöön EU:n ja Yhdysvaltojen välisen Privacy Shield-järjestelyn: vahvempi suoja transatlanttisille tietovirroille. Bryssel 12.7.2016.
[232] Komission täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä.

siirretään unionista sellaisille Yhdysvalloissa oleville organisaatioille, jotka on sisällytetty Yhdysvaltojen kauppaministeriön liitteessä II esitettyjen järjestelyn periaatteiden I ja III jakson mukaisesti ylläpitämään ja julkisesti saataville asettamaan Privacy Shield -luetteloon.

Päätöksen 2 artiklan mukaan päätös ei vaikuta henkilötietojen käsittelyä jäsenvaltioissa koskevien direktiivin 95/46/EY (henkilötietodirektiivi) säännösten, erityisesti 4 artiklan, soveltamiseen, lukuun ottamatta 25 artiklan 1 kohtaa. 3 artiklassa määrätään, että kun jäsenvaltioiden toimivaltaiset viranomaiset käyttävät toimivaltuuksiaan henkilötietodirektiivin 28 artiklan 3 kohdan mukaisesti keskeyttääkseen sellaiselle Yhdysvalloissa sijaitsevalle organisaatiolle suunnatut tietovirrat tai kieltääkseen ne lopullisesti, joka on sisällytetty Privacy Shield -luetteloon liitteessä II esitettyjen järjestelyn periaatteiden I ja III jakson mukaisesti yksilöiden suojelemiseksi henkilötietojen käsittelyssä, asianomaisen jäsenvaltion on ilmoitettava siitä komissiolle viipymättä.

4 artiklassa määrätään muun ohella päätöksen vuotuisesta arvioinnista ja esimerkiksi siitä, että komissio seuraa jatkuvasti EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toimintaa arvioidakseen, varmistaako Yhdysvallat edelleen järjestelyn puitteissa unionista Yhdysvalloissa sijaitseville organisaatioille siirrettyjen henkilötietojen suojan riittävän tason ja siitä, että jäsenvaltiot ja komissio ilmoittavat toisilleen mahdollisista havainnoista, joiden mukaan kansallisesta turvallisuudesta, lainvalvonnasta tai muusta yleisestä edusta vastaavat Yhdysvaltojen viranomaiset puuttuisivat henkilötietojen suojaa koskevaan oikeuteen enemmän kuin on ehdottoman välttämätöntä sekä niistä tilanteista, joissa komissio esittää luonnoksen toimenpiteistä päätöksen soveltamisen keskeyttämiseksi tai päätöksen muuttamiseksi tai kumoamiseksi taikka sen soveltamisalan rajoittamiseksi. 5 artiklan mukaan jäsenvaltioiden on toteutettava kaikki tämän päätöksen noudattamisen edellyttämät toimenpiteet ja 6 artikla määrää, että päätös on osoitettu kaikille jäsenvaltioille.

Privacy Shield-järjestely perustuu omaan varmennukseen, jolla yhdysvaltalaiset organisaatiot sitoutuvat EU:n ja Yhdysvaltojen välisen Privacy Shield-järjestelyn periaatteisiin. Rajoittamatta henkilötietodirektiivin

nojalla annettujen kansallisten säännösten soveltamista, päätöksellä sallitaan siirrot unionissa olevalta rekisterinpitäjältä tai henkilötietojen käsittelijältä Yhdysvalloissa sijaitseville organisaatioille, jotka ovat antaneet Yhdysvaltojen kauppaministeriölle oman varmennuksen järjestelyn periaatteiden noudattamisesta. Periaatteita sovelletaan ainoastaan yhdysvaltalaisen organisaation suorittamaan henkilötietojen käsittelyyn siltä osin, kuin tällaisten organisaatioiden suorittama käsittely ei kuulu unionin lainsäädännön soveltamisalaan. Järjestelmää hallinnoi ja valvoo Yhdysvaltojen kauppaministeriö.[233]

Kauppaministeriö pitää yllä luetteloa organisaatioista, jotka ovat ilmoittaneet noudattavansa järjestelyn periaatteita ja jotka kuuluvat ainakin yhden päätöksen liitteissä tarkoitetun täytäntöönpanoviranomaisen toimivallan piiriin. Ministeriö päivittää luettelon organisaatioiden vuosittain antamien uudelleenvarmennusten perusteella ja aina kun organisaatio peruuttaa osallistumisensa Privacy Shield -järjestelyyn tai se poistetaan järjestelyn piiristä. Organisaation on kuuluttava Yhdysvaltojen viranomaisten, erityisesti liittovaltion kauppakomission (FTC) tutkinta- ja täytäntöönpanovallan piiriin, jotta voidaan tehokkaasti varmistaa periaatteiden noudattaminen.

Jotta organisaatio voi jatkaa osallistumistaan järjestelyyn saadakseen henkilötietoja unionista, sen on vuosittain varmennettava uudelleen osallistumisensa järjestelyyn. Jos organisaatio jättäytyy järjestelyn ulkopuolelle, sen on poistettava kaikki julkiset lausumat, jotka antaisivat ymmärtää, että se osallistuu edelleen Privacy Shield -järjestelyyn tai että se on oikeutettu järjestelyn etuihin, erityisesti kaikki sen julkaistuissa tietosuojaperiaatteissa olevat viittaukset järjestelyyn.[234]

Yhdysvaltojen tiedusteluvirastot voivat pyytää henkilötietoja ainoastaan silloin, kun pyyntö on ulkomaantiedustelun valvontaa koskevan lain (Foreign Intelligence Surveillance Act, FISA) mukainen tai sen on tehnyt Yhdysvaltojen liittovaltion poliisi (FBI) niin sanotun kansallista turvallisuutta koskevan kirjeen (National Security Letter, NSL) perusteella. Yhdysvaltojen hallitus on antanut komissiolle nimenomaisen vakuutuksen siitä, että

[233] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 14, 15 ja 18.
[234] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 26, 31, 35 ja 54.

Yhdysvaltojen tiedusteluyhteisö ei harjoita kehenkään, esimerkiksi tavallisiin unionin kansalaisiin, kohdistuvaa kohdentamatonta valvontaa. Valikoimaton keruu voidaan hyväksyä ainoastaan poikkeuksellisesti, jos kohdennettu keruu ei ole mahdollinen, ja siihen liitetään ylimääräisiä suojatoimia, joilla kerättyjen tietojen määrä ja niihin pääsy minimoidaan.[235]

Komission analyysin mukaan Yhdysvaltojen lainsäädäntö sisältää useita rajoituksia Privacy Shield -järjestelyn puitteissa siirrettyihin tietoihin pääsylle ja niiden käytölle kansallisen turvallisuuden nimissä sekä valvontamekanismeja ja oikeussuojakeinoja, jotka tarjoavat riittävät suojatoimet tietojen suojaamiseksi tehokkaasti laittomalta pääsyltä ja väärinkäytösten riskiltä.[236]

8.2.1 Privacy Shield-periaatteet

Yhdysvaltain kauppaministeriön julkaisemia Privacy Shield-periaatteita on seitsemän. Järjestely sisältää lisäksi eräitä täydentäviä periaatteita. Euroopan komissio katsoo päätöksessään, että Yhdysvaltojen kauppaministeriön hyväksymät järjestelyn periaatteet varmistavat kokonaisuutena tarkastellen sellaisen henkilötietojen suojan tason, joka olennaisilta osin vastaa henkilötietodirektiivissä vahvistetuissa perusperiaatteissa taattua tasoa.[237]

Ilmoitusperiaate määrittää järjestelyyn sitoutuneelle organisaatiolle kuuluvia tiedonantovelvollisuuksia. Organisaation on muun muassa ilmoitettava osallistumisestaan järjestelyyn ja annettava ilmoitus siitä, minkä tyyppisiä henkilötietoja kerätään ja mihin tarkoituksiin niitä käytetään. Henkilölle on annettava tieto kaikista asiankuuluvista unionissa sijaitsevista elimistä, jotka voivat vastata tiedusteluihin tai valituksiin ja siitä, minkä tyyppisille kolmansille osapuolille organisaatio luovuttaa henkilötietoja sekä vaatimuksesta, jonka mukaan henkilötietoja on luovutettava lainmukaisen, julkisen viranomaisen esittämän pyynnön nojalla muun muassa kansalliseen turvallisuuteen tai lainvalvontaan liittyvien vaatimusten täyttämiseksi. Ilmoitus on annettava, kun henkilöä pyydetään ensimmäistä kertaa antamaan

[235] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 78, 82 ja 89.
[236] Täytäntöönpanopäätös (EU) 2016/1250, kohta 67.
[237] Täytäntöönpanopäätös (EU) 2016/1250, kohta 137.

henkilötietoja organisaatiolle, tai niin pian kuin ilmoituksen antaminen on käytännössä mahdollista.

Valintaperiaatteen mukaisesti henkilölle on muun muassa tarjottava mahdollisuus valita, voiko heidän henkilötietojaan luovuttaa kolmannelle osapuolelle tai käyttää olennaisesti erilaiseen tarkoitukseen kuin siihen, johon ne oli alun perin kerätty tai johon henkilöt ovat sittemmin antaneet suostumuksensa. Valintamahdollisuutta ei tarvitse tarjota, kun tiedot annetaan kolmannelle osapuolelle, joka toimii kyseisen organisaation edustajana suorittaen tiettyä tehtävää organisaation puolesta ja sen ohjeiden mukaisesti.

Henkilötietojen edelleen siirtämiseen liittyvä vastuuvelvollisuusperiaate määrää, jotta organisaatio voi siirtää henkilötietoja kolmannelle osapuolelle, sen on noudatettava ilmoitus- ja valintaperiaatteita. Sen on tehtävä sopimus rekisterinpitäjänä toimivan kolmannen osapuolen kanssa. Tietojen vastaanottajan on sitouduttava järjestämään tietosuoja, jonka taso vastaa järjestelyn periaatteita. Jotta organisaatio voi siirtää henkilötietoja kolmannelle osapuolelle, sen on siirrettävä henkilötietoja vain tiettyä rajoitettua tarkoitusta varten ja varmistettava, että edustaja käsittelee siirrettyjä henkilötietoja tavalla, joka vastaa periaatteiden mukaisia organisaation velvoitteita sekä vaadittava edustajaa ilmoittamaan, jos se toteaa, ettei enää kykene tarjoamaan vaadittavaa tietosuojaa. Jos luvatonta tiedonkäsittelyä havaitaan, organisaation on ryhdyttävä toimiin tilanteen korjaamiseksi.

Turvallisuusperiaatteen mukaan organisaatioiden, jotka keräävät, säilyttävät, käyttävät tai levittävät henkilötietoja, on toteutettava kohtuullisia ja asianmukaisia toimenpiteitä, joilla henkilötietoja suojataan katoamiselta, väärinkäytöltä, luvattomalta pääsyltä, luovuttamiselta, muuttamiselta tai tuhoamiselta. *Tietojen eheyden ja käyttötarkoituksen rajoittamisen periaate* määrää, että henkilötietojen laajuus on rajoitettava tietoihin, jotka ovat merkityksellisiä tietojenkäsittelyn tarkoituksen kannalta. Organisaation on varmistettava, että henkilötiedot ovat käyttötarkoitukseensa nähden luotettavia ja että ne ovat tarkkoja, täydellisiä ja ajantasaisia. Tietoja saa säilyttää muodossa, josta henkilöllisyys käy ilmi tai se on selvitettävissä vain

niin kauan kuin se on tarpeen. Velvoite ei estä organisaatioita käsittelemästä henkilötietoja pitempiäkin aikoja, jos käsittelyn kesto ja laajuus palvelevat kohtuullisella esimerkiksi tieteellistä tutkimusta.

Tietoihin pääsyä koskevan periaatteen mukaisesti henkilöiden on saatava itseään koskevat tiedot organisaatiolta ja voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä tai joita on käsitelty järjestelyn periaatteiden vastaisesti. Soveltamista on rajoitettu esimerkiksi sellaisissa tapauksissa, joissa tiedonsaantikustannukset olisivat suhteettoman suuria suhteessa tietosuojaan kohdistuviin riskeihin.

Muutoksenhaku-, täytäntöönpano- ja vastuuperiaatteen mukaan tehokkaaseen tietosuojaan on sisällyttävä helposti käytettävissä olevat riippumattomat muutoksenhakumekanismit, seurantamenettelyt ja organisaatioille asetettava velvollisuus korjata puutteet, jotka johtuvat siitä, että ne eivät ole noudattaneet järjestelyn periaatteita, vaikka ovat ilmoittaneet noudattavansa niitä ja tällaisille organisaatioille koituvat seuraamukset. Kun henkilötietoja lähetetään edelleen, Järjestelyyn sitoutunut organisaatio on vastuussa sellaisten henkilötietojen käsittelystä, jotka se on vastaanottanut järjestelyssä ja sittemmin siirtänyt sen edustajana toimivalle kolmannelle osapuolelle. Järjestelyyn sitoutunut organisaatio on periaatteiden mukaan korvausvelvollinen, jos sen edustaja käsittelee henkilötietoja tavalla, joka ei ole järjestelyn periaatteiden mukainen, ellei organisaatio osoita, että se ei ole vastuussa tapahtumasta, joka johti syntyneeseen vahinkoon.

8.3. Safe Harbor vs. Privacy Shield – merkittävimmät eroavaisuudet

Kokonaisuudessaan Privacy Shield-järjestely on edeltäjäänsä tarkempi ja kattavampi. Periaatteiden lähtökohdat ovat samat kuin Safe Harbor-järjestelyssä, mutta niihin on tehty eräitä tarkennuksia ja lisäyksiä ja joidenkin periaatteiden nimet ovat muuttuneet. Sopimuksessa on lisäksi perustettu täysin uusia velvoitteita henkilötietoja käsitteleville organisaatioille ja siinä on määritelty täsmällisemmin Yhdysvaltain viranomaisten pääsyä järjestelyn nojalla siirrettyihin henkilötietoihin. Sopimustekstistä on huomattavissa, että paljastukset Yhdysvaltojen harjoittamasta massavakoilusta ovat vaikuttaneet Privacy Shield-järjestelyn sisältöön.

EUT oli Schrems-tuomiossaan huomauttanut, ettei komissio ollut Safe Harbor-päätöksessään todennut Yhdysvaltojen tosiasiallisesti takaavan tietosuojan riittävää tasoa sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta.[238] Privacy Shield-sopimuksessa komissio toteaa analysoineensa Yhdysvaltojen lainsäädäntöä ja käytäntöä huolellisesti ja päättelee Yhdysvaltojen takaavan tietosuojan riittävän tason Privacy Shield-järjestelyn puitteissa siirretyille henkilötiedoille.[239]

Privacy Shield-järjestelyn keskeiset erot suhteessa kumottuun Safe Harboriin voidaan jakaa neljään eri kokonaisuuteen:

1) **Yrityksen ilmoitus. ja tiedonantovelvollisuudet**
2) **Yksilön valitusmahdollisuudet ja oikeussuojakeinot**
3) **Säännökset koskien tietojen siirtämistä eteenpäin**
4) **Yhdysvaltain viranomaisten pääsy henkilötietoihin**

Safe Harbor-järjestelyn ilmoitusperiaate oli yleisesti muotoiltu ja suppea. Periaate on Privacy Shieldin myötä muuttunut merkittävästi ja järjestelyyn sitoutuneilla yrityksillä on uusia ja tiukempia määräyksiä liittyen **ilmoitus- ja tiedonantovelvollisuuksiin**. Yrityksen on ilmoitettava sitoutumisestaan järjestelyyn ja annettava linkki Privacy Shield-luetteloon tai luettelon verkko-osoite. Yhteystietojen lisäksi on kerrottava, kuinka organisaatiolle voi esittää tiedusteluja tai valituksia ja tiedotettava unionin elimistä, jotka voivat vastata tiedusteluihin tai valituksiin. Organisaation on kerrottava henkilön oikeudesta tutustua henkilötietoihinsa ja hänen mahdollisuuksistaan rajoittaa henkilötietojensa käyttöä ja julkistamista. Lisäksi on tiedotettava riippumattomasta riitojenratkaisuelimestä, joka on nimetty valitusten käsittelyä varten ja johon henkilö voi turvautua maksutta.[240]

Ilmoitus- ja tiedonantovelvollisuuksiin kuuluu myös ilmoitus siitä, että organisaatio on Yhdysvalloissa toimivaltaisen lakisääteisen elimen tutkinta- ja täytäntöönpanovallan alainen, mahdollisuudesta saada asia sitovan välimiesmenettelyn käsiteltäväksi ja vaatimuksesta, jonka mukaan henkilötietoja on luovutettava pyynnön nojalla esimerkiksi kansalliseen

[238] Tuomio asiassa C-362/14, kohta 97.
[239] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 13 ja 136-40.
[240] Täytäntöönpanopäätös (EU) 2016/1250. Liite II, jakso II, kohta 1.

turvallisuuteen liittyvien vaatimusten täyttämiseksi sekä organisaation vastuusta silloin, kun tietoja on siirretty edelleen kolmansille osapuolille. Tiedonantovelvollisuuksiin liittyy myös tietoihin pääsyä koskeva periaate, jonka mukaan henkilön on saatava itseään koskevat tiedot organisaatiolta ja voitava korjata, muuttaa tai poistaa tiedot, jotka eivät ole paikkansapitäviä tai joita on käsitelty periaatteiden vastaisesti.[241]

Privacy Shield-järjestelyssä on kehitetty yksilölle kattavampia **valitusmahdollisuuksia ja oikeussuojakeinoja**. Jos henkilö epäilee, että hänen henkilötietojaan on käsitelty järjestelyn periaatteiden vastaisesti, hän voi tehdä valituksen organisaatiolle, organisaation nimeämälle riippumattomalle riitojenratkaisuelimelle, kansallisille tietosuojaviranomaisille tai liittovaltion kauppakomissiolle. Organisaatiolla on oltava käytössään tehokas oikeussuojamekanismi ja valituksen saatuaan sen on vastattava valituksen tekijälle 45 päivän kuluessa ja otettava kantaa valitukseen aiheellisuuteen ja siihen, miten mahdollinen ongelma aiotaan korjata. Valitus voidaan esittää myös organisaation valitsemalle Euroopan unionissa tai Yhdysvalloissa sijaitsevalle riippumattomalle riitojenratkaisuelimelle.[242] Esimerkiksi Facebook pyytää toimittamaan valitukset yhtiölle itselleen. Mikäli yhtiö ei ole vastannut valitukseen määrätyn 45 päivän kuluessa, pyytää se ottamaan yhteyttä valitsemaansa riitojenratkaisuelimeen.[243]

Privacy Shield-järjestelyn määrittämiä valituselimiä ovat myös unionin jäsenvaltioiden kansalliset tietosuojaviranomaiset sekä Yhdysvaltain kauppaministeriö. Jos mikään muu oikeussuojamekanismi ei ole ratkaissut valitusta tyydyttävästi, viimesijainen muutoksenhakumekanismi on Privacy Shield-paneelin sitova välimiesmenettely. Paneelissa on vähintään 20 kauppaministeriön ja komission nimittämää välimiestä ja yksittäisessä kiistassa asia on mahdollisuus ratkaista yhden tai kolmen välimiehen paneelissa.[244]

[241] Täytäntöönpanopäätös (EU) 2016/1250. Liite II, jakso II, kohdat 1 ja 6.
[242] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 41, 43, 44 ja 45.
[243] https://www.privacyshield.gov/participant?id=a2zt0000000GnywAAC&status=Active
[244] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 48-52 ja 56-57.

Jo Safe Harbor-järjestelyssä määritettiin **tietojen siirtämistä edelleen kolmannelle osapuolelle**, mutta Privacy Shield-järjestely asettaa tietojen siirtämiselle useita uusia velvoitteita ja rajoituksia. Organisaation on tehtävä sopimus rekisterinpitäjänä toimivan kolmannen osapuolen kanssa ja sopimuksessa on määrättävä, että tietoja voidaan käsitellä vain tiettyä tarkoitusta varten siten, että tarkoitus vastaa henkilön asiassa antamaa suostumusta. Tietojen vastaanottajan on järjestettävä tietosuoja, jonka taso vastaa Privacy Shield-järjestelyn periaatteita. Samat velvollisuudet ovat voimassa myös silloin, kun organisaatio siirtää henkilötietoja sen edustajana toimivalle kolmannelle osapuolelle. Organisaatio on vastuussa sellaisten henkilötietojen käsittelystä, jotka se on vastaanottanut järjestelyn nojalla ja siirtänyt edustajanaan toimivalle kolmannelle osapuolelle.[245]

Privacy Shield-järjestelyssä on rajoitettu **Yhdysvaltain viranomaisten pääsyä järjestelyn nojalla Euroopasta siirrettyihin henkilötietoihin**. Safe Harborin osalta EUT oli Schrems-tuomiossa todennut, ettei päätöksessä vaadittu Yhdysvaltojen viranomaisten noudattavan Safe Harbor-periaatteita.[246] Lisäksi paljastukset massavalvonnasta käytännössä edellyttivät, että uudessa järjestelyssä viranomaisten pääsyä tietoihin oli rajoitettava ja säänneltävä kattavasti, sillä paljastukset olivat vakavia ja liittyivät useisiin Safe Harbor-järjestelyyn sitoutuneisiin yhdysvaltalaisiin yrityksiin.

Yksi rajoitus koskee Yhdysvaltojen harjoittamaa signaalitiedustelutoimintaa, jota sääntelee vuonna 2014 annettu PPD 28-direktiivi (Presidential Policy Directive 28). Kyseessä on presidentin määräys, joka sitoo Yhdysvaltojen tiedusteluviranomaisia ja on sitova valtion hallinnossa tapahtuvista muutoksista huolimatta. Direktiivin mukaan tietojen keruun on perustuttava säädökseen tai presidentin hyväksyntään ja se on suoritettava Yhdysvaltojen perustuslain ja Yhdysvaltojen lainsäädännön mukaisesti. Toiminnassa on lisäksi huomioitava asianmukaiset suojatoimet kaikkien henkilöiden henkilötietojen osalta riippumatta heidän kansallisuudestaan tai siitä, missä he mahdollisesti asuvat. PPD-28 määrittää myös valikoimatonta ja kohdennettua tiedustelua. Vaikka signaalitiedustelutietoja on joskus kerättävä

[245] Täytäntöönpanopäätös (EU) 2016/1250, liite II, jakso II, kohdat 3 ja 7d.
[246] Tuomio asiassa C-362/14, kohta 82.

valikoimattomina, etusija on niillä keräämisvaihtoehdoilla, jotka mahdollistavat kohdennetun signaalitiedustelun.[247]

Yhdysvalloissa tuli vuonna 2015 voimaan USA Freedom Act-laki[248], joka vaikuttaa Privacy Shield-järjestelyn puitteissa siirrettyjen henkilötietojen suojaan. Laissa kielletään valikoimattoman tiedon kerääminen sekä yhdysvaltalaisista että ei-yhdysvaltalaisista henkilöistä FISA-lain nojalla tai käyttämällä kansallista turvallisuutta koskevia kirjeitä (NSL). Kielto käsittää erityisesti puhelinliikenteen metadatan, joka koskee Yhdysvalloissa olevien ja Yhdysvaltojen ulkopuolella olevien henkilöiden välisiä puheluita, ja kattaa myös näillä toimivaltuuksilla kerättyjä Privacy Shield -järjestelyn tietoja. Laissa edellytetään, että hallitus käyttää näitä tietojen haun mahdollistavia toimivaltuuksiaan ainoastaan ns. erityisen valintakriteerin pohjalta. Yhdysvaltojen hallituksen on vuosittain ilmoitettava kongressille haettujen ja myönnettyjen FISA-määräysten lukumäärä ja arviot valvonnan kohteena olevien yhdysvaltalaisten ja ei-yhdysvaltalaisten henkilöiden määrästä.[249]

Privacy Shield-järjestelyn toteuttamiseksi on luotu uusi, signaalitiedustelua koskeva valvonta- ja oikeussuojamekanismi Yhdysvaltain ulkoministeriöön perustetun oikeusasiamiehen viralla. Mekanismiin kuuluu tietosuojasta vastaava oikeusasiamies eli alivaltiosihteeri ja muuta henkilöstöä sekä muita toimivaltaisia valvontaelimiä, jotka valvovat tiedusteluyhteisön eri toimijoita. Oikeusasiamies vastaanottaa yksittäisiä valituksia ja vastaa niihin. Se on velvoitettu vahvistamaan, onko sovellettavia periaatteita noudatettu tai miten tilanne tullaan korjaamaan. Oikeusasiamiehen todetaan olevan Yhdysvaltojen tiedusteluyhteisöstä riippumaton. Komissio on todennut ottaneensa huomioon EUT:n Schrems-tuomion toteamuksen, jonka mukaan yksityisille ei Safe Harbor-järjestelyssä tarjottu tehokasta oikeussuojaa ja toteaa Yhdysvaltojen tarjoavan oikeussuojakeinoja esimerkiksi oikeusasiamiehen muodossa.[250]

Privacy Shield-järjestelyn periaatteiden noudattamista voidaan rajoittaa kansallisen turvallisuuden, yleisen edun tai lainvalvonnan vaatimusten vuoksi

[247] Täytäntöönpanopäätös (EU) 2016/1250, kohdat 68-72.
[248] USA Freedom Act of 2015. Public Law No. 114-23.
[249] Täytäntöönpanopäätös (EU) 2016/1250, liite VI, jakso III.
[250] Tuomio asiassa C-362/14, kohta 95. Täytäntöönpanopäätös (EU) 2016/1250, kohdat 117-121.

lailla, hallituksen antamalla asetuksella tai tuomioistuimen päätöksellä, jonka seurauksena syntyy ristiriitaisia velvoitteita tai jossa annetaan nimenomainen lupa tiettyyn toimintaan, jos organisaatio voi tällaista lupaa käyttäessään osoittaa, että organisaatio poikkeaa periaatteista vain siinä määrin kuin on tarpeellista, jotta lupaan liittyvä ensisijainen ja perusteltu intressi voi toteutua tai jos jäsenvaltion lainsäädännössä sallitaan poikkeus.[251]

8.4. Arvioita järjestelyn tehokkuudesta

29 direktiivin mukainen tietosuojatyöryhmä antoi oman lausuntonsa Privacy Shield-järjestelystä pian komission päätöksen hyväksymisen jälkeen. Se totesi odottaneensa tiukempia takuita oikeusasiamiehen itsenäisyydelle ja toimivallalle ja huomautti, ettei järjestely tarjoa konkreettisia takuita siitä, ettei massavalvontaa tai valikoimatonta tietojen keräämistä toteuteta. Työryhmä korosti järjestelyn ensimmäisen vuosiraportin merkitystä ja sitä, että kaikilla arviointiryhmän jäsenillä tulisi olla pääsy kaikkeen tarpeelliseen informaatioon arvioinnin suorittamiseksi myös sen osalta, missä määrin Yhdysvaltojen viranomaisilla on ollut pääsy henkilötietoihin.[252] Maximillian Schremsin mukaan Privacy Shield ei tule selviytymään oikeudellisista haasteistaan ja Edward Snowden ei uskonut järjestelyllä olevan todellisia rajoittavia vaikutuksia Yhdysvaltain suorittamaan massavalvontaan.[253]

Euroopan parlamentti arvioi huhtikuussa 2017 hyväksytyssä päätöslauselmassaan Privacy Shield-järjestelyn tarjoaman suojan riittävyyttä. Sen mukaan oli myönteistä, että järjestelyssä on parannettu normien selkeyttä ja annettu jäsenvaltioiden tietosuojaviranomaisille merkittävämpi rooli vaateiden tutkimisessa ja tietojen siirron keskeyttämisessä tarpeen tullen. Se esitti kuitenkin huolen siitä, että Yhdysvaltojen antamien ”kirjallisten vakuutusten” oikeudellinen asema oli edelleen epäselvä ja katsoi massavalvonnan olevan edelleen mahdollista. Parlamentti totesi lisäksi, että yksityishenkilöiden käytössä olevat kanneperusteet ovat vähäiset, eikä

[251] Täytäntöönpanopäätös (EU) 2016/1250, kohta 64 ja liite II, jakso 1, kohta 5.
[252] Article 29 Working Party. Statement on the decision of the European Commission on the EU-U.S. Privacy Shield, 26.7.2016.
[253] https://euobserver.com/digital/134322EU EU
https://euobserver.com/justice/134958

yksilöillä ole todellisuudessa käytössään sellaisia tehokkaita oikeussuojakeinoja, joita voitaisiin hyödyntää silloin, jos henkilötietoja on siirretty Privacy Shield-periaatteiden mukaisesti ja jos Yhdysvaltojen viranomaiset käsittelevät niitä yleisen edun ja lainvalvonnan nimissä. Parlamentti totesi, että järjestelyn tehokkuutta koskevat puutteet ja huolenaiheet voivat aiheuttaa sen, että tuomioistuimissa tullaan nostamaan kanteita suojan riittävyyttä koskevan päätöksen tarkastelemiseksi. Parlamentti pyysi komissiota varmistamaan, että Privacy Shield-järjestelyn sitoumukset pysyvät voimassa myös Yhdysvaltojen uuden hallinnon ottaessa tehtävänsä vastaan.[254]

Tietosuoja-alan vahtikoirajärjestöt eivät suhtautuneet optimistisesti järjestelyn tehokkuuteen. Electronic Frontier Foundation (EFF) totesi, ettei Privacy Shield estä Yhdysvaltojen viranomaisten joukkovalvontaa ja huomautti jääneen epäselväksi, mitä järjestelyllä ylipäätään halutaan suojella.[255] Jo pian sen jälkeen, kun Privacy Shield-periaatteet oli alkuvuodesta 2016 julkaistu, 17 kansainvälistä tietosuoja-alan kansalaisjärjestöä laati kirjeen Euroopan komission oikeusasioista vastaavalle komissaarille. Järjestöt totesivat, että Privacy Shield heikentää luottamusta digitaaliseen talouteen ja sen kautta joukkovalvonnassa tapahtuvat ihmisoikeusloukkaukset voivat jatkua. Muun muassa Amnesty International USA, Privacy International, Digital Rights Ireland ja Electronic Privacy Information Center kuuluivat kirjeen allekirjoittaneisiin järjestöihin.[256]

8.4.1. Privacy Shield-järjestelyn ensimmäinen vuosiraportti

Privacy Shield-päätöksen 4 artiklan 4 kohdan mukaisesti Euroopan komission tulee vuosittain arvioida päätöksen 1 artiklan 1 kohdan päätelmä eli se, että Yhdysvaltojen takaama suoja henkilötietojen siirrolle järjestelyn puitteissa on riittävä. Komissio antoi ensimmäisen vuosikertomuksensa

[254] Euroopan parlamentti. Päätöslauselma 6. huhtikuuta 2017 EU:n ja Yhdysvaltojen Privacy Shield -järjestelyn tarjoaman suojan riittävyydestä (2016/3018(RSP), kohdat 2, 5, 8, 11, 16, 24 ja 26.
[255] https://www.eff.org/deeplinks/2016/03/privacy-shield-riddled-surveillance-holes
[256] https://edri.org/wp-content/uploads/2016/03/PrivacyShield_Letter_Coalition_March2016.pdf

lokakuussa 2017 ja totesi Yhdysvaltojen perustaneen sovitut oikeussuojamekanismit, kuten oikeusasiamiehen viran ja turvaavan edelleen henkilötietojen suojan riittävän tason.[257]

Arviointiinsa perustuen komissio antoi suosituksia järjestelyn kehittämiseksi ja parantamiseksi. Se huomautti, etteivät sellaiset yritykset, joita kauppaministeriö ei ole vielä hyväksynyt Privacy Shield-järjestelyn osapuoliksi, saisi julkisesti ilmoittaa sertifioinnistaan. Tällainen toiminta aiheuttaa epäselvyyksiä ja heikentää järjestelyn luotettavuutta. Yritys saisi tehdä ilmoituksen vasta, kun se on mukana virallisella Privacy Shield-listalla. Komission mukaan kauppaministeriön tulisi säännöllisesti tehdä tarkistuksia siitä, onko olemassa yrityksiä, jotka väärin perustein väittävät olevansa järjestelyn osapuolia. Tarkistuksia voisi suorittaa esimerkiksi internet-hakujen avulla.[258]

Lisäksi komissio suositteli, että kauppaministeriön tulisi tehdä säännöllisiä tarkastuksia Privacy Shield-periaatteiden noudattamisesta esimerkiksi vuosittain suoritettavan organisaation uudelleen sertifioinnin yhteydessä. Komissio toivoi kauppaministeriöltä ja kansallisilta tietosuojaviranomaisilta tiivistä yhteistyötä, jotta ne laatisivat ohjeistuksia koskien niitä järjestelyn osa-alueita, joiden noudattaminen vaatii lisää selvennystä tai tarkennuksia.[259]

Komissio oli tullut siihen johtopäätökseen, että Yhdysvaltain lainsäädäntö, joka rajoittaa henkilötietojen käyttöä ja keräämistä kansallisen turvallisuuden käyttötarkoituksiin, tarjoaa riittävän suojan järjestelyn nojalla siirretyille henkilötiedoille.[260] Se toivoi erityisesti PPD-28:n yksityisyyden suojaa koskevien säännösten suojaamista FISA-laissa. Komission suositus liittyi FISA-lain 702 pykälään, joka antaa Yhdysvaltain tiedusteluviranomaisille mahdollisuuden pyytää pääsyä tiettyjen ei-yhdysvaltalaisten, Yhdysvaltojen ulkopuolella olevien henkilöiden tietoihin. Pykälässä oli päättymislauseke, jonka mukaan soveltaminen päättyi vuoden 2017 lopussa. Komission mukaan

[257] Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield. COM (2017) 611 final., s. 4.
[258] COM (2017) 611 final, s. 4-5.
[259] COM (2017) 611 final, s. 5-6.
[260] Commission Staff Working Document. Accompanying the document Report from the Commission to the European Parliament and the Council on the first annual review of the functioning of the EU–U.S. Privacy Shield. SWD (2017) 344 final, s. 21.

lainsäädäntöuudistus antoi Yhdysvaltojen hallinnolle mahdollisuuden vahvistaa FISA-lain yksityisyyden suojaa koskevia säännöksiä.[261]

FISA-laissa säädetään, että ulkomaantiedustelutiedon hankkiminen kohdistamalla tiedustelu Yhdysvaltojen ulkopuolella olevaan ei-yhdysvaltalaiseen henkilöön on luvallista ja että yhdysvaltalaiset sähköisiä viestintäpalveluja tarjoavat yritykset voidaan pakottaa avustamaan tässä. 702 §:n mukaista tiedonkeruuta pidetään signaalitiedusteluna, ja PPD-28:n vaatimuksia sovelletaan siihen.[262] Yhdysvallat hyväksyi FISA-lain uudistuksen tammikuussa 2018 ja sen vaikutuksia käsitellään Sääntelyn tulevaisuus ja johtopäätökset-luvussa.

Vaikka oikeusasiamiehen virka oli perustettu, sitä ei oltu vielä täytetty. Komissio totesi odottavansa, että osoittaakseen sitoutumistaan kyseessä olevaan oikeussuojamekanismiin, Yhdysvaltojen tulisi täyttää virka mahdollisimman pian.[263]

8.4.2. Tietosuojatyöryhmän raportti

Artiklan 29 mukainen tietosuojatyöryhmä osallistui Privacy Shield-järjestelyn ensimmäiseen vuosiarviointiin ja antoi siitä oman kertomuksensa. Se keskittyi arvioimaan sekä järjestelyn kaupallisia näkökulmia, että Yhdysvaltojen viranomaisten pääsyä henkilötietoihin tilanteissa, joissa on kyse kansallisesta turvallisuudesta.

Arvioidessaan järjestelyn toimivuutta kaupallisten näkökulmien osalta työryhmä huomioi Yhdysvaltojen viranomaisten toimet Privacy Shield-järjestelyn vaatimusten toteuttamiseksi, mutta esitti arviossaan myös seikkoja, joiden osalta järjestely ei toimi odotetusti. *Ohjeistuksen ja informaation puute* koskee sekä yrityksiä, että yksittäisiä unionin alueen kansalaisia. Työryhmän mukaan yrityksillä tulisi olla selkeät ohjeistukset järjestelyn vaatimusten pääasiallisesta sisällöstä ja siitä, kuinka vaatimukset toteutetaan käytännössä. Se totesi, että unionissa on useassa eri lähteessä

[261] COM (2017) 611 final, s. 4 ja 6.
[262] Täytäntöönpanopäätös (EU) 2016/1250, liite VI, jakso II.
[263] COM (2017) 611 final, s. 4 ja 6.

tarjolla Privacy Shield-järjestelyä koskevaa, yksityisille henkilöille suunnattua informaatiota. Kuitenkin suurin osa virallisella, Yhdysvaltain kauppaministeriön ylläpitämällä Privacy Shield-verkkosivulla olevasta informaatiosta on suunnattu yrityksille. Myös yksityisille tulisi olla tarjolla helposti saatavilla olevaa ja ymmärrettävää tietoa heidän oikeuksistaan ja saatavilla olevista oikeussuojakeinoista.[264] *Henkilöstöä koskevien tietojen* osalta työryhmä huomautti erilaisista tulkinnoista työntekijää koskevien henkilötietojen käsitteen soveltamisessa ja vaati komissiota aloittamaan toimet tilanteen korjaamiseksi. Puutteita huomattiin myös muun muassa *periaatteiden noudattamista koskevassa valvonnassa*.[265]

Tietosuojatyöryhmä arvioi rajoituksia, jotka koskivat Yhdysvaltain viranomaisten pääsyä unionista siirrettyihin henkilötietoihin. Se huomautti, että Yhdysvallat on tehnyt useita toimenpiteitä, jotka edesauttavat läpinäkyvyyden toteutumista sen suorittamassa valvonnassa, mutta toi myös esiin seikkoja, joiden osalta Privacy Shield-järjestelyn vaatimukset eivät täyty. Erityistä huolta työryhmä esitti siitä, ettei Yhdysvallat ole esittänyt todisteita tai oikeudellisesti sitovia velvoitteita tukeakseen väitettään siitä, ettei FISA-lain 702 pykälän mukainen tietojen kerääminen ole valikoimatonta.[266]

Oli käynyt myös ilmi, ettei yksityinen henkilö voinut nostaa kannetta PPD-28:n säännösten rikkomisesta. Tämän seurauksena unionin jäsenvaltion kansalaisen ainoa keino saada varmistus siitä, että Yhdysvaltojen viranomaiset ovat käsitelleet hänen henkilötietojaan vaatimusten mukaisesti, on pyytää oikeusasiamiestä selvittämään asia. Työryhmä katsoi, että pysyvä oikeusasiamies tulisikin nimittää virkaansa mahdollisimman nopeasti. Työryhmä totesi lisäksi, että oikeusasiamiehen valtuudet eivät tällä hetkellä ole sellaiset, joiden kautta se voisi tehokkaasti hoitaa velvollisuuksiaan. Arvioinnin yhteydessä oli myös todettu, ettei oikeusasiamiehen päätöksistä ole mahdollista valittaa.[267]

[264] Article 29 Data Protection Working Party. 17/EN WP 255. EU – U.S. Privacy Shield – First annual Joint Review, s. 7-9.
[265] WP29 (17/EN WP 255), s. 9-11.
[266] WP29 (17/EN WP 255), s. 14-16.
[267] WP29 (17/EN WP 255), s. 18-19.

Arviointinsa lopputuloksena tietosuojatyöryhmä vaati komissiota ja Yhdysvaltain viranomaisia aloittamaan uudet neuvottelut, jotta Privacy Shield-järjestelyssä havaitut puutteet voidaan korjata. Työryhmä totesi odottavansa, että keskeisimmät ongelmat, kuten oikeusasiamiehen viran täyttämättömyys on ratkaistu 25.5.2018 mennessä. Tuona päivänä uusi tietosuoja-asetus tulee voimaan. Muut puutteet tulisi korjata toiseen vuosiarviointiin mennessä. Mikäli parannuksia ei ole tehty, tietosuojatyöryhmä alkaa toimiin saattaakseen Privacy Shield-päätöksen Euroopan unionin tuomioistuimen tarkasteltavaksi.[268]

8.5. Privacy Shield ja EU:n uusi tietosuoja-asetus

Euroopan unionin uusi tietosuoja-asetus[269] tulee sovellettavaksi toukokuussa 2018. Asetuksen 1 artiklan 2 kohdan mukaan asetuksella suojellaan luonnollisten henkilöiden perusoikeuksia ja -vapauksia ja erityisesti heidän oikeuttaan henkilötietojen suojaan. 2 artiklan 1 kohdassa määrätään asetuksen soveltamisalasta ja sen mukaan asetusta sovelletaan henkilötietojen käsittelyyn, joka on osittain tai kokonaan automaattista, sekä sellaisten henkilötietojen käsittelyyn muussa kuin automaattisessa muodossa, jotka muodostavat rekisterin osan tai joiden on tarkoitus muodostaa rekisterin osa.

Tietosuoja-asetuksen 3 artikla määrittää asetuksen alueellista soveltamisalaa ja vahvistaa asetuksen Euroopan unionin ulkopuolelle ulottuvat vaikutukset. 3 artiklan 1 kohdan mukaan asetusta sovelletaan henkilötietojen käsittelyyn, jota suoritetaan unionin alueella sijaitsevassa rekisterinpitäjän tai henkilötietojen käsittelijän toimipaikassa toiminnan yhteydessä, riippumatta siitä, suoritetaanko käsittely unionin alueella vai ei. Saman artiklan 2 kohdan mukaan asetusta sovelletaan unionissa olevia rekisteröityjä koskevien henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä tai henkilötietojen käsittelijä ei ole sijoittautunut unioniin, jos käsittely liittyy a) tavaroiden tai palvelujen tarjoamiseen näille rekisteröidyille unionissa riippumatta siitä, edellytetäänkö rekisteröidyltä maksua tai b) näiden rekisteröityjen

[268] WP29 (17/EN WP 255), s. 20.

[269] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus).

käyttäytymisen seurantaan siltä osin kuin heidän käyttäytymisensä tapahtuu unionissa. 3 kohdan mukaan asetusta sovelletaan henkilötietojen käsittelyyn, jota suorittava rekisterinpitäjä ei ole sijoittautunut unioniin vaan toimii paikassa, jossa sovelletaan jonkin jäsenvaltion lakia kansainvälisen julkisoikeuden nojalla.

3 artiklan 2 kohta tarkoittaa sitä, että mikäli yhdysvaltalainen yritys, esimerkiksi LinkedIn, tarjoaa palvelujaan unionin alueella oleville käyttäjille, tietosuoja-asetusta sovelletaan unionin alueelta siirrettyjen henkilötietojen käsittelyyn ja tällöin käsittelyn on vastattava asetuksen vaatimuksia. Tietosuosuoja-asetuksessa todetaan, että henkilötietojen rajat ylittävien siirtojen lisääntyminen on tuonut uusia henkilötietojen suojaan liittyviä haasteita. Tietojen siirtäminen ei saisi vaarantaa henkilötietojen suojan tasoa, joka unionissa perustuu tietosuoja-asetukseen ja se voidaan toteuttaa ainoastaan asetusta kaikilta osin noudattaen.[270]

Tietosuoja-asetuksen V luku säätelee henkilötietojen siirtoa kolmansiin maihin tai kansainvälisille järjestöille. 45 artiklan 1 kohdan mukaan henkilötietojen siirto johonkin kolmanteen maahan tai kansainväliselle järjestölle voidaan toteuttaa, jos komissio on päättänyt, että kyseinen kolmas maa tai kolmannen maan alue tai yksi tai useampi tietty sektori tai kyseinen kansainvälinen järjestö varmistaa riittävän tietosuojan tason. Tällaiselle siirrolle ei tarvita erityistä lupaa. Saman artiklan 2 a kohdan mukaan komission on tietosuojan riittävyyttä arvioidessaan otettava huomioon muun muassa ihmisoikeuksien ja perusvapauksien kunnioitus sekä lainsäädäntö, joka koskee muun muassa kansallista turvallisuutta ja viranomaisten pääsyä henkilötietoihin.

45 artiklan 4 kohdan mukaan komissio seuraa jatkuvasti kolmansissa maissa ja kansainvälisissä järjestöissä tapahtuvaa kehitystä, joka saattaa vaikuttaa direktiivin 95/46/EY 25 artiklan 6 kohdan perusteella hyväksyttyjen päätösten toimivuuteen. Saman artiklan 9 kohdan mukaan komission direktiivin 95/46/EY 25 artiklan 6 kohdan nojalla antamat päätökset pysyvät

[270] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, kohta 101.

voimassa, kunnes niitä muutetaan, ne korvataan tai kumotaan tämän artiklan 3 tai 5 kohdan mukaisesti annetulla komission päätöksellä.

Privacy Shield-päätöksessä ei ole toteamusta siitä, millainen on päätöksen ja GDPR:n välinen suhde, vaikka asetuksen voimaantulo oli tiedossa järjestelystä neuvoteltaessa. Siinä on kuitenkin todettu, että koska tietosuojan tason riittävyyden toteamiseen voi vaikuttaa myös unionin oikeuden kehitys, komissio arvioi Privacy Shield -järjestelyn tarjoaman suojan tasoa yleisen tietosuoja-asetuksen soveltamisen alkamisen jälkeen.[271] Asetuksen 45 artiklan 4 ja 9 kohtien valossa näyttääkin siltä, että Privacy Shield-järjestely voi olla voimassa sellaisenaan, mutta sen tehokkuutta tulee seurata säännöllisesti.

Tietosuoja-asetus säätelee henkilötietojen siirtoa kattavammin kuin henkilötietodirektiivin ja sisältää tarkempia vaatimuksia muun muassa siitä, minkä perusteella komissio arvioi tietosuojan tason riittävyyttä kolmannen maan osalta. Huomioon on asetuksen mukaisesti otettava myös esimerkiksi oikeusvaltioperiaate, tietosuojaa koskevat säännöt sekä se, onko kyseisessä maassa vähintään yksi tehokkaasti toimiva riippumaton valvontaviranomainen, joka vastaa tietosuojasääntöjen noudattamisen varmistamisesta ja täytäntöönpanosta (45 artiklan 2 kohta).

Jokaisella valvontaviranomaisella on asetuksen 58 artiklan 2 j-kohdan mukaan valtuus määrätä tiedonsiirtojen keskeyttämisestä kolmannessa maassa olevalle vastaanottajalle tai kansainväliselle järjestölle. Kyseisen valtuuden myöntäminen mukailee EUT:n Schrems-tuomiossaan tekemää päätelmää, että Safe Harbor-päätöksen 3 artiklan 1 kohdassa oli suljettu pois viranomaisten mahdollisuus toteuttaa tiedonsiirron keskeytystoimenpiteitä henkilötietodirektiivin 25 artiklan noudattamisen varmistamiseksi.[272] Tietosuoja-asetuksessa valtuus on selkeästi vahvistettu.

Kuner on nähnyt toisaalta ongelmallisena sen, että asetus antaa jäsenvaltioiden tietosuojaviranomaisille vallan keskeyttää tietojen siirto kolmansiin maihin, sillä se saattaa saada aikaan erilaisia näkemyksiä kolmansien maiden tietosuojan tasosta tietosuojaviranomaisten ja

[271] Täytäntöönpanopäätös (EU) 2016/1250, kohta 146.
[272] Tuomio asiassa C-362/14, kohta 101.

jäsenvaltioiden kansallisten tuomioistuinten välillä. Tällaiset toimet heikentävät tietosuojan riittävyyttä koskevien päätösten tarkoitusta, koska ne voivat joutua toisistaan poikkeavien kansallisten tulkintojen ja arviointien alaisiksi.[273]

Tietosuoja-asetuksessa on vahvasti painotettu jäsenvaltioiden tietosuojaviranomaisten keskinäistä yhteistyötä ja todettu, että valvontaviranomaisten tulisi seurata asetuksen säännösten soveltamista ja edistettävä sen yhdenmukaista soveltamista koko unionissa. Lisäksi olisi perustettava yhdenmukaisuusmekanismi valvontaviranomaisten keskinäistä yhteistyötä varten, jotta voidaan varmistaa asetuksen johdonmukainen soveltaminen kaikkialla unionissa. Mekanismia olisi sovellettava erityisesti silloin, kun viranomainen aikoo hyväksyä oikeusvaikutuksia tuottavan toimenpiteen sellaisiin käsittelytoimiin liittyen, jotka vaikuttavat olennaisella tavalla merkittävään määrään useissa eri jäsenvaltioissa olevia rekisteröityjä.[274] Asetuksen VII luku sisältää säännöksiä koskien yhteistyötä ja yhdenmukaisuutta ja siinä säädetään muun muassa keskinäisestä avunannosta, tietojen vaihdosta ja yhdenmukaisuusmekanismista.

Kuner huomauttaa, että koska asetus sekä antaa jokaiselle valvontaviranomaiselle valtuudet tietojen siirron keskeyttämiseen, että asettaa kansallisille tietosuojaviranomaisille vaatimuksia yhtenäisen näkemyksen löytämiseksi tietosuojan tason riittävyyttä koskien, viranomaiset joutuvat tasapainoilemaan toisaalta itsenäisten valtuuksien toteuttamisen ja toisaalta yhtenäisten tulkintojen löytämisen välillä.[275]

Kokonaisuudessaan tietosuoja-asetus on sääntelyltään huomattavasti tarkempi ja tiukempi kuin henkilötietodirektiivi, jonka säännösten nojalla Privacy Shield-päätös on hyväksytty. Lisäksi Euroopan unionin tuomioistuin vaati Schrems-tuomiossa, että sen kolmannen maan, johon henkilötietoja siirretään, tulee tarjota sellainen suojan taso, joka *pääosin vastaa* unionin suojan tasoa.[276] Koska unionin takaama henkilötietojen suojan taso on tietosuoja-asetuksen myötä korkeampi kuin aiemmin, jo olemassa olevien

[273] Ks. Kuner 2017, s. 895.
[274] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, kohdat 123 ja 135.
[275] Ks. Kuner 2017, s. 895.
[276] Tuomio asiassa C-362/14, kohdat 73, 74 ja 96.

päätösten, kuten Privacy Shieldin, osalta arvioitavaksi voi tulla se, takaavatko ne pääosin unionin henkilötietojen suojan tasoa vastaavan tason. On arvioitu, että Privacy Shield-päätöstä saatetaan joutua muuttamaan, jotta se täyttäisi tietosuoja-asetuksen vaatimukset.[277]

[277] Kuner 2017, s. 903.

9 SÄÄNTELYN TULEVAISUUS JA JOHTOPÄÄTÖKSET

9.1. Sääntelyn tulevaisuuden näkymiä

Lähitulevaisuudessa Privacy Shield-järjestelyn toimivuuteen ja Yhdysvaltoihin suuntautuvaan henkilötietojen siirtoa koskevaan sääntelyyn yleensäkin vaikuttaa merkittävästi se, mitkä ovat sovellettavaksi tulevan tietosuoja-asetuksen vaikutukset järjestelyn kelpoisuudelle. Kuten edellisessä luvussa todettiin, asetuksen lähtökohta on, että henkilötietodirektiivin nojalla tehdyt päätökset pysyvät voimassa. Komissio on joka tapauksessa todennut arvioivansa järjestelyn tarjoamaa tietosuojan tasoa sen jälkeen, kun asetusta on alettu soveltaa.[278]

Tietosuoja-asetuksen vaatimukset henkilötietojen suojalle ja niiden siirrolle ovat tiukemmat kuin henkilötietodirektiivin. Tietosuoja-asetuksen säännösten lisäksi huomioon tulee ottaa unionin tuomioistuimen vaatimus siitä, että kolmannen maan tulee tarjota suojan taso, joka *pääosin vastaa* unionin suojan tasoa. Koska järjestelyn kelpoisuus on haastettu jo ennen, kuin tietosuoja-asetus on tullut sovellettavaksi, lienee perusteltua päätellä, että Privacy Shield asetetaan perusteellisen arvioinnin alaiseksi viimeistään asetuksen sovellettavaksi tulemisen myötä.[279]

Henkilötietojen suojaa koskeva, kenties olennaisin viime vuosien suuntaus on ollut perusoikeusmyönteisyys. Tämä on näkynyt ensinnäkin Euroopan unionin tuomioistuimen oikeuskäytännössä, joka on pian sen jälkeen, kun unionin perusoikeuskirjasta tuli oikeudellisesti sitova, alkanut säännöllisesti vedota perusoikeuksiin ja perustaa tuomioitaan niiden mukaisesti. Schrems-tapaus on ollut tästä kehityksestä merkittävää näkyvyyttä saanut esimerkki. Kuner pitää tuomiota merkkipaaluna, joka on vahvistanut henkilötietojen suojan perusoikeusasemaa Euroopan unionin oikeudessa.[280]

Perusoikeusmyönteisyyden voi arvioida näkyvän myös yleisemmin unionin tietosuojalainsäädännössä, sillä tietosuojalainsäädännön uudistus

[278] Täytäntöönpanopäätös 2016/1250, kohta 146.
[279] Privacy Shield-päätöksen kelpoisuus on Euroopan unionin tuomioistuimen käsiteltävänä tapauksissa T-670/16 ja T-738/16.
[280] Kuner 2017, s. 884.

kokonaisuudessaan vahvistaa yksityishenkilöiden henkilötietojen suojaa sekä yleisesti, että yksittäisillä aloilla muun muassa tietosuojadirektiivin muodossa. Sillä, että tietosuoja-asetus on nimenomaan asetus ja unionin lainsäädännön hierarkiassa korkeampi kuin direktiivi, on henkilötietojen suojaa vahvistava ja unionin ja sen jäsenvaltioiden käytäntöjä ja tulkintoja yhtenäistävä vaikutus.

Yhdysvallat on Edward Snowdenin vuonna 2013 alkaneiden massavalvontapaljastusten myötä joutunut tekemään sekä yhdysvaltalaisten että ei-yhdysvaltalaisten ihmisten henkilötietojen suojaa vahvistavia toimia. Myös Atlantin toisella puolella lainsäädännöllisiä uudistuksia ovat viime aikoina heijastelleet vaatimukset korkeammasta tietosuojan tasosta ja tietojen suojaamisesta siten, ettei Yhdysvaltain viranomaiset pääse käsiksi tietoihin enempää, kuin on lainmukaista. Vuonna 2015 hyväksyttyä USA Freedom Act-lakia voidaan pitää esimerkkinä tarkemmin säädellyn tietosuojan tason kehityksestä.

Maailmanlaajuisesti on osoittautunut haasteelliseksi luoda sellaisia henkilötietojen suojaa ja erityisesti niiden siirtoa koskevia sääntelyitä, joilla olisi globaali tai ainakin laaja kansainvälinen vaikutus. Laajempaa kansainvälistä yhtenäisyyttä on saavutettu tietosuojaperiaatteita koskevilla suosituksilla, kuten OECD:n tietosuojasuosituksilla, mutta suositukset eivät ole oikeudellisesti sitovia. Tietosuojasääntelyn määrä, kattavuus ja sitovuus on maailmanlaajuisesti niin vaihtelevaa, että yhtenäisten ja sitovien tietosuojasääntöjen aikaansaaminen ainakaan lähitulevaisuudessa vaikuttaa epätodennäköiseltä.[281] Mahdollisena on nähty myös, että vastareaktiona tietojen siirron globalisoitumiselle valtiot saattavat haluta korostaa itsenäisiä intressejään tietojen käsittelyn ja rajat ylittävien tietojensiirron sääntelyssä.[282] Rajat ylittävän tietojensiirron määrä tuskin on vähenemässä, joten yhtenäiseen kansainväliseen sääntelyyn kannattaa joka tapauksessa pyrkiä.

[281] Erilaisista tietosuojasääntelyistä ks. Bygrave 2014, s. 99-116.
[282] Kuner 2013, s. 31.

9.2. Johtopäätökset

Tutkielman tavoitteena on ollut selvittää, kuinka henkilötietojen sääntely transatlanttisissa henkilötietojen siirroissa on kehittynyt ja kuinka kattavasti voimassa oleva Privacy Shield-järjestely suojaa unionista siirrettäviä henkilötietoja. Privacy Shieldin voi todeta kohentavan yksityishenkilöiden oikeuksia, määräävän tiukempia vaatimuksia yhdysvaltalaisille yrityksille ja rajoittavan Yhdysvaltain viranomaisten pääsyä järjestelyn kautta siirrettyihin henkilötietoihin. Kansainvälisen kaupan kehittäminen ja sen myötä syntyvien valtavien tietovirtojen liikkumisen turvaaminen on niin Yhdysvalloille kuin unionillekin olennaisen tärkeää.

Koko henkilötietojen siirtoa unionista Yhdysvaltoihin koskevan sääntelyn voi todeta olleen monilta osin puutteellista. Privacy Shieldin avulla Safe Harborin puutteita on pyritty korjaamaan, mutta edelleen on epäselvää, voiko se todellisuudessa ja pitkäaikaisesti täyttää Euroopan unionin lainsäädännön vaatimukset henkilötietojen suojalle tietoja Yhdysvaltoihin siirrettäessä. Toisaalta on haasteellista kuvitella, minkälainen muu, tuhansia sitoutuneita yrityksiä käsittävä ja tarkat periaatteet sisältävä järjestely voisi toimia Privacy Shieldin korvaajana. Mikäli Privacy Shield tulee kumotuksi, edessä on jälleen uusi transatlanttinen kiista siitä, miten tietojen siirto tulisi tehokkaasti ja turvallisesti järjestää. Yksi mahdollinen kehityssuunta on se, että Yhdysvallat tiukentaa tietosuojasääntelyään huomattavasti ja rajoittaa tehokkaasti viranomaisten pääsyä unionista siirrettyihin henkilötietoihin.

Mielenkiintoisen ristiriidan aiheuttaa se, että samalla, kun henkilötietojen siirron tärkeys tunnustetaan kansainvälisen kaupan ja yhteistyön kehittämiseksi, se edelleen on lähtökohtaisesti kiellettyä kolmansiin maihin suuntautuvana.[283] Henkilötietojen siirron lähtökohtainen kielto ilmenee tietosuoja-asetuksen 44 artiklassa, jonka mukaisesti henkilötietojen siirto toteutetaan vain, jos rekisterinpitäjä ja henkilötietojen käsittelijä noudattavat asetuksen V luvussa vahvistettuja edellytyksiä ja ellei asetuksen muista säännöksistä muuta johdu. Siirto ei siten lähtökohtaisesti ole sallittua, kuten esimerkiksi unionin jäsenvaltioiden välillä vapaan liikkuvuuden periaatteen mukaisesti. Kieltoa ei kuitenkaan todellisuudessa voi määritellä ristiriidaksi,

[283] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, kohta 101 ja artikla 44.

sillä henkilötietojen suojan turvaaminen ja kansainvälisen kaupan kehittäminen eivät ole toisiaan pois sulkevia seikkoja, vaan ne molemmat on kyettävä turvaamaan ja niiden välille on löydyttävä sääntelyn tasapaino.

Samalla kun henkilötietojen siirtoa unionista Yhdysvaltoihin koskevan sääntelyn voi todeta olleen puutteellista, se on ollut myös erittäin kiistanalaista. Unionin tiettyjen elinten välillä on lähes parinkymmenen vuoden ajan vallinnut erimielisyys henkilötietojen siirtoa Yhdysvaltoihin koskevien komission päätösten, eli Safe Harborin ja Privacy Shieldin osalta. Parlamentti vastusti Safe Harborin hyväksymistä vuonna 2000 ja huhtikuussa 2017 antamassaan päätöslauselmassa se piti valitettavana, että Euroopan komissio järjesti Privacy Shield-päätöksen hyväksyntämenettelyn käytännössä siten, ettei parlamentti ole voinut tosiasiallisesti käyttää oikeuttaa täytäntöönpanosäädösluonnoksen valvontaan.[284] Järjestelyn tehokkuus on selkeästi kyseenalaistettu sekä WP29-tietosuojatyöryhmän että Euroopan parlamentin toimesta.[285]

Privacy Shield-järjestelyn ongelma ei ole ainoastaan se, että unionilla ja Yhdysvalloilla on perusteiltaan erilaiset lähtökohdat yksityisyyden ja henkilötietojen suojasta sääntelyn osalta. Perustavanlaatuisen ongelman aiheuttaa se, että Euroopan unionin sisällä Privacy Shieldin pätevyydestä ja tehokkuudesta ei ole olemassa yksimielisyyttä. Jotta Privacy Shield voisi toimia tehokkaasti ja pitkäaikaisesti, se ei vaadi toimenpiteitä ainoastaan Yhdysvalloilta. Myös Euroopan unionin elinten kesken on päästävä yhteisymmärrykseen järjestelyn toimivuudesta, koska unionin yhteinen ja keskeinen tavoite on sekä henkilötietojen suojan korkean tason turvaaminen, että kansainvälisen kaupan edellytysten ylläpitäminen.

Selvää on, että mikäli järjestely todella on tehoton, eikä esimerkiksi rajoita Yhdysvaltojen viranomaisten pääsyä henkilötietoihin siten, että unionin alueella olevien henkilöiden henkilötiedot voidaan suojata tietosuoja-asetuksen ja henkilötietojen perusoikeusaseman vaatimalla tavalla, järjestely on kumottava. Huomioitava on toisaalta myös se, että mikäli järjestelyn tehokkuutta halutaan pätevästi arvioida, sen toimivuudesta on saatava

[284] Heisenberg 2005, s. 8. Parlamentin päätöslauselma (2016/3018(RSP), kohta 30.
[285] WP29 (17/EN WP 255), Parlamentin päätöslauselma (2016/3018(RSP).

käytännön kokemuksia pidemmältä ajalta. Joka tapauksessa etusijalle on asetettava henkilötietojen suojan korkean tason turvaaminen ja järjestelyä tulee arvioida ensisijaisesti sen perusteella.

Koska järjestelyn tilanne on epävakaa, se voi estää yhdysvaltalaisten yritysten halukkuutta sitoutua järjestelyyn, sillä ne eivät voi olla varmoja järjestelyn pitävyydestä. Yritysten osalta tilanne on ymmärrettävä, sillä tiettyjen tietosuojakäytäntöjen luominen ja niihin mukautuminen vie aikaa ja tuottaa kustannuksia. Jos yritys ei voi luottaa siihen, että sen valitsema tietojen siirron menetelmä on pitävä, se saattaa jo lähtökohtaisesti hylätä Privacy Shield-järjestelyn ja päättää toteuttaa henkilötietojen siirto muun tietosuoja-asetuksen tarjoaman menetelmän kautta.

Unionin rooli kansainvälisessä tietosuojaa koskevassa keskustelussa on ollut merkittävä.[286] Myös tietosuojalainsäädännön kehittämisessä se on ollut kiistaton edelläkävijä, reagoinut teknologian kehityksen synnyttämiin lainsäädäntöhaasteisiin verrattain nopeasti ja samalla teknologian kehityksen rinnalla kehittänyt unionille kattavan tietosuojalainsäädäntöverkoston, jolla on maailmanlaajuisia vaikutuksia. Euroopan unioni ei kuitenkaan kykene vaikuttamaan kaikkeen, sillä kattavasta sääntelystä huolimatta Yhdysvaltojen tietosuojakäytännöillä on todellisuudessa suurempi vaikutus tietoverkkojen tietosuojan tasoon. Internetin käytön keskiössä ovat valtavat yhdysvaltalaisyritykset, kuten Google ja Facebook, joiden perusta on Yhdysvaltain lainsäädännössä.[287]

Yhdysvallat on tehnyt selkeitä toimia unionista siirrettävien henkilötietojen suojan turvaamiseksi muun muassa oman, kansallisen lainsäädäntönsä ja Privacy Shield-järjestelyssä perustettujen uusien oikeussuojamekanismien muodossa. Yhdysvaltojen Privacy Shield-päätöksessä antamien sitoumusten ja vakuutusten oikeudellinen sitovuus on kuitenkin epävarmaa, eikä Yhdysvaltojen sisäisen poliittisen tilanteen vuoden 2017 alussa uudistuneen hallinnon myötä voi todeta olevan lainsäädännön pysyvyyden kannalta vakaa. Yhdysvaltain presidentti Trump on ilmoittanut aikovansa kumota kaikki edeltäjänsä, presidentti Obaman toimeenpanemat määräykset.[288] Tällainen

[286] Ks. Schwartz 2013, s. 1968.
[287] Ks. Bygrave 2014, s. 107.
[288] Kuner 2017, s. 903.

määräys on esimerkiksi PPD-28, jolla on merkittäviä vaikutuksia Privacy Shield-järjestelyn mukaisen henkilötietojen suojan toteuttamisessa.

Tietosuoja-asiat ovat tällä hetkellä maailmanlaajuisesti ajankohtaisia niin uudistuvan, kansainvälisesti vaikuttavan EU-lainsäädännön kuin jälleen uusien henkilötietojen suojan rikkomista koskevien paljastusten myötä. Maaliskuussa 2018 alkanut, Facebookia koskeva Cambridge Analytica-kohu on saanut aikaan valtavan liikehdinnän ja toimenpiteitä niin Yhdysvalloissa kuin Euroopan unionissa yksityisten ihmisten henkilötietojen suojan paremman turvaamisen takaamiseksi. Kohun keskiössä on paljastus, jonka mukaan Facebook-sovellus oli kerännyt jopa 50 miljoonan Yhdysvaltojen kansalaisen tietoja, joita on käytetty äänestäjien profiloimiseksi. Profiloinnin tarkoituksena oli ollut, että Donald Trumpin vaalikampanja voisi suorittaa täsmällisemmin kohdennettua mainontaa.[289]

Vaikuttaa siltä, että Cambridge Analytica-kohun myötä sekä Yhdysvalloissa että unionissa on saatu tarpeeksi suurten verkossa toimivien yritysten, pääasiallisesti Facebookin, heikosta henkilötietojen suojan tasosta. Yhdysvaltojen liittovaltion kauppakomissio FTC on Cambridge Analytica-kohun seurauksena alkanut tutkia Facebookia.[290] Artiklan 29 mukainen tietosuojatyöryhmä on ilmoittanut perustavansa erillisen sosiaalisen median tietosuojatyöryhmän ja todennut tietojen suojaamisessa alkavan uuden aikakauden.[291] Tähän asti yhdysvaltalaiset yritykset, kuten Facebook, ovat ajautuneet EU-lainsäädännön johdosta konfliktiin Euroopan unionin tietosuojaviranomaisten kanssa.[292] Nyt käynnissä on tilanne, jossa myös Yhdysvaltojen viranomaiset ovat havahtuneet yritysten tietosuojan tason riittämättömyyteen. On erityisen mielenkiintoista nähdä, onko Cambridge Analytica-kohulla tiukentavia ja rajoittavampia vaikutuksia Yhdysvaltain lainsäädäntöön.

Yhdysvallat hyväksyi tammikuussa 2018 FISA-lain uudistuksen ilman merkittäviä muutoksia. Laki, joka muun muassa sallii ulkomaantiedustelutiedon hankkimisen kohdistamalla tiedustelun

[289] https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html
[290] http://www.bbc.com/news/world-us-canada-43476594
[291] https://edps.europa.eu/sites/edp/files/publication/18-04-11_wp29_press_release_en.pdf
[292] Bygrave 2014, s. 208.

Yhdysvaltojen ulkopuolella olevaan, ei-yhdysvaltalaiseen henkilöön, on ollut uudistusvaatimusten alaisena Edward Snowdenin massavalvontapaljastuksista lähtien. Tietosuoja-alan vahtikoirajärjestö Electronic Privacy Information Center (EPIC) totesi, että hyväksymällä lain ilman suurempia muutoksia Yhdysvallat vaaransi suhteensa Euroopan unioniin.[293]

Privacy Shield-järjestelyn vaiheita on niin Euroopassa kuin Yhdysvalloissa seurattava tarkoin, sillä kritiikistä huolimatta se on edelleen voimassa oleva järjestely, jonka nojalla 2869 yhdysvaltalaista yritystä käsittelee unionista siirrettyjä henkilötietoja.[294] Seuraavia merkittäviä vaiheita ovat järjestelyn tila unionin tietosuoja-asetuksen sovellettavaksi tullessa, Privacy Shieldin toinen vuosiraportti sekä Euroopan unionin tuomioistuimen ratkaisut järjestelyn riittävyydestä. Tuomioistuin ottanee sääntelyn kokonaisvaltaisen kelpoisuuden lisäksi kantaa myös muun muassa FISA-lain uudelleen hyväksynnän vaikutuksiin Privacy Shield-järjestelyn osalta.

Samalla, kun Euroopan unioni säätää yhä tiukempaa henkilötietojen suojaa koskevaa lainsäädäntöä, sen on oleellista huomioida, minkälaisia vaikutuksia sääntelyllä on globaaliin, digitaaliseen maailmaan. Mikäli unionin rajat ylittävä sääntely on niin tiukkaa, että se heikentää taloudellisten suhteiden edellytyksiä unionin ulkopuolisten valtioiden kanssa, sen on voitava suhteuttaa sääntelyvaatimukset siten, että unionin talous ei kärsi. Unionin on lisäksi pohdittava avoimemmin ja laajemmin sitä, että mikäli Privacy Shield kumotaan, millä tavalla se aikoo järjestää henkilötietojen siirron tulevaisuudessa siten, että sääntely olisi selkeää, kaikkien osapuolten intressit huomioon ottavaa, Euroopan unionin tietosuojaperusoikeudet turvaavaa ja mahdollisimman suurta yhdysvaltalaista yritysjoukkoa palvelevaa.

[293] https://epic.org/2018/01/congress-renews-controversial-.html
[294] https://www.privacyshield.gov/list Privacy Shield-listassa oli 25.4.2018 2869 aktiivista yhdysvaltalaista yritystä.