REKISTERINPITÄJÄN ASIANMUKAISET TEKNISET JA ORGANISATORISET TOIMENPITEET OSANA SISÄÄNRAKENNETTUA JA OLETUSARVOISTA TIETOSUOJAA

Maisteritutkielma

Ville Heikkinen

Oikeusinformatiikka

Oikeustieteiden tiedekunta

Lapin yliopisto

2021

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Rekisterinpitäjän asianmukaiset tekniset ja organisatoriset toimenpiteet osana sisäänrakennettua ja oletusarvoista tietosuojaa.

Tekijä: Ville Heikkinen

Opetuskokonaisuus ja oppiaine: Oikeusinformatiikka

Työn laji: Maisteritutkielma

Sivumäärä: XVI + 92

Vuosi: 2021

Tiivistelmä

Sisäänrakennetulla ja oletusarvoisella tietosuojalla tarkoitetaan käytännössä uudenlaisen ajattelumallin ottamista käyttöön henkilötietoja käsiteltäessä. Kyse on siitä, että tietosuojasuunnittelu upotetaan mahdollisimman varhaisessa vaiheessa osaksi organisaation käytänteitä ja prosesseja. Samalla tulisi pitää kaikessa organisaation toiminnassa huolta siitä, että henkilötietojen suoja otetaan esille ennen muihin toimenpiteisiin ryhtymistä. Asianmukaisilla teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan sellaisia toimenpiteitä, joilla sisäänrakennettua ja oletusarvoista tietosuojaa voidaan käytännössä toteuttaa. Ei ole kuitenkaan olemassa mitään tyhjentävää luetteloa kaikista mahdollisista toimenpiteistä. Jokaisessa kontekstissa vaikuttavat erilaiset tarpeet, mihin myös vaatimus asianmukaisuudesta viittaa. Suurin osa näistä toimenpiteistä liittyy tietoturvallisuuden varmistamiseen, mutta toisaalta osassa kyse on yleisistä organisaation sisäisesti toteutettavista keinoista.

Taustalla on ajatus siitä, että jokaisen henkilötietoja käsittelevän organisaation tulee omassa toiminnassaan ottaa henkilötietojen suoja huomioon uudella tavalla. Huomiota on syytä kiinnittää siihen, että kaikissa toimenpiteissä, jotka kohdistuvat henkilötietoihin, tulee huolehtia henkilötietojen suojan toteutumisesta ennen käsittelytoimiin ryhtymistä. Tutkielmassa luon katsauksen siihen, miten vaatimuksen sisältöä tulee tulkita ja miten rekisterinpitäjä voi täyttää velvollisuutensa. Tässä tulee huomata, että yleistä tietosuoja-asetusta tulee käsitellä kokonaisvaltaisesti eikä vain pyrkiä tulkitsemaan yhtä artiklaa.

Yleisen tietosuoja-asetuksen myötä rekisterinpitäjille syntyi uudenlainen velvollisuus huolehtia siitä, että yksilöiden henkilötietoja käsitellään perus- ja ihmisoikeuksia kunnioittavasti. Seurauksena laiminlyönneistä on hallinnollinen seuraamusmaksu. Ongelmallista on kuitenkin ollut se, että yleinen tietosuoja-asetus sisältää paljon periaatesääntelyä, joka ei anna yksiselitteisiä vastauksia kaikkiin kysymyksiin. Tutkimuksella pyrin täyttämään aukkoa, joka on syntynyt liian monimutkaiselta vaikuttavasta periaatesääntelystä. Samalla haluan osoittaa, että tietoisuus oikein toteutetusta tietosuojatyöstä voi antaa organisaatiolle myös positiivisia vaikutuksia.

Avainsanat: oikeusinformatiikka, tietosuoja, GDPR, yleinen tietosuoja-asetus, rekisterinpitäjä, toimenpiteet, asianmukaisuus, sisäänrakennettu, oletusarvo

SISÄLLYS

LÄHDELUETTELO

Aarnio, A. (2011). *Luentoja lainopillisen tutkimuksen teoriasta.* Helsinki: Forum Iuris. Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

Alapuranen, L.; Lehtonen, L.; Koskinen, S.; & Wiberg, M. (2020). *Henkilötietojen käsittely työelämässä* (3. painos). Helsinki: Edita Publishing Oy.

Alexy, R. (2003). On Balancing and Subsumption: A Structural Comparison. *Ratio Juris*, 16(4), s. 433–449.

Andreasson, A.; & Koivisto, J. (2013). *Tietoturvaa toteuttamassa.* Helsinki: Tietosanoma.

Andreasson, A.; Riikonen, J.; & Ylipartanen, A. (2019). *Osaava tietosuojavastaava ja EU:n yleinen tietosuoja-asetus.* Tallinna: Tietosanoma Oy.

Brownsword, R. (2017). Law, Liberty, and Technology. Teoksessa R. Brownsword; E. Scotford; & K. Yeung (Toim.), *The Oxford Handbook of Law, Regulation, and Technology*, s. 41–68. Oxford: Oxford University Press.

Burkert, H. (2014). Information Law: From Discipline to Method. Teoksessa D. Wiese Schartum; L. A. Bygrave; & A. G. Berge Bekken (Toim.), *Jon Bing. En Hyllest / A Tribute,* s. 388–400. Gyldendal Latvia.

Bygrave, L. A. (2001). Core principles of data protection. *Privacy Law and Policy Reporter, 7*(9). Haettu 17. Maaliskuuta 2021 osoitteesta http://www.austlii.edu.au/cgi-bin/viewdoc/au/journals/PrivLawPRpr/2001/9.html.

Bygrave, L. A. (2002). *Data Protection Law - Approaching Its Logic and Limits.* Haag: Kluwer Law International.

Bygrave, L. A. (2014). *Data Privacy Law. An International Perspective.* Oxford: Oxford University Press.

Bygrave, L. A. (2017). Hardwiring Privacy. Teoksessa R. Brownsword; E. Scotford; & K. Yeung (Toim.), *The Oxford Handbook of the Law and Regulation of Technology*, s. 754-775. Oxford: Oxford University Press.

Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles.* Toronto: Information and Privacy Commissioner of Ontario.

Cocq, C. C. (2016). Encryption and anonymisation online : challenges for law enforcement authorities within the EU. Teoksessa T. Bräutigam; & S. Miettinen (Toim.), *Data protection, Privacy and European Regulation in the Digital Age*, s. 178–204. Helsinki: Unigrafia.

Cohen, J. E. (2008). Privacy, Visibility, Transparency, and Exposure. *The University of Chicago Law Review, 75*(1), s. 181–201.

De Hert, P. (2009). Data Protection in the Case Law of Strassbourg and Luxemburg: Constitutionalisation in Action. Teoksessa S. Gutwirth; Y. D. Poullet; & S. Nouwt (Toim.), *Reinventing Data Protection?*, s. 3–44. Dordrecht; London: Springer.

De Terwangne, C. (2021). Council of Europe convention 108+: A modernised international treaty for the protection of personal data. *Computer Law & Security Review*, vol. 40 (2021), s. 1–18.

Dienst, S. (2018). Lawful Processing of Personal Data in Companies under the General Data Protection Regulation. Teoksessa T. Kugler; & D. Rücker (Toim.), *New European General Data Protection Regulation - A Practitioner's Guide*, s. 49–103. Baden-Baden: Nomos Verlagsgesellschaft.

Edwards, L. (2019). *Law, Policy and the Internet.* Oxford: Hart Publishing.

Friedman, B. (1997). *Human Values and the Design of Computer Technology.* Cambridge: Cambridge University Press.

Gürses, S.; & van Hoboken, J. (2017). Privacy after the Agile Turn. Teoksessa E. Selinger; J. Polonetsky; & O. Tene (Toim.), *The Cambridge Handbook of Consumer Privacy*, s. 579–601. Cambridge: Cambridge University Press.

Hanninen, M.; Laine, E.; Rantala, K.; Rusi, M.; & Varhela, M. (2017). *Henkilötietojen käsittely - EU-tietosuoja-asetuksen vaatimukset.* Helsinki: Kauppakamari.

Hartzog, W. (2018). *Privacy's Blueprint: The Battle to Control the Design of New Technologies.* Lontoo: Harvard University Press.

Heino, I. (2016). *Yksityisyyden suoja ja luottamus liikkumisen sähköisissä palveluissa.* Espoo: Teknologian tutkimuskeskus VTT Oy.

Hirvonen, A. (2011). *Mitkä Metodit? Opas oikeustieteen metodologiaan.* Helsinki: Yleisen oikeustieteen julkaisuja 17.

IT Governance Privacy Team. (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* (2. painos). ITGP Privacy Team IT Governance Publishing.

Jay, R.; Malcolm, W.; Parry, E.; Townsend, L.; & Bapat, A. (2017). *Guide to the general data protection regulation : a companion to Data protection law and practice.* London: Sweet & Maxwell.

Jyränki, A. (2000). *Uusi perustuslakimme.* Jyväskylä: IuraNova.

Järvinen, P. (2012). *Arjen tietoturva: Vinkit ja ratkaisu.* Jyväskylä: Docendo.

Järvinen, P. (2018). *Kyberuhkia ja somesotaa: Digiaikana sinäkin olet etulinjassa.* Jyväskylä: Docendo.

Kangas, U. (1982). *Lesken oikeudellinen asema. Oikeusdogmaattinen tutkimus lesken sosiaaliturvan laajuudesta.* Vammala: Suomalaisen Lakimiesyhdistyksen julkaisuja. A-sarja nro 156.

Kangas, U. (1997). Minun metodini. Teoksessa J. Häyhä (Toim.), *Minun metodini*, s. 90–109. Porvoo: WSOY Lakitieto.

Karapuu, H. (1972). *Oikeus yksityiselämän suojaan.* Valtiosääntökomitea 21.4.1972.

Koillinen, M. (2013). Henkilötietojen suoja itsenäisenä perusoikeutena. *Oikeus 2/2013*, s. 171–193.

Konstari, T. (1992). *Henkilörekisterilaki: säännökset ja käytäntö.* Helsinki: Lakimiesliiton Kustannus.

Koops, B.; & Leenes, R. (2005). "Code" and the Slow Erosion of Privacy. *12 Michigan Telecommunications and Technology Law Review*, s. 115–188.

Korhonen, R. (2003). *Perusrekisterit ja henkilötietojen suoja : informaatio-oikeudellinen tutkimus yksityisyyden suojasta yhteiskunnan perusrekisteritietojen käsittelyssä.* Rovaniemi: Lapin yliopisto.

Korhonen, R. (2003). *Perusrekisterit ja tietosuoja.* Helsinki: Edita Publishing Oy.

Korhonen, V.; Koskinen, S.; Ojanen, M.; & Pesonen, P. (2004). *Työelämän uusi tietosuoja.* Helsinki: Edita.

Korja, J. (2016). *Biometrinen tunnistaminen ja henkilötietojen suoja : tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta.* Rovaniemi: Lapin yliopisto.

Korpisaari, P. (2016). Kirja-arvostelu teoksesta Korja, Juhani: Biometrinen tunnistaminen ja henkilötietojen suoja. Tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. *Lakimies 6/2016*, s. 991–1001.

Korpisaari, P.; Pitkänen, O.; & Warma-Lehtinen, E. (2018). Uusi tietosuojalainsäädäntö. Helsinki: Alma Talent.

Kremer, J. (2017). *The End of Freedom in Public Places? : Privacy Problems Arising from Surveillance of the European Public Space.* Helsinki: Helsingin yliopisto.

Lambert, P. (2017). *Understanding the New European Data Protection Rules.* Boca Raton: CRS Press.

Leiser, M.; & Murray, A. (2017). Governance of New and Emerging Digital Technologies. Teoksessa R. Brownsword; E. Scotford; & K. Yeung (Toim.), *The Oxford Handbook of Law, Regulation, and Technology*, s. 670–701. Oxford: Oxford University Press.

Lessig, L. (1999). *Code and Other Laws of Cyberspace* . New York: Basic Books.

Limnéll, J.; Majewski, K.; & Salminen, M. (2014). *Kyberturvallisuus.* Jyväskylä: Docendo.

Lohiniva-Kerkelä, M. (2003). *Verosalaisuus: Yksityisyyden ja luottamuksellisen liiketoimintatiedon suoja verotuksessa.* Rovaniemi: Lapin yliopisto.

Lynskey, O. (2015). *The Foundations of EU Data Protection Law.* Oxford: Oxford University Press.

Länsineva, P. (1998). Perusoikeudet - Nyt. Teoksessa P. Länsineva; & V.-P. Viljanen (Toim.), *Perusoikeuspuheenvuoroja*, s. 103–119. Turku: Turun yliopisto.

Mahkonen, S. (1997). *Oikeus yksityisyyteen.* Porvoo: Werner Söderström Lakitieto Oy.

Malin, B.; & Sweeney, L. (2000). Determining the Identifiabiity of DNA Database Entries. *In Proceedings of the American Medical Informatics Association Annual Symposium*, s. 537-541. United States: American Medical Informatics Association.

McDonald, A. M. (2015). When Self-help Helps: User Adoption of Privacy Technologies. Teoksessa M. Rotenberg; J. Horwitz; & J. Scott, *Privacy in the Modern Age: The Search for Solutions*, s. 127-137. New York: The New Press.

Melis, J. (2001). *History of encryption*, 2. Haettu 2. Maaliskuuta 2021 osoitteesta https://www.sans.org/reading-room/whitepapers/vpns/history-encryption-730.

Möller, C. (2016). Is EU law "fit to go digital": A consideration of the adequacy of the current legislative framework to meet data protection and data security challenges related to IND 4.0. Teoksessa T. Bräutigam; & S. Miettinen (Toim.), *Data Protection, Privacy and European Regulation in the Digital Age.* Helsinki: Unigrafia.

Neuvonen, R. (2014). *Yksityisyyden suoja Suomessa.* Helsinki: Lakimiesliiton Kustannus.

Neuvonen, R. (2019). *Viestintä- ja informaatio-oikeuden perusteet.* Kauppakamari.

Nissenbaum, H. (2015). "Respect for Context": Fulfilling the Promise of the White House Report. Teoksessa M. Rotenberg; J. Horwitz; & J. Scott (Toim.), *Privacy in the Modern Age: The Search for Solutions*, s. 152–164. New York: The New Press.

Norman, D. (1988). *The Design of Everyday Things.* New York: Basic Books.

Park, J. (2017). VPN: Privacy and Anonymity for All. *Georgetown Law Technology Review*, s. 129–136.

Pitkänen, O.; Tiilikka, P.; & Warma, E. (2013). *Henkilötietojen suoja.* Vantaa: Talentum Media Oy.

Pothos, M. (2018). Accountability requirements. Teoksessa E. Ustaran (Toim.), *European Data Protection Law and Practice*, s. 213–232. Portsmouth: International Association of Privacy Professionals.

Pyyhtiä, T. (2019). *Digiajan johtajan käsikirja : käytännönläheinen, helppolukuinen ja tiivis opas digiajan johtamiseen.* Helsinki: BoD - Books on Demand.

Pöysti, T. (1999). *Tehokkuus, informaatio ja eurooppalainen oikeusalue.* Helsinki: Helsingin yliopiston oikeustieteellisen tiedekunnan julkaisuja.

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

Pöysti, T. (2002). Verkkoyhteiskunnan viestintäinfrastruktuurin metaoikeudet. Teoksessa H. Kulla, *Viestintäoikeus,* s. 35–81. Helsinki: WSOY Lakitieto.

Raitio, J. (2016). *Euroopan unionin oikeus.* Helsinki: Talentum Pro.

Reidenberg, J. R. (1993). Rules of the Road for Global Electronic Highways: Mergin Trade and Technical Paradigms. *Harvard Journal of Law & Technology vol. 6*, s. 287–306.

Richards, N. M. (2015). Four Privacy Myths. Teoksessa A. Sarat (Toim.), *A World without Privacy: What Law Can and Should Do?*, s. 33–82. Cambridge: Cambridge University Press.

Romanou, A. (2017). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer Law & Security Review, 34*(1), s. 99–110.

Room, S. (2018). Security of Personal Data. Teoksessa E. Ustaran (Toim.), *European data protection : law and practice*, s. 169–212 (2. painos). Portsmouth: International Association of Privacy Professionals.

Rost, M.; & Pfitzmann, A. (2009). Datenschutz-Schutzziele-revisited. *Datenschutz und Datensicherheit, 33*(6), s. 353–358.

Rubinstein, I. S. (2011). Regulating Privacy by Design. *Berkeley Technology Law Journal, 26*(3), s. 1409–1456.

Rudgard, S. (2018). Origins and Historical Context of Data Protection Law. Teoksessa E. Ustaran (Toim.), *European Data Protection Law and Practice*, s. 3–22. Portsmouth: International Association of Privacy Professionals.

Råman, J. (2006). *Regulating Secure Software Development: Analysing the potential regulatory solutions for the lack of security in software.* Rovaniemi: Lapin yliopisto. (Råman 2006a)

Råman, J. (2006). Tietoturvallisuus on myös perusoikeus. *Lakimies 5/2006*, s. 818–824. (Råman 2006b)

Saarenpää, A. (1987). ATK ja yksilön suoja. Teoksessa *Oikeusinformatiikka*, s. 200–219. Rovaniemi: Pohjoismaisen oikeuden instituutin julkaisuja. Lakimiesliiton Kustannus.

Saarenpää, A. (1994). Tieto ja suoja. Teoksessa H. Lindroth; & T. Pöysti (Toim.), *Juhlajulkaisu: Oikeustieteen ylioppilaiden yhdistys Artikla ry 15 vuotta*, s. 153–185. Rovaniemi: Pandecta.

Saarenpää, A. (2000). Verkkoyhteiskunnan oikeutta - johdatusta aiheeseen. *Oikeus 1/2000*, 3–14.

Saarenpää, A. (2002). *Näkökohtia yksilön suojasta - 55 teesiä tietosuojasta.* (Saarenpää 2002a)

Saarenpää, A. (2002). Oikeusinformatiikka. Teoksessa R. Haavisto (Toim.), *Oikeusjärjestys 2000, osa I*, s. 1–59 (2. painos). Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 31. Lapin yliopistopaino. (Saarenpää 2002b)

Saarenpää, A. (2002). Yksityisyys, yksityiselämä ja yksilön suoja - yksityisyyden käsitteellistä kuvausta. Teoksessa R. Haavisto (Toim.), *Professori Kyösti Holman juhlakirja 11.6.2002*, s. 313–337. Rovaniemi: Lapin yliopisto. (Saarenpää 2002c)

Saarenpää, A. (2012). Henkilö- ja persoonallisuusoikeus. Teoksessa T. Tammilehto (Toim.), *Oikeusjärjestys. Osa 1*, s. 218–409 (8. painos). Rovaniemi: Lapin yliopiston oikeustieteellisiä julkaisuja. Sarja C 59.

Saarenpää, A. (2015). Henkilö- ja persoonallisuusoikeus. Teoksessa M.-L. Niemi (Toim.), *Oikeus tänään: Osa II*, s. 203–427. Rovaniemi: Lapin yliopisto.

Saarenpää, A. (2016). Oikeusinformatiikka. Teoksessa M.-L. Niemi (Toim.), *Oikeus tänään osa I*, s. 67–273. Rovaniemi: Lapin ylopiston oikeustieteellisiä julkaisuja. Sarja C 64.

Saraviita, I. (2005). *Suomalainen perusoikeusjärjestelmä.* Helsinki: Talentum.

Sartor, G. (2017). Human Rights and Information Technologies. Teoksessa R. Brownsword; E. Scotford; & K. Yeung (Toim.), *The Oxford Handbook of Law, Regulation, and Technology*, s. 424–450. Oxford: Oxford University Press.

Schaub, F.; Balebako. R.; Durity, A., L.; & Faith Cranor, L. (2015). A Design Space for Effective Privacy Notices, Symposium on Usable Privacy and Security. Ottawa: USENIX Association.

Scheinin, M. (2012). Perusoikeuskonfliktit. Teoksessa T. Heinonen; & J. Lavapuro, *Oikeuskulttuurin eurooppalaistuminen: Ihmisoikeuksien murroksesta kansainväliseen vuorovaikutukseen.* Helsinki: Suomalainen Lakimiesyhdistys.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton Company.

Seipel, P. (1990). *Juristen och datorn, Introduktion till rättsinformatiken* (3. painos). Lund: Norstedts Förlag AB.

Seipel, P. (1992). *Juristen och datorn. Introduktion till rättsinformatiken. Skrifter från Institutet för rättsinformatik 1.* (4. painos). Kristianstad: Norstedts Juridik.

Shadbolt, N.; & Hampson, R. (2019). *The Digital Ape, How to Live (in Peace) with Smart Machines.* Oxford: Oxford University Press.

Solove, D. J. (2007). *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven: Yale University Press.

Solove, D. J. (2008). *Understanding Privacy.* Cambridge: Harvard University Press.

Solove, D. J.; & Schwartz, P. M. (2019). *Privacy Law Fundamentals* (5. painos). Portsmouth: International Association of Privacy Professionals (IAPP).

Spiekermann, S. (2015). *Ethical IT Innovation: A Value Based System Design Approach*. New York: Auerbach Publications.

Spiekermann, S.; & Connor, L. F. (2009). Engineering Privacy. *IEEE Transactions on Software Engineering, vol. 35* (no. 1), s. 67–82.

Stewart-Pollack, J.; & Menconi, R. (2005). *Designing for Privacy and Related Needs.* New York: Fairchild Publications, Inc.

Talus, A. (2016). The European Data Protection Board and other developments under the GDPR. Teoksessa T. Bräutigam; & S. Miettinen (Toim.)*, Data Protection, Privacy and European Regulation in the Digital Age.* Helsinki: Unigrafia.

Véliz, C. (2020). *Privacy is Power: Why and How You Should Take Back Control of Your Data.* Lontoo: Bantam Pres.

Viljanen, V.-P. (2001). *Perusoikeuksien rajoitusedellytykset.* Helsinki: WSOY Lakitieto.

Voigt, P. (2017). *The EU General Data Protection Regulation (GDPR).* Cham: Springer International Publishing.

Voigt, P.; & Von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR) - A Practical Guide.* Springer International Publishing.

Voutilainen, T. (2012). *Oikeus tietoon. Informaatio-oikeuden perusteet.* Porvoo: Edita Publishing Oy.

Wallin, A.-R.; & Konstari, T. (2000). *Julkisuus- ja salassapitolainsäädäntö. Laki viranomaisten toiminnan julkisuudesta ja siihen liittyvät lait.* Helsinki: Suomalaiset oikeusjulkaisut.

Wallin, A.-R.; & Nurmi, P. (1991). *Tietosuojalainsäädäntö: Henkilörekisterilaki ja siihen liittyvät säädökset.* Helsinki: Lakimiesliiton Kustannus.

Wasastjerna, M. (2019). *Competition, data and privacy in the digital economy : testing conventional boundaries and expanding horizons - towards a privacy dimension in competition policy?* Helsinki: University of Helsinki.

Wiener, N. (1954). *The Human Use of Human Beings: Cybernetics and Society* (2. painos). New York: Doubleday Anchor.

Suomalainen virallisaineisto

Lainsäädäntö

Henkilörekisterilaki (471/1987)

Henkilötietolaki (523/1999)

Kirjanpitolaki (1336/1997)

Laki henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä (1054/2018)

Laki majoitus- ja ravitsemustoiminnasta (308/2006)

Perustuslaki (731/1999)

Rikoslaki (39/1889)

Tietosuojalaki (1050/2018)

Muut virallislähteet

EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö

Euroopan ihmisoikeussopimus (SopS 63/1999)

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

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

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

HE 125/2003 vp. Hallituksen esitys eduskunnalle sähköisen viestinnän tietosuojalaiksi ja eräiksi siihen liittyviksi laeiksi

Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (SopS 7–8/1976)

KM 1992:3 Perusoikeuskomitean mietintö

KM 1997:9 Henkilötietotoimikunnan mietintö

PeVL 14/2002 vp. Perustuslakivaliokunnan lausunto koskien hallituksen esitystä eduskunnalle Kansaneläkelaitoksen toimeenpanemiin etuuksiin liittyviin tietojen saamista ja luovuttamista koskevien säännösten muuttamiseksi

PeVL 51/2014 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laeiksi luonnonmukaisen tuotannon valvonnasta sekä elintarvikelain 3 ja 5 §:n muuttamisesta

PeVL 14/2018 vp. Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle EU:n yleistä tietosuoja-asetusta täydentäväksi lainsäädännöksi

Suomen kansallisen valvontaviranomaisen akkreditointikriteeristö yleisen tietosuoja-asetuksen mukaisten käytännesääntöjen valvontaelimille. Tietosuojavaltuutetun toimisto Dnro 572/117/20, annettu 29.1.2021

TSV 18.5.2020. Työnhakijoiden henkilötietojen kerääminen tarpeettomasti Dnro 137/161/2020, annettu 18.05.2020

TSV 26.05.2020. Henkilötietojen käsittelyn vaikutustenarviointi, käsittelyperuste ja rekisteröityjen informointi Dnro 8393/161/2019, annettu 26.5.2020.

TSV 25.06.2020. Pysäköintiluvan osoittavassa kortissa ilmoitettavat tiedot ja tietojen minimointi Dnro 2984/182/2019, annettu 25.6.2020

TSV 19.3.2021. Tietojen minimointi pysäköinninvalvontamaksujen yhteydessä Dnro 5373/182/2018, annettu 19.3.2021

Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, ns. Yleissopimus 108 (SopS 36/1992)

VAHTI 8/2008 Valtionhallinnon tietoturvasanasto

Oikeuskäytäntö

Etelä-Savon KO ratkaisu 18/114227, annettu 29.3.2018

Helsingin KO ratkaisu 18/119000, annettu 3.5.2018

Oulun KO ratkaisu 18/142895, annettu 9.10.2018

Pohjois-Karjalan KO ratkaisu 19/109031, annettu 28.2.2019

Satakunnan KO ratkaisu 19/106975, annettu 14.2.2019

Satakunnan KO ratkaisu 20/104108, annettu 30.1.2020

Turun HO ratkaisu 14/136034, annettu 4.9.2014

Turun HO ratkaisu 17/121354, annettu 26.5.2017

Vaasan HO ratkaisu 20/109076, annettu 4.3.2020

Euroopan unionin virallisaineisto

EU:n lainsäädäntö

Euroopan unionin perusoikeuskirja (2012/C 326/02)

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

Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (tietosuojadirektiivi)

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

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa

Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi). Viimeisin konsolidoitu versio 19/12/2009

Euroopan parlamentin ja neuvoston direktiivi 2013/40/EU, annettu 12 päivänä elokuuta 2013, tietojärjestelmiin kohdistuvista hyökkäyksistä ja neuvoston puitepäätöksen 2005/222/YOS korvaamisesta

Euroopan parlamentin ja neuvoston direktiivi (EU) 2015/2366, annettu 25 päivänä marraskuuta 2015, maksupalveluista sisämarkkinoilla, direktiivien 2002/65/EY, 2009/110/EY ja 2013/36/EU ja asetuksen (EU) N:o 1093/2010 muuttamisesta sekä direktiivin 2007/64/EY kumoamisesta (ETA:n kannalta merkityksellinen teksti)

Euroopan unionin tuomioistuimen oikeuskäytäntö

Asia C-311/18, Data Protection Commissioner v. Facebook Irlanti ja Schrems, ECLI:EU:C:2020:559

Asia C-496/17, Deutche Post AG v. Hauptzollamt Köln, ECLI:EU:C:2019:26

Asia C-582/14, Patrick Breyer v. Saksan liittotasavalta, ECLI:EU:C:2016:779

Asia C-92/09, Volker sekä Markus Schecke ja Eifert v. Land Hessen, ECLI:EU:C:2010:662

Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö

Amann v. Sveitsi, no. 27798/95

Rotaru v. Romania, no. 28341/95

Muu Euroopan unionin virallisaineisto

KOM(2007) 228 lopullinen. Komission tiedonanto Euroopan parlamentille ja neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla, annettu 2.5.2007

KOM(90) 314 lopullinen; SYN 287. Komission ehdotus direktiiviksi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, annettu 27.7.1990 (90/C 277/03)

Euroopan komission suositus älykkäiden verkkojen ja älykkäiden mittausjärjestelmien tietosuojaa koskevan vaikutustenarvioinnin laadintamallista, annettu 10.10.2014 (2014/724/EU)

Euroopan unionin tietosuojatyöryhmä

WP 136 Lausunto 4/2007 henkilötietojen käsitteestä, annettu 20. kesäkuuta 2007

WP 173 Lausunto 03/2010 osoitusvelvollisuuden periaatteesta, annettu 13.7.2010

WP 203 Lausunto 03/2013 käyttötarkoitussidonnaisuudesta, annettu 2.4.2013

WP 216 Lausunto 5/2014 anonymisointitekniikoista, annettu 10. huhtikuuta 2014

WP 248 Ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu "korkea riski", annettu 4. huhtikuuta 2017

WP 260 Asetuksen (EU) 2016/679 mukaista läpinäkyvyyttä koskevat suuntaviivat, annettu 29.11.2017

Euroopan tietosuojaneuvosto

Euroopan tietosuojaneuvoston ohje 1/2019 käytännesääntöjä ja valvontaelimiä koskevista suuntaviivoista, versio 2.0., hyväksytty 4.6.2019

Euroopan tietosuojaneuvoston ohje 4/2019 Artikla 25: Sisäänrakennettu ja oletusarvoinen tietosuoja, versio 2.0., hyväksytty 20.10.2020

Yhdysvaltojen oikeuskäytäntö

FTC v. Wyndham Worldwide Corp. No. 13 – 1887 F.3d 236 (3d Cir. 2015)

In re: DesignerWare, LLC No. 1123151, Docket No. C-4390, (2013)

In re: Eli Lilly & Co., FTC Docket No. C-4047, (2002)

In re: Facebook, FTC No. 092 – 3184, Docket No. C-4365, (2012)

In re: Microsoft Corp., FTC, Docket No. C-4069, (2002)

In re: Sears Holdings Mgmt. Corp., FTC No. C-4264, (2009)

Muut lähteet

Deliberation No. 2014-500 of 11 December 2014 on the Adoption of a Standard for the Deliverance of Privacy Seals on Privacy Governance Procedures Privacy Seals on Privacy Governance Procedures (CNIL), annettu 11.12.2014.

ISO/IEC 27000:2018

London School of Economics: Study on the economic benefits of privacy-enhancing technologies (PETs), 2010.

OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data.

Ordinanza ingiunzione nei confronti di Wind Tre S.p.A. Registro dei provvedimenti n. 143 del 9 luglio 2020

TeleTrusT & ENISA: IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the art", Technical and organizational measures, 2021.

The European Union Agency for Network and Information Security (ENISA): Privacy and Data Protection by Design - from policy to engineering, 2014.

LYHENTEET

CNIL	Commission nationale de l'informatique et des libertés
DPIA	Data Protection Impact Assessment
EDPB	Euroopan tietosuojaneuvosto (European Data Protection Board, EDPB)
EDPS	Euroopan tietosuojavaltuutettu
EIT	Euroopan ihmisoikeustuomioistuin
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
FIPs	Fair Information Practices
FTC	Federal Trade Commission
HO	Hovioikeus
IAPP	International Association of Privacy Professionals
ICO	Information Commissioner's Office
KO	Käräjäoikeus
NAI	Network Advertising Initiative
OSS	One-stop-shop
PET	Privacy-Enhancing Technologies
PIA	Privacy Impact Assessment
TSA	Tietosuoja-asetus
WP 29	Tietosuojatyöryhmä

1. JOHDANTO

1.1. Tutkimusaihe ja käytetty metodi

Oletko saanut joskus mainoksen tai yhteydenoton koskien juuri miettimääsi asiaa? Ei ole nykyään ihmeellistä, että talousvaikeuksissa olevalle opiskelijalle pyritään internetin kautta tarjoamaan mainoksia, jotka koskevat pikavippejä tai rahoitusta. Sama voi koskea yritystä, joka kärsii vastaavista ongelmista.[1] Kysymys on maailmasta, jossa elämme. Tietotekniikan kehittyminen merkitsee jo yksistään haasteita yksityisyyden ja henkilötietojen suojalle, mutta toisaalta kiinnostus niihin on kasvanut. Tärkeää on osana arkipäivää ottaa huomioon henkilötietojen suoja kaikessa toiminnassamme. Enää ei tule jättää huomioimatta heti aluksi yksityisyydelle aiheutuvia riskejä, vaan ne tulee ottaa huomioon jo kehitettäessä uusia tapoja kerätä, käsitellä ja säilyttää henkilötietoja. Yksi yhdysvaltalaisen yksityisyyden pioneereista, Woodrow Hartzog tiivistää oivallisesti ongelmaa:

> *Opponents of tech regulations contend that there are no bad technologies, only bad users. They say 'tech doesn't hurt people, people hurt people'. – Lawmakers have attempted to establish limits on the collection, use and distribution of personal information. But they have largely overlooked the power of design.*[2]

Ilman internetiä ja ohjelmistoja, joita käytämme päivittäin, tilanne olisi *sine qua non* – emme pystyisi hyödyntämään teknologian tuomaa arjen helpotusta. Tästä syystä nostamme hattua heille, jotka tämän ovat saaneet aikaiseksi, mutta samalla meidän tulee tunnustaa, että sosiaalisen median, hakukoneiden ja esineiden internetin maailmassa yksityisyydelle aiheutuvat ongelmat eivät suurimmaksi osaksi ole aivan ilmeisiä. Verkkoyhteiskunnassa[3], jossa elämme, teknologinen suunnittelu saattaa olla niin huomaamatonta, että emme sitä edes huomaa. Esimerkiksi *Hartzog* tuo esiin yksityisyyden suojan ongelmia puhelimia valmistavien yritysten tavassa käyttää matkapuhelimia ja itkuhälyttimiä valvonnan välineenä. Huonosti suunniteltu teknologia rikkoo jatkuvasti käyttäjien odotuksia tietojen jakamisesta, mikä johtaa käyttäjien luopumiseen yksityisyydestään. Uhkat ovat suuria, sillä monet eivät lue pitkiä tietosuojaselosteita sovelluksista, joita arjessa käytämme.[4] Kun järjestelmiä ja sovelluksia hankitaan esimerkiksi

[1] Ks. esim. Schneier, 2015, s. 61–62.
[2] Hartzog, 2018, s. 5.
[3] Saarenpää määrittelee verkkoyhteiskunnan yhteiskunnaksi, jonka merkittävät toiminnot ja prosessit ovat järjestäytyneet erilaisten toisiinsa liittyneiden verkkojen muotoon. Ks. Saarenpää, 2000, s. 4–5. Toisaalta perinteisesti on puhuttu oikeusinformatiikassa siitä, että elämme oikeudellisessa verkkoyhteiskunnassa, jossa yhteiskuntamme oikeudellistuu nopeasti ja uusin tavoin ja missä tietotekniikkasidonnaisuus ja teknologinen konvergenssi lisääntyy. Ks. Saarenpää, 2002b, s. 5 ja 14. Ks. myös Pöysti, 2000, s. 92–93 ja Korhonen, 2003, s. 14–16.
[4] Hartzog, 2018, s. 3–6.

työntekijöille työsuhdetta varten, tulee huomioida niiden tietoturvaratkaisut ja lukea huolella tietosuojaselosteet. Aina tietosuojaselosteen lukeminenkaan ei auta. Yksi tunnetuimmista tapauksista oli eräs taskulamppusovellus, jonka käyttämiseen ani harva uskoisi vaadittavan käyttäjän GPS-sijaintia. Käyttäjä hyväksyi taskulamppua käyttäessään sen, että sovellus saa kerätä kaikkea informaatiota ja myydä sitä kolmansille.[5]

Yksilöistä kerättävä data on nykyään jopa arvokkaampaa kuin perinteiset pienet maksut, joita ohjelmistoiden käytöstä joutuu maksamaan.[6] Kun ohjelmistojen tai sosiaalisen median alustojen käyttäminen on ilmaista, tulee palveluntarjoajien saada niihin rahoitus muualta. Tämä tapahtuu esimerkiksi henkilötietoja myymällä.[7] Samoin yritykset pyrkivät kasvattamaan tietovarantojaan yksilöiden liikkeistä ja tekemisistä keräämällä käyttäjistään mahdollisimman paljon tietoja. Hyvänä esimerkkinä *Bruce Schneier* tuo esiin muun muassa Googlen keräämän datan kaikista hauista, jotka suoritetaan Googlen välityksellä. Nykyaikaisessa työkulttuurissa halutaan käyttää tehokkainta reittiä, ja yksi tällainen on tiedonhakusivustojen, kuten Googlen käyttäminen tiedonhaun yhteydessä. Hakutulosten perusteella Google pystyy päättelemään käyttäjästään yllättävän paljon ja mahdollisesti luomaan yrityksille jopa tietoturva-aukon. Jos käyttäjä päätteellään suorittaa tietyntyyppisiä hakuja, se voi kertoa yrityksessä meneillään olevista toimenpiteistä tai paljastaa liikesalaisuuksia.[8] Kyse ei ole välttämättä siitä, että yritykset käyttäisivät Googlen palveluita. Kyse on siitä, että tietosuojakysymyksissä kaikki lähtee asenteesta ja ymmärryksestä. Myös tämän tutkimuksen osalta keskeisessä roolissa on se, että sisäänrakennettua ja oletusarvoista tietosuojaa voidaan käytännön tasolla toteuttaa vain yksilöistä eli henkilötietojen käsittelyyn yhteydessä olevista luonnollisista henkilöistä käsin. Tietosuojan toteuttaminen edellyttää ajattelutapojen muutosta ja riskien tunnistamista sekä uusien toimintatapojen sisäistämistä.

Tutkimuksen tavoitteena on käsitellä ja tutkia EU:n yleisen tietosuoja-asetuksen (2016/679, jäljempänä TSA) rekisterinpitäjälle asettamaa velvollisuutta toteuttaa sisäänrakennettua ja oletusarvoista tietosuojaa. Tarkemmin tutkimuksen kohteena on rekisterinpitäjältä edellytettävät asianmukaiset tekniset ja organisatoriset toimenpiteet. Tarkastelussa mielenkiintoni kohdistuu yksilön oikeuteen henkilötietojen suojaan, yksityisyyteen ja itsemääräämisoikeuteen. Käytännössä pyrin tarkastelemaan aihealuetta yksilön suojaamisen näkökulmasta, vaikka objektiivisesti pyrin esittämään myös rekisterinpitäjän näkökulmaa toimenpiteiden suorittamisessa.

[5] Ks. Schneier, 2015, s. 54–55.
[6] Ks. identiteettivarkauksien taloudellisesta hyödystä Korja, 2016, s. 184–185 ja sosiaalisen median hyödyntämästä tiedosta Hartzog, 2018, s. 205–206.
[7] Järvinen, 2012, s. 294.
[8] Schneier, 2015, s. 36–37 ja 55–59.

On yllättävän hankalaa tietää ilman syvempää perehtymistä, mitä TSA:ssa tarkoitetut asianmukaiset toimenpiteet kulloinkin ovat. Tutkimuskysymykselläni pyrin selvittämään, *miten yleisessä tietosuoja-asetuksessa rekisterinpitäjältä asetettua vaatimusta asianmukaisten teknisten ja organisatoristen toimenpiteiden suorittamisesta osana sisäänrakennettua ja oletusarvoista tietosuojaa tulee tulkita, ja mitä nämä toimenpiteet käytännössä ovat*.

Aiheen valinnassa keskeisenä seikkana on minulle ollut tietosuoja-asetuksen tietyissä konteksteissa esiintyvä epämääräisyys. Olen pitänyt kummallisena sitä, että isojen sanktioiden uhalla sekä yksityiset että julkiset toimijat ovat velvollisia noudattamaan yleistä tietosuoja-asetusta ja siten sisäänrakennettua ja oletusarvoista tietosuojaa, mutta käytännössä rekisterinpitäjille ei ole tuotettu riittävää informaatiota tämän velvollisuuden toteuttamisen vaatimuksista.[9] Toisaalta tulee muistaa punnita sekä yksilön että organisaation intressejä. Kysymys on siitä pitäisikö viranomaisen määritellä oikeasuhtainen käsittely kaikkiin tilanteisiin. Ehkä ei, mutta kenen oikeus väistyy toisen edeltä? Asiaa tarkemmin tarkasteltaessa herää kysymys siitä, voidaanko tällaista tilannetta ylipäänsä pitää mahdollisena demokraattisessa yhteiskunnassa, jossa toimivien tulisi tuntea voimassa oleva lainsäädäntö. Kansalaisen on tunnettava laki. Tietämättömyys laista ei ole anteeksiantoperuste: *ignorantia iuris nocet.* Samoin rikosoikeuden periaatteiden mukaan ketään ei tule tuomita rangaistukseen sellaisen teon perusteella, jota ei tekohetkellä ole laissa säädetty rangaistavaksi (*nulla poena sine lege)*. Entä sitten, kun rekisterinpitäjä ei tiedä velvoitteidensa sisältöä?

Oikeustieteellisessä tutkimuksessa keskeistä on tutkimusmetodin valinta. Oikeustieteessä ajatellaan usein, että ei ole olemassa mitään yleispätevää, todettua ja standardisoitua metodisäännöstöä.[10] Perinteisenä lähtökohtana oikeustieteellisessä tutkimuksessa on pidetty oikeusdogmaattista eli lainopillista lähestymistapaa. Lainopillisessa tutkimuksessa selvitetään oikeuslähteiden avulla voimassa olevan oikeuden sisältöä ja eri säännösten välisiä suhteita. Kysymys on yksinkertaistetusti siitä, miten lakia tulisi erilaisissa tilanteissa tulkita. Tämän tuloksena lainopilla tuotetaan normi- ja tulkintakannanottoja. Normikannanottojen tehtävänä on yksinkertaisuudessaan osoittaa ne oikeusnormit, jotka kuuluvat voimassa olevaan oikeuteen eli oikeusjärjestykseen. Oikeusjärjestyksellä tarkoitetaan tietyssä valtiossa vaikuttavien oikeusnormien muodostamaa kokonaisuutta. Tällöin oikeusnormien sisältöä analysoidaan ja annetaan siitä tulkinnallinen näkemys.[11] Lainopissa ei ole kyse pelkästään yksittäisten normien tulkinnasta tai niiden esittämisestä. Laajemmin lainopillisesti voidaan tutkia myös oikeusperiaatteita.

[9] Ks. Dienst, 2018, s. 52.
[10] Aarnio, 2011, s. 12.
[11] Hirvonen, 2011, s. 21–22.

Lainopillisin menetelmin pyritään tulkitsemaan oikeussäännöksiä sekä punnitsemaan ja yhteensovittamaan eri oikeusperiaatteita keskenään. Tällaisia tuloksia voidaan pitää punnintakannanottoina. Oikeusjärjestyksen systematisoinnissa kyse on johdonmukaisen kokonaisuuden luomisesta, johon sisältyy lainsäätäjän muodostamien normien järjestäminen oikeudenaloittain ja niistä syntyvän koherentin kokonaisuuden rakentaminen.[12] Oikeustiedettä harjoitettaessa oikeuden yleistieteiden ja perinteisen lainopin välillä on käynnissä jatkuva tieteellinen yhteys, jossa teorialla on vaikutus metodiin, metodilla on vaikutusta käytäntöön ja käytännöllä puolestaan sekä metodiin että teoriaan. *Saarenpää* puhuu tässä yhteydessä oikeudellisen tiedon ja taidon hermeneuttisesta kehästä, missä oikeudellinen tieto ja taito saavat toisiltaan jatkuvasti uusia impulsseja.[13]

Oikeusinformatiikan tieteenalaa on pidetty perinteisessä oikeudenalajaottelussa uutena oikeudenalana. Kirjallisuudessa on esitetty kysymys siitä, onko tieteenalalla jokin oma metodinsa, jota tulisi käyttää oikeusinformatiikan tutkimuksessa. Suomalaisessa oikeudellisessa tutkimuksessa esimerkiksi sekä *Kangas* että *Korja* on nähnyt mahdolliseksi liittää oikeusinformatiikan tutkimukseen metodinen lähtökohta, jossa oikeudellista sääntelyä kokeillaan teknologian taustalla olevaan informaatioon ja informaatiovirtoihin. Tällä metodilla täydennettävä lainopillinen tutkimus voidaan *Kankaan* mukaan jakaa lisäksi ongelmakeskeiseen ja normikeskeiseen lähestymistapaan. Ongelmakeskeisen lähestymistavan piirteisiin lukeutuu oikeudenalat ylittävä asenne, jossa muodostetaan kokonaiskuva oikeudellisen ongelman sääntelystä yhteiskunnasta eikä niinkään oikeusjärjestyksestä käsin.[14] Ongelmakeskeisen metodin avulla pystyn tuomaan esille uutta näkökulmaa ja tätä kautta arvioimaan ja optimoimaan informaatioon kohdistuvaa oikeudellista lähestymistapaa. Oikeusinformatiikan metodin avulla on myös mahdollista korvata teknologiariippuvaisia lähestymistapoja sekä auttaa ymmärtämään teknologioiden luonnetta.[15] Ennen kaikkea metodissa on siis kysymys siitä, että kysytään ajan ehdoilla.[16] Sanotun pohjalta tämän tutkimuksen kannalta keskeisessä asemassa on voimassa oleva lainsäädäntö. Tutkimusmetodina käytän lainopillista eli oikeusdogmaattista metodia, jota täydennän oikeusinformatiikan metodilla. Tavoitteeni on synnyttää uudenlaista ymmärrystä vallitsevista rekisterinpitäjän velvollisuuksista luoden tulkinta-apua niukkaan säädöstekstiin. Pyrkimyksenä sen ohella on herättää ymmärrystä sisäänrakennetun ja oletusarvoisen tietosuojan sisällöstä ja systematisoida keinoja, joilla tietosuojaystävällisiin tavoitteisiin voidaan päästä. Metodin

[12] Hirvonen, 2011, s. 24–25.
[13] Saarenpää, 2016, s. 128.
[14] Korja, 2016, s. 13–15 ja Kangas, 1997, s. 90–95, sekä Kangas, 1982, s. 385–386.
[15] Burkert, 2014, s. 399.
[16] Korja, 2016, s. 13.

valintaan vaikutti erityisesti se, että haastavan tehtävän edessä problematiikkaa voidaan selventää asettamalla se kysymyksenalaiseksi käytännön toimien kohdalla. Ongelma on siinä, ettei velvoitteen sisältöä vastuun taustalla tunneta riittävän hyvin.

Sisäänrakennettu ja oletusarvoinen tietosuoja on käsitteenä hyvin laaja. Organisatoristen ja teknisten toimenpiteiden esittäminen ei ole yksinkertaista. Huomioiden tietoteknisen ja yhteiskunnallisen kehityksen aiheuttamat ongelmat ei teknisistä toimenpiteistä ole mahdollista luoda tyhjentävää luetteloa. Tästä syystä olen rajannut tutkimukseni siten, että en käsittele sisäänrakennettua ja oletusarvoista tietosuojaa itsessään kovin syvällisesti, sillä erilaisista tulkinnoista voisi tehdä kokonaan oman teoksen. En käsittele myöskään esimerkiksi teknisten toimenpiteiden ja ratkaisujen yksityiskohtaista käytännön toteutusta. Yleisesti ottaen tämä ei olekaan tarpeellista oikeudellisesta näkökulmasta, sillä yleensä toiset asiantuntijat toteuttavat tekniset ratkaisut. Keskeisenä pidän sitä, että lukija ymmärtää kontekstin sisällä käsitteiden ja velvollisuuksien suhteen rekisterinpitäjältä edellytettäviin toimenpiteisiin. Tutkimus ei ole miltään osin sidottu yksittäiseen toimialaan, jossa esimerkiksi rekisterinpitäjä toimisi. Tutkimuksessa esitetyt esimerkit on lähinnä luotu selventämään käytännönläheisin keinoin kunkin toimenpiteen merkityssisältöä. Tämä on seurausta siitä, että ei ole mahdollista esittää yleispäteviä ohjeita, jotka toimisivat jokaisella yhteiskunnan osa-alueella. Syytä on myös kiinnittää huomiota siihen seikkaan, että tutkimuksessa ei käsitellä tarkkarajaisesti julkisen ja yksityisen sektorin välistä jakoa tai esimerkiksi rikosasioihin liittyviä kysymyksiä, joita varten on erikseen annettu EU:n tasolla lainsäädäntöä. Kyse ei myöskään ole työelämän tietosuojan tulkitsemisesta, josta on erikseen kirjoitettu oikeuskirjallisuudessa[17]. Tutkimuksella ei myöskään ole liityntää sähköiseen viestintään ja niin sanottuun *ePrivacy*-sääntelyyn.

1.2. Oikeusinformatiikka oikeuden yleistieteenä

Oikeudenalajaottelussa tämä tutkimus lukeutuu oikeusinformatiikan alaan. *Oikeusinformatiikkaa*[18] on pidetty suhteellisen uutena mutta vakiintuneena kansainvälisenä oikeustieteellisenä tutkimusalana. Oikeusinformatiikassa tutkitaan oikeuden ja informaation sekä oikeuden ja tietotekniikan välisiä suhteita sekä niiden yhteydessä ilmeneviä sääntely- ja tulkintakysymyksiä.[19] Oikeusinformatiikan status suhteellisen uutena oikeustieteellisenä tutkimusalana johtuu sen tietotekniikkasidonnaisuudesta, ja siitä voidaankin puhua muutosten tieteenä.

[17] Ks. esim. Alapuranen ym., 2020.
[18] Oikeusinformatiikasta käytetään ruotsiksi termiä *rättsinformatik*, saksaksi *rechtsinformatik*, englanniksi *legal Informatics*, espanjaksi *derecho Informática*, ranskaksi *droit et Informatique*, hollanniksi *retsinformatik*, norjaksi *rettsinformatikk*. Ks. Seipel, 1990, s. 24.
[19] Saarenpää, 2002b, s. 1.

Oikeusinformatiikan syntyminen yhdistetään usein tietokoneiden syntymisen aikaan.[20] Alun perin oikeusinformatiikkaa pidettiin oikeustieteen aputieteenä, jonka tarkoituksena nähtiin tutkimustarve teknologian ja oikeuden välisestä suhteesta.[21] *Lee Loevinger* puhui jurimetriikasta, jossa hän piti tärkeänä tietokoneen käyttämistä oikeustieteen apuna siellä, missä kaivattiin tarkkaa informaatiota.[22]

Virallisesti oikeusinformatiikan termi nousi keskustelussa esiin Saksassa *Wilhem Steinmüllerin* tutkiessa oikeudellisia ongelmia liittyen teknologiseen informaatioon ja tietokoneisiin.[23] Sittemmin oikeusinformatiikka on vakiinnuttanut paikkansa eurooppalaisessa oikeustieteessä omana oikeudenalanaan niin opetuksessa kuin tieteellisessä tutkimuksessa.[24]

Oikeusinformatiikan piirissä on nykyään tunnusomaista tutkia riskien tunnistamista, lainsäädännön muutostarpeita, informaation yhteiskunnallista merkitystä, tietojärjestelmien ja tietoverkkojen käyttömahdollisuuksia sekä oikeudellisia tietovarantoja ja niiden käyttämistä. Tutkimuksessa keskeisenä on oikeusinformatiikan eteenpäin katsova luonne.[25]

Vaikka oikeusinformatiikan asemasta oikeustieteessä on sen historian aikana ollut paljon keskustelua, nykyään se luetaan ainakin osaksi oikeuden yleistieteitä.[26] Oikeusjärjestelmäämme kuvaavan perusteoksen *Encyclopedia Iuridica Fennicassa* oikeusinformatiikka luetaan oikeusteorian, oikeuslingvistiikan ja oikeussosiologian ohella oikeuden yleistieteisiin. Oikeusinformatiikka on laaja-alainen tiede, jolla voidaan nähdä olevan liityntöjä niin oikeusfilosofiaan, oikeusteoriaan, oikeusvertailuun kuin myös teoreettiseen ja perinteiseen lainoppiin.[27]

Perinteisesti oikeudenalan olemassaololle on asetettu vaatimuksia, joista yksi on sen muista erottava oikeusperiaate. Siinä missä oikeusinformatiikan eri osa-alueilla on omia periaatteita, voidaan ihmisoikeusperiaate nähdä niitä kaikkia yhdistävänä periaatteena, joka ei toisaalta ole erottava vaan kaikkea oikeustiedettä yhdistävä periaate.[28]

Perinteisessä keskustelussa oikeusinformatiikka on jaettavissa yleiseen ja erityiseen osaan. Saarenpään jaon mukaan oikeusinformatiikan yleisen osan puitteissa tutkitaan verkkoyhteiskunnan oikeudellisesti merkityksellistä kehitystä, uudenlaista informaatioinfrastruktuuria ja

[20] Ks. Saarenpää, 2016, 73–83 ja Korhonen, 2003, s. 26
[21] Korhonen, 2003, s. 26. Ks. oikeusinformatiikan kehitysvaiheista Saarenpää, 2016, 89–95.
[22] Korhonen, 2003, s. 26.
[23] Steinmüller otti ensimmäisenä käyttöön oikeusinformatiikan käsitteen oikeustieteellisessä opetuksessa vuonna 1970.
[24] Ks. Korhonen, 2003, s. 26–29 ja Saarenpää, 2016, s. 94.
[25] Saarenpää, 2016, s. 95.
[26] Korhonen, 2003, s. 26.
[27] Saarenpää, 2016, s. 128, ks. Encyclopedia Iuridica Fennica osa VII Oikeuden yleistieteet.
[28] Saarenpää, 2016, s. 129.

oikeudellisen informaation merkitystä yhteiskunnassa sekä verkkoyhteiskunnan lakimiesprofessiolle asettamia vaatimuksia. Erityiseen osaan on perinteisesti katsottu lukeutuvan oikeudellinen tietojenkäsittely, oikeudellisen informaation tutkimus, informaatio-oikeus sekä tietotekniikkaoikeus.[29] Pöysti näkee oikeusinformatiikan erikoistumisalojen jakautuvan vielä lisäksi käytännölliseen ja teoreettiseen lähestymistapaan ja näkee oikeusinformatiikan monialaisena tieteenalana sisäisesti ja rajojensa ulkopuolella. Hänen mielestään oikeusinformatiikka on siten erityinen näkökulma ja tutkimuksen väline verrattuna perinteiseen lainopin puitteissa toteutettavaan geneeriseen oikeustieteeseen.[30]

Informaatio-oikeus voidaan nähdä oikeusinformatiikan alalla ehkä kaikkein käytännönläheisimpänä ja toiminnallisesti määräytyvänä oikeudenalana. Käytännönläheisyydestä huolimatta informaatio-oikeuden haasteina on oikeudellisen kontekstin sovittaminen voimassa oleviin säännöksiin ja uusiin informaation käsittelymuotoihin.[31] Informaatio-oikeudellinen kehitys on pitkälti myös EU:ssa tapahtuneiden muutosten seurausta. Saarenpään luetteloon informaatio-oikeuden yleisistä opeista – oikeudesta tietoon, oikeudesta viestintään, informaatioon ja sen kulun vapauteen, tiedolliseen itsemääräämisoikeuteen ja oikeuteen tietoturvasta – sisältyy paljon nykyisin vaikuttavia oikeusperiaatteita. Saarenpää pitääkin yleisiä oppeja metaoikeuksina eli yhteiskuntasopimusten tasoisina, tavoitteellisina ja moraalisina päämääräoikeuksina. Saarenpään mukaan yleisiä periaatteita täydentävät puolestaan erityiset oikeusperiaatteet, kuten yksityisyys, julkisuus, viestinnän vapaus ja tietoturvallisuus.[32] Toisaalta, vaikka informaatio-oikeutta on pidetty perinteisesti osana oikeusinformatiikkaa, on viime aikoina kehitelty ajatusta siitä, että informaatio-oikeus olisi kokonaan uusi ja itsenäinen oikeudenala tai ainakin tulevaisuudessa muotonsa saava oikeudenala.[33]

Aineelliselta osalta tämä tutkimus lukeutuu oikeusinformatiikan sisäisessä jaottelussa informaatio-oikeuteen ja siten osaksi oikeusinformatiikan erityistä osaa. Toki myönnettäköön, että tutkimuksen moninaisen sisällön johdosta siinä on viitteitä myös muilta oikeusinformatiikan osa-alueilta, kuten tietoturvallisuuden osalta oikeudellisesta tietojenkäsittelystä ja tietotekniikkaoikeudesta. Toisaalta on hyvä huomata, että perinteisesti henkilötietojen suoja on systemaattisesti ensisijaisesti siviilioikeuteen kuuluvaa persoonallisuusoikeuden ydinaluetta[34].

[29] Saarenpää, 2002b, s. 1, 9 ja 11–21.
[30] Pöysti, 1999, s. 25 ja 359–360, näin myös Seipel, 1992, s. 15–16.
[31] Seipel, 1992, s. 36–39.
[32] Saarenpää, 2002b, s. 41–45.
[33] Korpisaari, 2016, s. 993. Ks. myös Neuvonen, 2019, s. 16–17.
[34] Saarenpää, 2016, s. 75.

1.3. Tutkimuksen rakenne ja käytetyt lähteet

Tutkimuksen kantavana ajatuksena on syventyä yksilöiden asemaan suhteessa heidän tietojaan käsitteleviin organisaatioihin. Tarkoitan tällä sitä, että näen yksilöiden aseman suhteessa isoihin toimijoihin olevan heikko – vaikkakin se on sääntelyn ansiosta näennäisesti korostetussa asemassa. Isot toimijat käytännössä sanelevat sen, miten yksilöiden tietoja käsitellään. Yhtenä tekijänä nykypäivänä on se, että yksilöillä ei ole kykyä tai mahdollisuutta edes tietää, miten heistä tietoja kerätään. Tämä voi johtaa tilanteeseen, jossa oikeustieteen tulee pystyä tieteenä osoittamaan lainsäädännön epäkohdat. Itse olen omakohtaisesti kokenut sen, että organisaatiot pyrkivät keräämään minulta mahdollisimman paljon henkilötietoja. Kyse voi toisaalta olla esimerkiksi tietämättömyydestä henkilötietojen suojaamisesta.

Tutkimuksen aluksi on syytä tutustua yksilölle turvattuihin oikeuksiin. Aluksi pyrin esittelemään yksityisyyden sisältöä ja sen merkitystä yksilölle mutta toisaalta tuomaan esille seikkoja, joita rekisterinpitäjän tulisi kunnioittaa käsitellessään yksilöiden henkilötietoja. Samalla käyn lävitse tämän tutkimuksen tärkeimmät käsitteet. Nykyään henkilötietojen suojaa pyritään täsmentämään erinäisin sääntelykeinoin, joita ovat niin oikeudelliset normit kuin ohjeistukset. Pyrin esittämään myös sääntelyn kehityksen aiheen kannalta relevantein osin sekä tuomaan esille sen, että vastauksia kysymyksiin voidaan löytää yllättävänkin helposti.

Tämän jälkeen syvennyn varsinaiseen aiheen kannalta tärkeään vaatimukseen, sisäänrakennettuun ja oletusarvoiseen tietosuojaan. Tietosuojaa ei tule pitää minään mörkönä, jota tulisi pelätä. Päinvastoin näen sen oikein toteutettuna jopa organisaatiota hyödyttävänä. Asianmukaisten toimenpiteiden vaatimuksen sisällöstä huomataan, että se sisältää hyvin lavean ilmauksen siitä, mitä toimenpiteitä rekisterinpitäjän tulee käytännössä tehdä täyttääkseen yleisen tietosuoja-asetuksen asettamat vaatimukset. Rekisterinpitäjältä edellytettäviin organisatorisiin ja teknisiin toimenpiteisiin syvennytään käsittelemällä niitä tutkimuksessa kolmessa osassa. Käsittelen teknisiä ja organisatorisia toimenpiteitä erillään ja kolmantena käsittelen aihetta toimenpiteiden toteuttamista ohjaavan osoitusvelvollisuuden kautta. Lopuksi pyrin vetämään yhteen tutkimuksella saavutetut tulokset.

Rakenteen olen muodostanut kumulatiiviseksi, jotta se on kaikkien asiaan perehtymättömien myös helppo sisäistää. Jokainen kappale pitää sisällään tietoa, jota hyödynnetään myöhemmässä vaiheessa. Pidän myös tärkeänä käsitellä yksilön yksityisyyden suojaa sekä itsemääräämisoikeutta ja oikeutta henkilötietojen suojaan siinä määrin, että lukijalle käy selväksi niiden korostunut asema tietosuojalainsäädännön taustalla. Vetoan varsin paljon siihen, että rekisteröidyn oikeuteen turvalliseen ja yksityisyyttä kunnioittavaan henkilötietojen käsittelyyn ei

panosteta tarpeeksi tai ei välttämättä ymmärretä sen merkitystä. On syytä huomata, että kaikki tässä tutkielmassa esille nousevat teemat ovat sidoksissa toisiinsa. Kuten myöhemmin ilmenee, sisäänrakennettu ja oletusarvoinen tietosuoja ei ole pelkästään yksi artikla muiden joukossa – päinvastoin, sillä on useita liitoskohtia yleisen tietosuoja-asetuksen sisällä.

Tutkielman lähteinä olen käyttänyt etenkin virallisaineistoa ja oikeuskirjallisuutta. Organisatorisia ja teknisiä toimenpiteitä on tutkittu tähän asti lähinnä liittyen johonkin tiettyyn oikeudelliseen ongelmaan, kuten *big dataan*. Tutkimus on tällöin ollut sidoksissa yksittäiseen ongelmaan, mutta käsittääkseni aihetta ei ole tutkittu tämän tutkimuksen laajuudessa. Pyrin omalla tutkimuksellani täyttämään aukkoa, joka on syntynyt liian kapeasta aiheen käsittelystä. Virallislähteiden avulla on aiheeseen saatu viime aikoina tulkinta-apua esimerkiksi Euroopan tietosuojaneuvoston ohjeista. Toisaalta joissain teoksissa on sivuttu asianmukaisia toimenpiteitä mutta hyvin lyhyesti. Virallislähteinä käytän sekä eurooppalaista että kansallista lainsäädäntöä ja valmisteluasiakirjoja. Oikeuskirjallisuudesta pyrin kokoamaan juuri aiheeseen liittyviä näkökulmia, sillä tyypillisesti aihepiiriä on käsitelty yksittäisessä teoksessa osana rekisterinpitäjän velvollisuuksia. Näiden pohjalta pyrin luomaan johdonmukaisen koherentin kokonaisuuden, josta mahdollisimman hyvin selviävät ne tietosuoja-asetuksen taustalla olevat keinot, joilla toteutetaan sisäänrakennettua ja oletusarvoista tietosuojaa. Lisäksi käsitellään tarkemmin niitä organisatorisia ja teknisiä toimenpiteitä, jotka ovat ainakin välttämättömiä *lähes* jokaiselta rekisterinpitäjältä. Oikeuskäytännössä aihe ei ole vielä esiintynyt. Syynä lienee se, että kyse on suhteellisen uudesta lainsäädännöstä. Oikeuskäytäntöä käytän kuitenkin tietyissä ja saatavilla olevissa tilanteissa selkeyttämään varsinaisista kirjallisista lähteistä tekemiäni johtopäätöksiä.

2. YKSITYISYYS, HENKILÖTIETOJEN SUOJA JA YLEINEN TIETOSUOJA-ASETUS

2.1. Käsitteistä

2.1.1. Yksityisyys ja yksityisyyden suoja

Yksityisyys on epämääräinen ja vaikeasti ymmärrettävä käsite, mikä on yllättävää, kun otetaan huomioon sen keskeinen rooli lainsäädännössä ja jokapäiväisessä elämässämme. Jokainen yritys sen määrittelyssä on päätynyt yleisesti ottaen joko liian tarkkaan määrittelyyn tai liian yleiseen määrittelyyn ollakseen hyödyllinen. Näin ollen tarkkaan ottaen yksityisyydelle ei voida antaa yksiselitteistä määritelmää, joka läpäisisi eri oikeusjärjestyksiä.[35]

[35] Bygrave, 2002, s. 125–127.

Suomessa ei ole määritelty yksityisyyden käsitettä missään laissa tai säädöksessä. Yksityisyyden käsitettä käytetään yleisesti olettaen, että sen sisältö tunnetaan. Niinpä sitä käytetään myös sellaisenaan lainsäädännössä. Yksityisyys on yksi itsemääräämisoikeutemme elementeistä.[36] Oikeudellisena käsitteenä yksityisyys on lähtöisin Yhdysvalloista. Käsite on muodostunut oikeuskirjallisuudessa, jossa toimeenpaneva voima oli *Warrenin & Brandleisin* muotoilu oikeudesta olla yksin. Varsinaisesti yksityisyys oikeutena ja sen sisältö on kehittynyt oikeuskäytännössä.[37] Perusoikeusnäkökulmasta yksityisyyden käsitettä ilmentävät useat eri perusoikeudet. Henkilötietolain (523/1999) esitöissä todettiin, että yksityisyyden suoja muodostuu itsemääräämisoikeuden ja yksityiselämän suojan lisäksi myös oikeudesta kunniaan, yhdenvertaiseen ja ihmisarvoiseen kohteluun ja turvallisuuteen sekä yhdenvertaisuudesta, syrjinnän kiellosta ja oikeudesta vaikuttaa itseään koskeviin asioihin. Lisäksi yksityisyys voi ilmetä eri tilanteissa eri tavoin.[38] Perusoikeudet eivät ole aina toisistaan selkeästi erotettavissa, vaan ne ovat monilta osin päällekkäisiä ja toisiinsa vaikuttavia. Edellä mainittujen lisäksi henkilötietojen suojaan vaikuttavia perusoikeuksia voidaan katsoa olevan uskonnon ja omantunnon vapaus, sananvapaus sekä julkisuus.[39]

Tämän tutkimuksen kannalta tärkein yksityisyyden osa-alue on henkilötietojen suoja. Tätä osa-aluetta yksityisyyden suojan osalta on pidetty tärkeänä sen korostuneen aseman vuoksi, sillä nykyaikaisessa yhteiskunnassamme toimiminen edellyttää jossain määrin henkilötietojen suojasta ja yksityisyydestä luopumista useissa kaupallisissa ja sosiaalisissa tilanteissa.[40] Yksityisyyden käsitettä on yritetty määritellä *kyvyksi hallita tietoja, oikeudeksi olla yksin, salaisuudeksi, läheisyydeksi, autonomiaksi* ja *vapaudeksi*. Kaikki nämä ovat sekä oikeita että vääriä ainakin tietyissä konteksteissa. Esimerkiksi yksityisyyden ajattelu pelkästään kontrollin näkökulmasta sopii huonosti julkisen valvonnan aiheuttamiin ongelmiin tai yksityiseen toimintaan, kuten seksuaaliseen vapauteen liittyviin vapauksiin. Salassapito soveltuu puolestaan huonosti tietoihin, joita pidämme yksityisinä, mutta jaamme niitä kuitenkin muiden kanssa. [41]

Vaikka laaja tieteellinen ja oikeudellinen kirjoittaminen yksityisyydestä on tuottanut monia erilaisia käsityksiä yksityisyydestä, ne voidaan luokitella *Soloven* tulkinnan mukaan kuuteen yleiseen tyyppiin: yleiseen tyyppiin;

[36] Yksityisyydestä ja sen osa-alueista ks. Saarenpää, 2015, s. 313–324.
[37] Ibid., s. 318–319 ja Korhonen, 2003, s. 108–111.
[38] KM 1997:9 s. 40 ja 84–85 ja HE 96/1998 vp., s. 30–31.
[39] EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmän (TATTI) mietintö, s. 73.
[40] Neuvonen, 2014, s. 60.
[41] Kremer, 2017, s. 52–57.

1) oikeuteen olla yksin, missä kyse on *Samuel Warrenin* ja *Louis Brandleisin* kuuluisasta muotoilusta oikeudesta yksityisyyteen,
2) rajoitettuun pääsyyn itseensä, missä säilytetään kyky suojautua muiden ei-toivotulta pääsyltä,
3) salailuun, missä tietyt asiat salataan muilta,
4) henkilökohtaisten tietojen valvontaan, missä pystytään hallitsemaan itseään koskevia tietoja,
5) persoonallisuuteen, jossa säilytetään yksilöllisyys ja sen arvokkuuden suojaaminen, ja
6) läheisyyteen, jossa korostetaan läheisten suhteiden tai elämän osa-alueiden hallintaa tai rajoitetaan pääsyä lähipiiriin.[42]

Eri lähestymistavoilla on erilaiset tarkoitusperät. Osassa käsityksistä keskitytään keinoihin, joilla yksityisyys voidaan saavuttaa. Toisissa keskitytään yksityisyyden tavoitteisiin. Esimerkiksi salailussa on kyse pyrkimyksestä saavuttaa absoluuttinen yksityisyys pitämällä kaikki asiat yksityisinä. Puolestaan rajoitetussa pääsyssä itseensä on kyse yksityisyydestä, jonka yksilö saa aikaiseksi käyttämällä itsemääräämisoikeuttaan. *Solove* pitää yksityisyyden määrittelyn vaikeuden syynä käytettyjä metodeja. Useimmat yritykset käsitteellistää yksityisyyttä ovat tähän mennessä noudattaneet perinteistä konseptointimenetelmää. Suurin osa teoreetikoista hahmottelee yksityisyyden määrittelemällä sen *per genus et differentiam*. Toisin sanoen teoreetikot etsivät yhteisiä tarpeellisia ja riittäviä elementtejä, jotka määrittävät yksityisyyden ainutlaatuiseksi muista käsitteistä. He pyrkivät löytämään yksityisyyden "olemuksen". Tällöin teoriat kaatuvat omiin ehtoihinsa – ne eivät koskaan saavuta tavoitetta löytää yhteinen nimittäjä.[43]

Esimerkiksi *Helen Nissenbaum* on esittänyt, että se, mitä pidämme yksityisenä, on täysin normien funktio, jonka informaatiovirtojen konteksti määrittelee. Kun voimassa olevia normeja rikotaan, näiden tietojen kontekstuaalista eheyttä on rikottu ja samoin yksityisyyttämme on loukattu. Kontekstuaalinen eheys saavutetaan, kun toimet ja käytännöt ovat yhteydessä informaationormeihin. Sitä rikotaan, kun toimet tai käytännöt uhmaavat odotuksia häiritsemällä juurtunutta tai normatiivista tiedonkulkua.[44] *Solove* ehdottaa uutta tapaa käsitteellistää yksityisyys. Yksityisyyttä olisi pidettävä eräänlaisena sateenvarjoterminä, joka viittaa laajaan ja eriävään ryhmään asioita. Hänen käsityksensä mukaan meidän pitäisi ymmärtää yksityisyys suojana moninaisilta erillisiltä mutta toisiinsa liittyviltä ongelmilta. Jokaisella ongelmalla on yhteisiä liityntäkohtia muiden kanssa, mutta ei välttämättä samaa yksittäistä tekijää – niillä on yhteisiä

[42] Ks. luokittelusta ja perusteluista tarkemmin Solove, 2008, s. 12–38.
[43] Ibid.
[44] Nissenbaum, 2015, s. 157.

perhekytköksiä keskenään siinä, mitä kutsumme yksityisyydeksi.[45] *Neil Richards* pitää yksityisyyttä kysymyksinä säännöistä ja normeista, jotka säätelevät henkilökohtaisiin tietoihimme liittyvää toimintaa tai toimettomuutta.[46] *Hartzogin* mielestä on puolestaan tärkeää keskittyä yksityisyyden erityisiin käsitteisiin, ongelmiin ja sääntöihin sen sijaan, että keskityttäisiin laajaan pyrkimykseen muodostaa yksityisyyden käsite. Yksityisyyttä tulisi hänen mielestään arvostaa hyödyllisyydestään, ja siksi se pitää sisällään käsitteitä luottamuksesta, epävarmuudesta ja autonomiasta, vaikka siihen liittyy monia erilaisia arvoja.[47]

Nissenbaum puhuu paljon kontekstin korostamisesta. Hän on pohtinut sitä, mitä konteksti tarkoittaa. Yksi esimerkki on Yhdysvalloissa vuonna 2012 hyväksytty laki koskien kuluttajien tietosuojaa[48]. Laki sisältää periaatteen, jonka mukaan kontekstia tulee kunnioittaa. Konteksti on armottoman monitulkintainen termi, joka voi merkitä yksilöille kaikkea maan ja taivaan väliltä. Sen merkitykset vaihtelevat puhekielestä ja yleisestä territoriaalisiin sekä spesifeihin määritelmiin. Sen määrittäminen, mitä kontekstin kunnioittaminen tarkoittaa, avaa lisää tulkinnallisia kysymyksiä. Kontekstin tulkintaa voidaan lähestyä monesta suunnasta, joista *Nissenbaum* pitää neljää merkityksellisenä: konteksti teknologia-alustana tai -järjestelmänä, konteksti liiketoimintamallina tai käytäntönä, konteksti teollisuutena tai teollisuuden alana ja konteksti sosiaalisessa ympäristössä. Hän toteaa, että lähes kaikissa näkemyksissä yksityisyydestä puhuttaessa pyritään ajattelemaan, että yksityisyyteen keskittymisessä on kyse henkilötietojen paljastumisesta tai rekisteröityjen kontrollin vähentymisestä.[49]

Kuten todettua *Nissenbaum* pitää yksityisyyden arvioinnissa kontekstuaalisen eheyden periaatetta tärkeänä. Teknologia, liiketoimintakäytännöt, teollisuus ja sosiaalinen ympäristö puolestaan muovaavat kontekstia. Yksittäisissä tapauksissa nämä tekijät yhdessä tai yksinään vaikuttavat yksilöiden odotuksiin siitä, miten tietoa heistä kerätään, käytetään ja hyödynnetään. Mikään näistä ei kuitenkaan tarjoa oikeaa analyysitasoa tai ei voi antaa samaa moraalista ja poliittista painoarvoa kuin sosiaalinen ympäristö. Kontekstin kunnioittamisen periaate edellyttää hänen mielestään sitä, että informaatiovirrat arvostetaan tietotyyppien, toimijoiden ja siirtoperiaatteiden perusteella. Näitä informaatiovirtoja tulee arvioida tasapainossa siten, että otetaan huomioon toimijoiden intressit sekä mahdolliset vaikutukset arvoihin ja kontekstiin. Tällaiset arvioinnit ulottuvat tavanomaisten sidosryhmien etujen ulkopuolelle ja jopa yksityisyyskeskusteluissa laajalti tunnustettujen yleisten moraalisten ja poliittisten arvojen ulkopuolelle.

[45] Ks. Solove, 2008, s. 45 ja 171–172.
[46] Richards, 2015, s. 34–36.
[47] Hartzog, 2018, s. 10–11.
[48] Consumer Privacy Bill of Rights.
[49] Nissenbaum, 2015, s. 153–163.

Konteksti ei ole siten vain passiivinen tausta, jonka perusteella asianosaisten osapuolten etuja mitataan, tasapainotetaan ja vaihdetaan. Lisäksi konteksti määrittelee, miten näitä etuja ja arvoja olisi punnittava. Itse kontekstin eheys on tiedollisten käytänteiden välinen, lopullinen ratkaisu. Kontekstin yhteiskunnallisessa ympäristössä tulkinnan mukaan kontekstin kunnioittaminen tarkoittaa yleisiä eettisiä ja poliittisia arvoja edistäviä informaationormeja sekä kontekstikohtaisia päämääriä, tarkoitusta ja arvoja.[50] Käytännössä kyse on kunkin yksilön odotuksista kussakin yksittäisessä tilanteessa. Kaikki tekijät muokkaavat kontekstia ja siten yksittäisessä tilanteessa myös yksilön oletuksia. Kontekstisidonnaisuus merkitsee sitä, mitä henkilö kohtuudella voi odottaa tai ymmärtää. Tästä syystä kontekstin ymmärtäminen on hyvin tärkeää.

Edellä olevissa esimerkeissä yksityisyyden suojaa peilataan johonkin muuhun, toiseen kohteeseen. Suomessa esimerkiksi *Mahkonen* on pitänyt yksityisyyttä eristäytyneisyyden tilana, jossa sitä peilataan sosiaalisuuteen, yhteisöllisyyteen tai itsemääräämisoikeuteen.[51] *Neuvonen* pitää tällaista jaottelua perusteltuna mutta muistuttaa, että oikeudellisessa käsitteistössä on lähdettävä siitä, että oikeus (tai oikeudet) yksityisyyteen antavat jollekin oikeuden ja toiselle velvollisuuden kunnioittaa tätä oikeutta ja tosiasiallisen mahdollisuuden oikeuden toteutumiseen. Esimerkkeinä hän pitää työpaikan ja kodin välistä eroa ja yksityisyyden merkitystä siinä. Toisaalta yksityisyydessä on hänen mielestään kyse sellaisten tietojen suojaamisesta, jotka eivät ole julkisia, ja toisaalta sillä tarkoitetaan yksityisyyttä sosiaalisessa toiminnassa, kuten ihmissuhteissa.[52]

Ihmisoikeutta tiedolliseen yksityisyyteen, henkilötietojen suoja mukaan luettuna, voidaan pitää siten periaatteena – tai periaatteesta johtuvana oikeutena – ainakin siinä mielessä, jossa *Robert Alexy* sen esittää. Toisin sanoen voisi todeta oikeuden tiedolliseen yksityisyyteen olevan tavoite, jonka saavuttamista on suojeltava ja tuettava, kunhan sen saavuttamisen edistäminen ei johda vakavammin muihin arvokkaisiin yksilöllisiin tai kollektiivisiin tavoitteisiin puuttumiseen. Yksityisyys abstraktina periaatteena kattaa kaiken manuaalisen, automaattisen ja tietoteknisen henkilötietojen käsittelyn.[53] Tästä syystä on hyvä ymmärtää, että vaikka tietosuojalla pyritään takaamaan yksilöiden yksityisyys, ei yksityisyyden käsitteellistämiseen tule takertua. Mielestäni selkeänä lopputulemana voidaankin pitää yksityisyyttä sellaisena asiantilana, jota kukin omalla tahollaan voisi kuvitella. Kun yksilöiden yksityisyyttä lähdetään toteuttamaan tietosuojan kautta, tuleekin pohtia sitä, minkä tasoista yksityisyyttä kulloisessa tilanteessa yksilö voisi kohtuudella odottaa. Jos osallistun esimerkiksi kilpailuun jättämällä yhteystietoni,

[50] Nissenbaum, 2015, s. 153–163.
[51] Mahkonen, 1997, s. 16. Neuvonen ei täysin hyväksy Mahkosen näkemystä. Eristäytyminen ja yksityisyys sosiaalisuuden vastakohtana tarkoittaa sitä, että yksityisyys edellyttäisi aktiivista toimintaa ja näin ei tule olla. Ks. Neuvonen, 2014, s. 30.
[52] Neuvonen, 2014, s. 29.
[53] Alexy, 2003, s. 436–438. Ks. myös Sartor, 2017, s. 441.

olettaisin itse lähtökohtaisesti esimerkiksi sitä, että minulle ei jatkossa tule satoja soittoja vuodessa liittyen markkinointitarkoituksiin. Kyse on pitkälti siitä, miten tietojen käsittelystä on informoitu, sillä oikein informoituna tällainen ei ole TSA:n vastaista.

Yksityiselämän suoja on turvattu Suomen perustuslailla (731/1999). Perustuslain 10 §:n 1 momentin mukaan *jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla*. Säädöstekstissä on otettu huomioon niin Euroopan ihmisoikeussopimuksen 8 artiklan kuin kansalaisoikeuksia ja poliittisia oikeuksia koskevan kansainvälisen yleissopimuksen (KP-sopimuksen) 17 artiklan sanamuoto. Lähtökohtana yksityiselämän suojaamisessa voidaan pitää tavoitetta yksilön oikeudesta elää omaa elämäänsä ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista tämän yksityiselämään. Yksityiselämän piirin määrittäminen on nähty hankalaksi, mutta siihen voi kuulua esimerkiksi yksilön oikeus solmia ja ylläpitää vapaasti suhteita muihin ihmisiin ja ympäristöön sekä oikeus määrätä itsestään.[54] Kuten johdannosta voidaan huomata, eivät yksityiselämän suojaan kohdistuvat loukkaukset ole itsestään selviä. Hyväksymme ne vain osana arkea. Absoluuttista tilannetta täydellisestä yksityisyyden saavuttamisesta onkin mahdotonta saavuttaa, mikä jokaisen on jossain määrin hyväksyttävä.

Kuten edellä käy ilmi, yksityisyyttä pidetään vahvana itseisarvona. Tämä pätee myös tietojen suojaamiseen. Yksilön suojaa ja oikeuksia tietojenkäsittelyssä on tapana kuvata käsitteellä yksityisyyden suoja. Tätä käsitettä käytetään toisinaan samassa merkityksessä kuin käsitettä yksityiselämän suoja.[55] Yksityisyyden suojaan kuuluu myös yksilön oikeus tietää itseään koskevien tietojen käytöstä, kuten myös oikeus päättää näiden tietojen käytöstä.[56] Yksityisyyden suojaa toteutetaan esimerkiksi säätämällä tutkimuksen kohteena olevan sisäänrakennetun ja oletusarvoisen tietosuojan kaltaisia mekanismeja, jotka tosiasiassa suojaavat yksilöä tietojen käsittelyssä. Aiheen kannalta on syytä huomata se, että tietojen käsittelyn suojaaminen lukeutuu saman suojan piiriin, kuin esimerkiksi kotirauha.

2.1.2. Henkilötietojen suoja, henkilötieto ja tietosuoja

Tietosuojasta käytetään englannin kielessä termiä *data protection*.[57] Käsite on kansainvälisesti vakiintunut puhuttaessa henkilötietojen oikeudellisesta sääntelystä. Lain tasoisella säännöksellä tietosuojan käsitettä ei ole kuitenkaan määritelty. Myöskään tietosuoja-asetuksessa käsitettä ei ole tarkemmin määritelty. Suomessa tietosuojan käsitteestä on puhuttu laajasti jo ennen

[54] KM 1992:3, s. 292; HE 309/1993 vp., s. 52–53 ja HE 184/1999 vp., alajakso 2.1.
[55] Karapuu, 1972, s. 1.
[56] Saarenpää, 2012, s. 240.
[57] Ks. tietosuoja käsitteen kansainvälisestä kehityksestä Bygrave, 2002, s. 4–5, s. 93–95 ja s. 247–249.

tietosuoja-asetuksen aikaa.[58] Suomessa tietosuojalla on yleensä viitattu henkilörekisterilain (471/1987) ja henkilötietolain yhteydessä niihin säännöksiin, jotka määrittelevät henkilötietojen käsittelyyn liittyviä oikeuksia ja velvollisuuksia.[59] Tietosuojalla pyritään turvaamaan tiedon kohteen eli rekisteröidyn luonnollisen henkilön yksityisyyttä, oikeutta ja etuja suhteessa rekisterinpitäjään. Tietosuoja on keino näiden rekisteröityjen henkilötietojen suojaamiseksi.[60]

Tietosuojalainsäädännöllä toteutetaan henkilötietojen suojaa. Henkilötietojen suoja on yksilön, tämän yksityisyyden ja tiedollisen itsemääräämisoikeuden suojaamista tietosuojalainsäädännön avulla. Saarenpään mukaisesti tietosuojalainsäädäntö suojaa yksilöitä ja heidän perusoikeuksiaan henkilötietojen käsittelyn avulla toteutettavaa informaatioväkivaltaa vastaan.[61] TSA 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. Euroopan ihmisoikeustuomioistuin (EIT) on myös omaksunut käytännössään, että perusoikeuskirjan 7 ja 8 artikloilla taattu oikeus yksityiselämän suojaan koskee henkilötietojen käsittelyssä kaikkia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja.[62]

On hyvä huomioida, että henkilötieto ei rajaudu pelkästään kirjalliseen muotoon. Myös tieto, joka on esimerkiksi suullisesti ilmaistu eikä siten tallennettu, on myös asetuksen tarkoittama henkilötieto. Henkilötietojen käsittelyllä taas viitataan kaikenlaisiin henkilötietoihin kohdistuviin toimenpiteisiin alkaen tietojen keräämisestä aina niiden tuhoamiseen asti. TSA:n tarkemman määritelmän mukaan kyse on toiminnoista, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin joko automaattista tietojenkäsittelyä käyttäen tai manuaalisesti. Nämä toiminnot sisältävät 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.[63] Vielä tämäkään luettelo ei ole tyhjentävä. Tärkeintä on huomata, että sääntely kattaa tietojen elinkaaren koko matkan.

[58] Ks. tietosuojan käsitteestä Suomessa Saarenpää, 1994, s. 158–159.
[59] Konstari, 1992, s. 13 ja Wallin – Konstari, 2000, s. 44–45.
[60] Ks. Wallin – Konstari, 2000, s. 45.
[61] Ks. Saarenpää, 2002c, s. 319–320 ja Saarenpää, 2015, s. 325–326.
[62] Ks. Amann v. Sveitsi, no. 27798/95, kohdat 68–81 ja Rotaru v. Romania, no. 28341/95, kohdat 45–63.
[63] TSA 4 artiklan 2 kohta.

Kritiikkiä henkilötiedon käsitteestä on esitetty paljon. On esitetty, että tarvitaan TSA:ta tiukempia määritelmiä siitä, mikä lasketaan henkilötietoihin. Tällä hetkellä TSA:ta ei esimerkiksi sovelleta anonymisoituihin tietoihin. Tuskin soveltamisalaa tullaan ikinä laajentamaan anonymisoituihin tietoihin. Liian usein anonyymeiksi luultavat tiedot päätyvät helposti uudelleen tunnistettaviksi ja siten henkilötiedoiksi[64]. Osa ongelmaa on myös se, että emme ole varmoja siitä, mitä tekniikoita tulevaisuudessa voidaan kehittää ja käyttää henkilöiden tunnistamiseen uudelleen "nimettömässä" tietokannassa. Siksi meillä tulisi olla mielikuvitusta, jotta voimme määritellä, mikä lasketaan henkilötiedoksi.[65] Toisaalta muita kuin henkilötietoja olisi kyettävä jakamaan laajalti yhteistyön ja innovoinnin edistämiseksi. Tietojenkäsittelytieteilijä *Nigel Shadbolt* ja taloustieteilijä *Roger Hampson* ovat esittäneet yhtenä vaihtoehtona tietojen jakamisen yhdistelmäksi "avointa julkista dataa" ja "turvattua yksityistä dataa".[66] Henkilötiedon käsitteen abstraktisuus edellyttää syvempää tarkastelua tieteen keinoin. Tässä tutkielmassa keskeisenä pidän sitä, että henkilötiedon käsite tulee käsittää laajasti. Jos tilanne edellyttää arviointia siitä, lukeutuuko kyseinen tieto henkilötiedon käsitteen alle, tulee siten ensimmäisenä toimenpiteenä ja lähtökohtana pitää sitä, että se on henkilötieto TSA:n merkityksessä.

Henkilötietojen suoja Suomessa on perustuslaissa turvattu perusoikeus. Henkilötietojen suoja ilman nimenomaista perustuslain pykälää lukeutuu oikeushyvänä yksityiselämää suojaavan perusoikeuden alle.[67] Henkilötietojen suoja on siten yksi yksityiselämän suojan osa-alueista. Henkilötietojen suoja ei ole pelkästään osa yksityisyyden suojaa, vaan se kattaa sitä laajemman alan. Suojaa voivat nauttia myös sellaiset henkilöä koskevat henkilötiedot, jotka eivät sellaisinaan kuuluisikaan yksityiselämän alaan.[68] Henkilötietojen suojan lukeutuminen osaksi yksityiselämän suojan piiriä rajoittaa jossain määrin lainsäätäjän liikkumavaraa henkilötietojen käsittelyn säätämisessä. Selvää on kuitenkin se, että lainsäätäjän tehtävänä on turvata henkilötietojen suoja tavalla, jota voidaan pitää perusoikeusjärjestelmä kokonaisuutena huomioon ottaen hyväksyttävänä.[69]

Perusoikeudet ovat kokonaisuus, joka saattaa antaa perusoikeussuojaa sellaisillekin oikeuksille, jotka ovat seurausta useiden perusoikeussäännösten yhteisvaikutuksesta.[70] Valtiosääntöperiaatteiden ja perusoikeusjärjestelmän itsessään voidaan katsoa muodostavan sellaisen

[64] Ks. Malin – Sweeney, 2000.
[65] Véliz, 2020, s. 129–130.
[66] Shadbolt – Hampson, 2019, s. 318.
[67] Jyränki, 2000, s. 301
[68] Korpisaari, ym., 2018, s. 5.
[69] PeVL 14/2018, s. 8.
[70] KM 1992:3, s. 382–384 ja PeVL 14/2002, s. 2.

kokonaisjärjestelmän, jossa perusoikeuksia ei tarkastella toisistaan irrallisten oikeuksien muodostamana kokonaisuutena vaan yhtenäisenä järjestelmänä.[71]

Henkilötietojen suoja käsittää yksilön persoonallisuuden, ja siihen yhdistetään tiedollinen itsemääräämisoikeus. Kantavana ajatuksena on yksityiselämän suoja. Henkilötietojen suoja on oikeudellinen peruskäsite, jota käytetään usein synonyyminä tietosuojan kanssa, vaikka nämä käsitteet eroavat toisistaan. Lakiteknisestä näkökulmasta henkilötietojen suoja on tietosuojalainsäädännön avulla toteutettavaa yksilön perusoikeuksien, usein yksityisyyden, suojaa. Henkilötietojen suoja on ennen kaikkea yksilön suojaa, ei tietojen suojaa.[72] Henkilötietojen suojan kohdalla kysymys on *Saarenpään* mukaan ihmisiä koskevista tiedoista ja ihmisen oikeudesta yksityisyyteen.[73] On syytä pitää mielessä, että henkilötiedot ovat kuitenkin tarpeellisia esimerkiksi hyvinvointivaltion palvelujen tarjoamiseen ja kaupallisiin tarkoituksiin. Yhteiskunnan toiminnan tehostaminen, palveluiden käyttäminen ja tehokas toiminta markkinoilla edellyttävät yksilön luopuvan osasta yksityisyyttään. Henkilötietojen suojan keskeinen tehtävä rakentuu niiden ehtojen järjestämiseen, joiden puitteissa henkilötietoja on sallittua käsitellä.[74] Vaikka tämän tutkielman yhteydessä tuon esille sitä, että henkilötietojen asemaa on syytä korostaa yksilön oikeutena, ei yhteiskunta voi rakentua täydellisen yksityisyyden päälle. Tämä ei myöskään ole yksilön kannalta edes järkevää, sillä liiallinen yksityisyyden korostaminen johtaa toimintavapauden rajoittamiseen.

Henkilötietojen suojan merkityksen kasvu on osoituksena siitä, että yksityisyyttä painotetaan entistä enemmän. Siten henkilötietojen suoja on osa oikeusjärjestelmää, milloin sen tehtävänä on tiedollisen yksityisyyden suojaaminen.[75] Henkilötietojen suojaa itsenäisenä perusoikeutena voidaan pitää siinä määrin hyväksyttävänä, että henkilötietojen suojaaminen osana yksityiselämän suojaa kaventaisi luonnollisen henkilön suojattavien henkilötietojen alaa. Tällöin henkilötiedon käsitettä voitaisiin käsitellä supistavasti eikä alisteisuus yksityisyyden suojalle antaisi riittävää suojaa erilaisiin tietojen käyttötarkoituksiin, kuten tiedonlouhintaan. Tästä syystä henkilötietojen suojan pitämistä itsenäisenä perusoikeutena voidaan pitää oikeutettuna, sillä se ensinnäkin laajentaa mahdollista toimintaympäristöä mutta toisaalta lisää yksilön itsemääräämisoikeutta.[76]

[71] Länsineva, 1998, s. 113.
[72] HE 125/2003 vp., s. 9.
[73] Saarenpää, 1987, s. 203.
[74] Korja, 2016, s. 117.
[75] Ks. Korja, 2016, s. 119.
[76] Pöysti, 1999, s. 487–488 ja Korpisaari, ym., 2018, s. 14. Ks. myös Koillinen, 2013, s. 172.

2.2. Sääntelykehyksestä

2.2.1. Henkilötietojen suojaa koskeva sääntely

Tutkimuksen kohteina olevien seikkojen, kuten yksityisyyden ja henkilötietojen suojan sekä tietoturvan sääntely on pitkälti sidoksissa kansainväliseen lainsäädäntöön. Syynä tälle on teknologian merkitys. Siinä missä kansallisesti säännellään sellaisia asioita kuin maankäyttöä ja ympäristöä, ovat teknologiasidonnaiset seikat sidoksissa rajat ylittävään kehitykseen, jota erityisesti (kompleksissa) globaalissa maailmassa on yksinkertaisempaa säännellä rajat ylittävästi. Näin myös tutkimuksen sääntely aihepiirin ympärillä on kehittynyt hitaasti kansainvälisesti, ja sitä on sittemmin pyritty täsmentämään EU:n tasolla sekä kansallisesti vaadituilta osin.

Kaiken lähtökohtana voidaan pitää YK:n vuoden 1948 Ihmisoikeuksien yleismaailmallista julistusta, jonka 12 artiklassa todetaan, ettei kenenkään yksityiselämään tule puuttua. Tällä voidaan nähdä yhteys julistuksen 19 artiklassa turvattuun sanan ja mielipiteen vapauteen sekä 3 artiklassa turvattuun oikeuteen turvallisuudesta. Ihmisoikeuksien yleismaailmallinen julistus oli selkeä lähtökohta yksilöiden suojelua koskevien normien määrittelemiseksi. Ihmisoikeuksien yleismaailmalliseen julistukseen kirjatut periaatteet ovat tarjonneet perustan myöhemmille eurooppalaisille tietosuojalaeille ja -standardeille. Oikeus yksityiselämään ja siihen liittyviin vapauksiin sisältyy ihmisoikeuksien yleismaailmallisen julistuksen 12 artiklaan:

> *Älköön mielivaltaisesti puututtako kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon älköönkä loukattako kenenkään kunniaa ja mainetta. Jokaisella on oikeus lain suojaan sellaista puuttumista tai loukkausta vastaan*.

Sanamuodosta voitaisiin päätellä, että oikeudet olisivat ehdottomia. Tämä ristiriita on otettu huomioon julistuksen 29 artiklan 2 kohdassa, jossa todetaan, että yksilön oikeudet eivät ole ehdottomia ja että tulee tapauksia, joissa on löydettävä tasapaino eri oikeuksien välillä.

Euroopan integraatio tuotti tulosta, ja vuonna 1950 Euroopan neuvosto kehotti yksittäisiä valtioita allekirjoittamaan Euroopan ihmisoikeussopimuksen, joka on kansainvälinen sopimus ihmisoikeuksien ja perusvapauksien suojelemiseksi. Euroopan ihmisoikeussopimusta sovelletaan vain jäsenmaihin. Kaikki Euroopan neuvoston jäsenvaltiot ovat Euroopan ihmisoikeussopimuksen osapuolia. Euroopan ihmisoikeussopimus on tehokas väline sen suojelemien perus- ja vapausoikeuksien määrän vuoksi. Näiden oikeuksien suojelemiseksi on perustettu Euroopan ihmisoikeustuomioistuin, jossa tutkitaan Euroopan ihmisoikeussopimuksen väitettyjä rikkomuksia. Euroopan ihmisoikeussopimuksen 8 artiklassa sivutaan ihmisoikeusjulistuksen 12 artiklan sisältöä:

> *1. Jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta.*

Tässä artiklassa suojellaan yksityishenkilöiden oikeuksia siten, että heidän henkilötietonsa pysyvät yksityisinä. Vaikka 8 artiklassa käsitellään oikeutta yksityisyyteen, myös sananvapautta koskevassa 10 artiklassa on mahdollistettu yksilöiden yksityisyyden suojaaminen:

> *2. Koska näiden vapauksien käyttöön liittyy velvollisuuksia ja vastuuta, se voidaan asettaa sellaisten muodollisuuksien, ehtojen, rajoitusten ja rangaistusten alaiseksi, joista on säädetty laissa ja jotka ovat välttämättömiä demokraattisessa yhteiskunnassa -- muiden henkilöiden maineen tai oikeuksien turvaamiseksi, luottamuksellisten tietojen paljastumisen estämiseksi --.*

Seuraava askel oli taloudellisen kehityksen ja yhteistyön järjestö OECD:n yksityisyyden suojaa ja kansainvälistä henkilötietojen siirtoa koskeva suositus (OECD:n tietosuojasuositus). Vaikka OECD:n tehtävänä on edistää politiikkaa, jonka tarkoituksena on saavuttaa mahdollisimman kestävä talouskasvu ja työllisyys sekä elintason nousu sekä jäsenvaltioissa että kolmansissa maissa, järjestö laati vuonna 1980 ohjeet yksityisyyden suojasta ja rajat ylittävistä henkilötietojen virroista. Näissä suuntaviivoissa vahvistetaan perussäännöt, jotka säätelevät rajat ylittäviä tietovirtoja sekä henkilötietojen ja yksityisyyden suojaa, mikä helpottaa tietosuojalainsäädännön yhdenmukaistamista jäsenvaltioiden välillä. Koska OECD:n jäsenyys ulottuu Euroopan ulkopuolelle, suuntaviivoilla on kauaskantoinen vaikutus globaalisti. Suuntaviivojen tavoitteena on löytää tasapaino yksilöiden yksityisyyden sekä oikeuksien ja vapauksien suojelun välillä luomatta kaupan esteitä ja sallimalla henkilötietojen keskeytymätön kulku kansallisten rajojen yli. Suuntaviivat ovat puolueettomia käytetyn teknologian suhteen sekä julkisen ja yksityisen sektorin välillä.[77]

1) Keräämisen rajoittaminen: Henkilötiedot on kerättävä oikeudenmukaisesti ja laillisesti ja tarvittaessa yksilön tietämyksellä tai suostumuksella.
2) Tietojen tarkoituksellisuus: Henkilötietojen on oltava merkityksellisiä, täydellisiä, tarkkoja ja ajan tasalla.
3) Tarkoituksen määrittely: Henkilötietojen käyttötarkoitus on ilmoitettava viimeistään tietojen keruun yhteydessä, ja niiden käytön on oltava tämän tarkoituksen määritelmän mukaisia.

[77] Ks. Bygrave, 2014, s. 31–53 ja Korja, 2016, s. 229–235.

4) Käytön rajaus: Henkilötietojen luovuttamisen on oltava täsmällistä määriteltyjen tarkoitusten kanssa, ellei henkilö ole antanut siihen suostumustaan tai rekisterinpitäjällä ole siihen laillisia valtuuksia.
5) Turvatoimet: On otettava käyttöön kohtuulliset turvatoimet riskejä vastaan, kuten henkilötietojen menettämisen tai luvattoman käytön, tuhoamisen, muuttamisen tai luovuttamisen estämiseksi.
6) Avoimuus: Henkilötietojen käyttöön sekä rekisterinpitäjän henkilöllisyyteen ja sijaintiin tulisi olla käytössä yleinen avoimuuspolitiikka.
7) Osallisuus tietoihin: Henkilöllä on oikeus saada rekisterinpitäjältä häntä koskevat henkilötiedot pyydettäessä. Tästä on tullut yksi myöhemmän tietosuojalainsäädännön tärkeimmistä näkökohdista.
8) Vastuu: Rekisterinpitäjän tulisi olla vastuussa edellä mainittujen periaatteiden varmistavien toimenpiteiden noudattamisesta.[78]

Vuonna 1981 allekirjoitettiin yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä.[79] Yleissopimus 108 oli ensimmäinen oikeudellisesti sitova kansainvälinen väline tietosuojan toteutukseen liittyen. Se eroaa tietosuojasuosituksesta siten, että siinä vaaditaan allekirjoittajia ryhtymään tarvittaviin toimiin omassa lainsäädännössään, jotta ne voivat soveltaa henkilötietojen käsittelyssä yleissopimuksen periaatteita. Euroopan neuvosto oli sitä mieltä, että niillä, jotka pitävät ja käyttävät henkilötietoja tietokonemuodossa, on erityisesti sosiaalinen vastuu tällaisten henkilötietojen suojaamisesta, koska tuolloin yksilöihin vaikuttavat päätökset perustuvat yhä enemmän teknisiin tiedostomuotoihin tallennettuihin tietoihin. Yleissopimuksessa todetaan, että sen tavoitteena on lisätä jäsenmaiden yhtenäisyyttä ja laajentaa kaikkien oikeuksien ja perusvapauksien takeita. Yleissopimus on nähty hyvin abstraktina ja laveana pyrkimyksenä kehittää tietosuojakäytäntöjä.[80] Yleissopimus koostuu kolmesta pääosasta, joista 2 luku sisältää aineellista oikeutta koskevia määräyksiä. Luvun 2 periaatteet perustuvat vuosien 1973 ja 1974 Euroopan neuvoston päätöslauselmiin sisältyviin periaatteisiin, jotka ovat monin tavoin samankaltaisia kuin suuntaviivoihin sisältyvät periaatteet.[81] Yleissopimuksen 5 artiklan mukaan automaattisessa tietojenkäsittelyssä käsiteltävien henkilötietojen tulee olla

1) asianmukaisesti ja laillisesti hankittuja ja käsiteltyjä

[78] Rudgard, 2018, s. 7–9.
[79] Suomen osalta yleissopimus on saatettu voimaan säädöskokoelman sopimussarjassa (SopS 36/1992).
[80] Saarenpää, 2002a, kohta 10.
[81] Rudgard, 2018, s. 10–11.

2) määriteltyihin ja laillisiin tarkoituksiin talletettuja, eikä niitä saa käyttää tavalla, joka on ristiriidassa mainittujen tarkoitusten kanssa

3) riittäviä, asiaan liittyviä eivätkä liian laajoja niihin tarkoituksiin nähden, joita varten ne on talletettu

4) oikeita ja tarpeen mukaan ajan tasalla pidettyjä

5) sellaisessa muodossa säilytettyjä, ettei tiedon kohteen yksilöinti ole mahdollista kauemmin kuin mitä vaaditaan siihen tarkoitukseen, jota varten tiedot on talletettu.

Yleissopimuksen 108 ja tietosuojasuosituksen tavoitteena oli ottaa käyttöön yhdenmukainen lähestymistapa tietosuojaan täytäntöönpanoperiaatteesta tehdyllä kansainvälisellä sopimuksella, jonka täytäntöönpano jätettiin jäsenvaltioiden harkintaan. Näiden periaatteiden täytäntöönpano kansallisessa lainsäädännössä johti monipuolisten tietosuojaratkaisujen kehittämiseen. Samalla katsottiin, että yhtenäisen lähestymistavan puuttumisella jäsenvaltioissa näiden periaatteiden hyväksymisessä voisi olla vakavia vaikutuksia yksilöiden perusoikeuksiin, ja se voisi haitata Rooman sopimuksessa[82] vahvistettua unionin alueella tapahtuvaa vapaakauppaa. Sen vuoksi EU:ssa tehtiin työtä yhdenmukaistamisen lisäämiseksi. Kasvava huoli tietosuojalainsäädäntöä koskevien kansallisten lähestymistapojen moninaisuudesta jäsenmaiden kanssa johti ehdotukseen direktiivistä yksilöiden suojelusta henkilötietojen käsittelyssä. Direktiivit ovat jäsenmaita sitova lainsäädäntömuoto, mutta ne jättävät kansallisten viranomaisten valittavaksi täytäntöönpanomuodon ja -menetelmät.[83] Tässä ehdotuksessa Euroopan komissio totesi, että kansallisten lähestymistapojen moninaisuus ja yhteisön tasolla suojelujärjestelmän puute voi olla este sisämarkkinoiden toteuttamiselle. Siten, jos rekisteröidyn perusoikeuksia ja erityisesti hänen oikeuttaan yksityisyyteen ei turvata yhteisön tasolla, ei rajat ylittävä tiedonkulku voi kehittyä.[84] Euroopan komission työn huipentuma oli direktiivi (95/46/EY) yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (tietosuojadirektiivi). Direktiivin tavoitteena oli sovittaa edelleen yhteen yksilöiden perusoikeuksien suojelu ja tietojen vapaa kulku jäsenvaltiosta toiseen ja säilyttää johdonmukaisuus Euroopan ihmisoikeussopimuksen 8 ja 10 artiklan kanssa.[85]

[82] Rooman sopimus allekirjoitettiin 25.3.1957, ja sillä luotiin Euroopan talousyhteisö.
[83] Ks. EU:n lainsäädännön vaikutuksista esimerkiksi Raitio, 2016, s. 195–206.
[84] Ks. Komission ehdotus direktiiviksi yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, perusteluiden kohta 5.
[85] Rudgard, 2018, s. 13–14.

Euroopan parlamentin puhemiehet, neuvosto ja komissio allekirjoittivat ja julistivat Euroopan perusoikeuskirjan toimielintensä puolesta Nizzassa 7.12.2000.[86] Euroopan unionista tehdyllä sopimuksella, Euroopan unionin tuomioistuimen oikeuskäytännöllä[87], Euroopan unionin jäsenvaltion valtiosääntöperinteillä ja Euroopan ihmisoikeussopimuksesta johtuvilla sopimuksilla lujitetaan edelleen EU:ssa sovellettavia perusoikeuksia. Perusoikeuskirja sisältää Euroopan ihmisoikeussopimuksen yleiset periaatteet, mutta siinä viitataan lisäksi henkilötietojen suojaan. Joulukuussa 2009, kun Lissabonin sopimus[88] tuli voimaan, perusoikeuskirja sai sitovan oikeusvaikutuksensa. Perusoikeuskirjan 7 ja 10 artiklassa otetaan huomioon Euroopan ihmisoikeussopimuksen 8 ja 10 artiklan määräykset, ja perusoikeuskirjan 8 artiklassa turvataan oikeus henkilötietojen suojaan:

> *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.*
>
> *3. Riippumaton viranomainen valvoo näiden sääntöjen noudattamista.*

Perusoikeuskirjan 8 artiklassa vahvistetaan tietyt henkilötietojen suojaamisen perusarvot: 1) käsittelyn oikeudenmukaisuus, 2) käyttötarkoitussidonnaisuus, 3) käsittelyn laillisuus, 4) yksilön oikeus omiin henkilötietoihinsa ja tarvittaessa niiden oikaisuun sekä 5) valvontaviranomaisen tulee valvoa sääntöjen noudattamista.[89]

Lissabonin sopimuksen tarkoituksena oli kehittää ja vahvistaa EU:n toimintaa entistä tehokkaammaksi. Lisäksi sopimus sisälsi EU:n kaksi ydinsopimusta, sopimuksen Euroopan unionista (SEU) ja sopimuksen Euroopan unionin toiminnasta (SEUT). SEUT noudattelee EU:n Perusoikeuskirjan 8 artiklan sisältöä, ja SEUT 16 artiklan 1 kohdassa todetaan jokaiselle oikeus henkilötietojen suojaan. Artiklan 2 kohdassa todetaan:

> *Euroopan parlamentti ja neuvosto antavat tavallista lainsäätämisjärjestystä noudattaen luonnollisten henkilöiden suojaa koskevat säännöt, jotka koskevat --*

[86] Nizzan sopimuksella pyrittiin vastaamaan EU:n laajentumisesta aiheutuviin haasteisiin. Sopimus adoptoitiin Suomessa säädöskokoelman sopimussarjaan (SopS 19/2003).
[87] Esimerkiksi tapauksessa C-92/09, Volker und Markus Schecke ja Eifert 9.11.2010 Euroopan unionin tuomioistuin katsoi kohdassa 47, että perusoikeuskirjan mukainen perusoikeus liittyi kiinteästi perusoikeuskirjan 7 artiklassa vahvistettuun yksityiselämän suojaan.
[88] Lissabonin sopimus tuli voimaan kaikkien jäsenvaltioiden ratifioitua sen. Suomessa eduskunta hyväksyi sopimuksen 11.6.2008.
[89] Rudgard, 2018, s. 14–15.

henkilötietojen käsittelyä, sekä säännöt, jotka koskevat näiden tietojen vapaata liikkuvuutta. Näiden sääntöjen noudattamista valvoo riippumaton viranomainen.

Tällä artiklalla varmistetaan, että kaikkien Euroopan unionin toimielinten on suojeltava yksityishenkilöitä henkilötietoja käsitellessään. Perusarvojen, kuten ihmisarvon, vapauden, demokratian, tasa-arvon, oikeusvaltion ja ihmisoikeuksien kunnioittamisen edistäminen on yksi sopimuksen päätavoitteista. Henkilötietojen suojan periaate vahvistettiin Lissabonin sopimuksen myötä. Samalla henkilötietojen suojasta tuli siten yksiselitteisesti EU-oikeuden mukainen perusoikeus.[90]

Vaikka tietosuojadirektiivin piti olla teknologianeutraali, kävi ilmi, ettei se pysynyt nopean teknologisen kehityksen ja globalisaation tahdissa. Tämä ja sen ohella yhdenmukaisen soveltamisen puuttuminen jäsenvaltioiden välillä johti siihen, että Euroopan komissio käynnisti vuonna 2009 tietosuojaa koskevan oikeudellisen kehyksen tarkastelun. Tuloksena oli komission tammikuussa 2012 antama ehdotus tietosuojadirektiivin kattavasta uudistamisesta: yleisessä tietosuoja-asetuksessa säädettäisiin yhtenäisistä säännöistä kaikkialla EU:ssa. Kehitys ei ollut helppo, vaan päinvastoin kyse oli työläästä hyväksymismenettelystä osapuolten kesken. Asetuksen tarkoituksena on maksimoida johdonmukaisuus EU:n jäsenvaltioiden välillä. Tätä helpottaa se, että asetukset ovat suoraan jäsenvaltioita velvoittavia verrattuna direktiiviin. Tietosuoja-asetuksen ohella on kuitenkin huomattava, että jäsenmaat voivat kuitenkin joissakin tilanteissa antaa tarkempia säännöksiä. Tämä tarkoittaa, että jäsenvaltioiden välillä on erilaisia lähestymistapoja tavoissa, joilla tietosuoja-asetuksen täytäntöönpano käytännössä toteutetaan.[91] Tosiasiallisesti näitä eroja on hyvinkin paljon.

Yleisessä tietosuoja-asetuksessa tunnustetaan, että vaikka tietosuojadirektiivin tavoitteet ja periaatteet ovat edelleen vakaat, on se johtanut tietosuojan hajanaiseen täytäntöönpanoon kaikkialla Euroopan unionissa, oikeudelliseen epävarmuuteen ja laajalle levinneeseen yleiseen käsitykseen siitä, että henkilötietojen suojaan liittyy vähäisiä riskejä erityisesti verkkotoiminnan osalta. Teknologian nopea kehitys ja globalisoituminen ovat johtaneet siihen, että yksityiset yritykset ja toimivaltaiset viranomaiset käyttävät henkilötietoja ennen näkemättömällä tavalla. Yleisen tietosuoja-asetuksen tarkoituksena on luoda vahva ja yhtenäinen tietosuojakehys ja täytäntöönpano mahdollisuus. Tällä rakennetaan luottamusta, mikä on edellytys digitaalisen talouden kehittymiselle sisämarkkinoilla. Keskeisiin muutoksiin kuuluvat muun muassa 1) vaatimus tietosuojan huomioon ottamisesta uusia teknologioita kehitettäessä, eli tutkimuksen keskeinen

[90] Ks. De Hert, 2009, s. 11–12.
[91] Rudgard, 2018, s. 16–17.

velvollisuus sisäänrakennetusta- ja oletusarvoisesta tietosuojasta, sekä 2) osoitusvelvollisuuden käsitteen käyttöönotto, jonka avulla organisaatioiden on pystyttävä osoittamaan, että tietosuoja-asetusta noudatetaan.[92]

Suomessa henkilötietojen suoja sisällytettiin perustuslakiin vuoden 1995 perustuslakiuudistuksessa. Säännöksen mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu, ja henkilötietojen suojasta säädetään tarkemmin lailla. Kansallisesti tarkempi lainsäädäntö on vaihtunut muutamaan otteeseen ja nykyään henkilötietojen suojasta säädetään tietosuojalaissa 1050/2018.[93] Perusoikeusuudistuksella tähdättiin siihen, että kansainvälisten sopimusten ihmisoikeusvelvoitteet lisätään kansalliseen perustuslakijärjestelmään erityisesti Euroopan neuvoston ihmisoikeussopimukseen liittymisen vuoksi.[94] Tämä merkitsee sitä, että henkilötietojen suoja on perusoikeustasoinen oikeus.[95]

Perusoikeuksilla on erityisesti vertikaalinen luonne. Niillä pyritään suojelemaan yksilöitä suhteessa julkiseen valtaan. Vaikka tällä vertikaalivaikutuksella onkin keskeinen rooli, ohjaavat perusoikeudet myös horisontaalista kanssakäymistä yksilöiden ja yritysten välillä.[96] Myös perustuslain uudistuksen yhteydessä lainsäätäjän pyrkimys oli parantaa yksityisten mahdollisuutta vedota oikeuksiinsa tukeutumalla perusoikeussäännöksiin.[97] Henkilötietojen suojaan liittyy myös monia muita perusoikeusliittymiä. Yhtenä näistä on perinteisesti pidetty itsemääräämisoikeutta, joka voidaan liittää perusoikeussäännösten muodostamaan kokonaisuuteen. Sitä turvaavat perustuslain säännöksistä erityisesti henkilökohtaista koskemattomuutta, yksityiselämän suojaa ja vapausoikeuksia koskevat säännökset.[98] *Scheinin* onkin luonnehtinut itsemääräämisoikeutta eräänlaiseksi yleisperusoikeudeksi.[99] Henkilötietojen käsittelyssä perusoikeuksien kannalta keskeisessä asemassa ovatkin juuri yksilön itsemääräämisoikeus ja oikeus henkilökohtaiseen vapauden turvaamiseen. Perustuslain 1 §:ssä turvataan yksilön ihmisarvon loukkaamattomuus ja yksilön vapauksien ja oikeuksien.[100] Tästä johtuu, että uudistusten alussa sekä myös nyt käsiteltävänä olevassa yleisessä tietosuoja-asetuksessa yksilöllä tulee olla mahdollisuus vaikuttaa omien tietojensa käyttöön.[101] Mahdollisuus ei ole tietenkään absoluuttinen, sillä

[92] Rudgard, 2018, s. 16–17.
[93] Tietosuojalaki korvasi sitä aikaisemman henkilötietolain. Henkilötietolakia edelsi puolestaan henkilörekisterilaki.
[94] Ks. HE 309/1993 vp., s. 15 sekä Saraviita, 2005, s. 98–99.
[95] Ks. Saraviita, 2005, s. 370 sekä Viljanen, 2001, s. 396–397.
[96] Viljanen, 2001, s. 134–136 ja ks. myös Korhonen, ym., 2004, s.35.
[97] Ks. HE 309/1993 vp., s. 15.
[98] Viljanen, 2001, s. 336.
[99] Scheinin, 2012, s 223.
[100] Ks. Lohiniva-Kerkelä, 2003, s. 138–139.
[101] Ks. KM 1997:9, s. 40.

tietyissä tilanteissa lailla on mahdollista säätää poikkeuksista yksilön mahdollisuuksien käyttämiseen.

Itsemääräämisoikeuden ohella perusoikeusjärjestelmässä myös yksityisyyden suoja on turvattu. Säännöksen sisältö on saanut vaikutteita Euroopan ihmisoikeussopimuksen 8 artiklasta. Yksityiselämän suojan pohjalla on yksilön oikeus elää omaa elämäänsä vapaasti ilman viranomaisten tai muiden ulkopuolisten tahojen mielivaltaista tai aiheetonta puuttumista yksityiselämään.[102] Siihen kuuluu esimerkiksi oikeus määrätä itsestään ja omista toimistaan sekä oikeus vapaasti päättää suhteestaan muihin ihmisiin ja ympäristöön. Kun uutta tietosuojalakia säädettiin Suomessa, myös lain esitöissä todettiin, että perusoikeudet eivät ole aina toisistaan selkeästi erotettavissa, vaan ne ovat päällekkäisiä ja toisiinsa vaikuttavia. Henkilötietojen suojaan vaikuttavia perusoikeuksia on monia, ja edellä esiin nostettujen lisäksi vaikutuksia on uskonnon ja omatunnon vapaudella, sananvapaudella ja julkisuudella.[103] Sekä kansainväliseen että kansalliseen ajatusmaailmaan henkilötietojen suojasta voidaan lukea useita eri vapausoikeuksia. Molemmissa konteksteista huomataan myös, että oikeudet sekoittuvat keskenään, eikä niitä tule ajatella irrallisina konteksteistaan. Tutkimuksen kannalta keskeistä on ymmärtää, että henkilötietojen suoja on sekä kansallisesti että kansainvälisesti tunnustettu perus- ja ihmisoikeus, joka tulee henkilötietoja käsiteltäessä ottaa huomioon. Mielestäni henkilötietojen käsittelyssä tulisi toimia vastaavalla tavalla kuin tuomioistuimessa: tuomioistuimen tulee ratkaisua tehdessään valita ratkaisu, joka parhaiten toteuttaa perusoikeuksien toteutumista. Tarkoitan sitä, että käsillä olevista vaihtoehdoista tulisi valita sellainen, joka parhaiten vastaa perusoikeuksien ja ihmisoikeuksien asettamia vaatimuksia.[104] Henkilötietojen suojassa kyse ei ole siten ainoastaan yhden perusoikeuden vaikutuksesta vaan kokonaisarvioinnista eri tilanteissa.

Viimeisimpänä uudistuksena, vuonna 2018 avattiin allekirjoitettavaksi yleissopimuksen lisäpöytäkirja yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä. Uudistuksesta on puhuttu *yleissopimus 108+*:na. Tarve päivitykselle oli suuri, sillä lähes 40 vuoden aikana teknologinen kehitys sai aikaan uudenlaisia haasteita ihmisoikeuksien toteutumiselle. Yleissopimus 108+ tarkoituksena oli lähtökohtaisesti päivittää aikaisempi yleissopimus 108 vastaamaan yleisen tietosuoja-asetuksen sisältöä. Yleissopimus 108+ sisältää tärkeitä innovaatioita: siinä julistetaan, että on tärkeää suojella oikeutta tiedolliseen itsemääräämisoikeuteen ja ihmisarvon kunnioittamiseen teknologisen kehityksen edessä. Siinä vahvistetaan samalla tietojenkäsittelyn suhteellisuusvaatimusta ja vahvistetaan rekisteröidyn mahdollisuuksia toteuttaa

[102] HE 309/1993 vp, s. 52.
[103] EU:n yleisen tietosuoja-asetuksen täytäntöönpanotyöryhmä TATTI mietintö, s 73.
[104] HE 309/1993 vp, s. 31. Ks. myös PeVL 6/1988 vp ja PeVL 2/1990 vp.

oikeuksiaan. Se vahvistaa tietojenkäsittelystä vastanneiden vastuuta ja avoimuutta. Se edellyttää ilmoitusta tietoturvaloukkauksista, vahvistaa valvontaviranomaisten riippumattomuutta, valtuuksia ja toimintakeinoja. Se myös vahvistaa mekanismia, jolla varmistetaan yleissopimuksen tehokas täytäntöönpano, valtuuttamalla yleissopimuksella perustettu komitea valvomaan osapuolten tekemien sitoumusten noudattamista.[105] Lisäksi yleissopimukseen sisällytettiin käsite sisäänrakennetusta tietosuojasta. Uudistuksessa yleissopimukseen lisättiin TSA:n 25 artiklaa vastaava asianmukaisten teknisten ja organisatoristen toimenpiteiden vaatimus. Mielenkiintoisen yleissopimuksesta tekee se, että siihen voi liittyä myös EU:n ulkopuoliset jäsenvaltiot. Siten henkilötietojen siirtäminen yleissopimuksen ratifioimien valtioiden välillä nauttii osapuolten luottamusta. Yleissopimus 108 on edelleen ainut universaalisesti osapuolia velvoittava oikeudellinen instrumentti, ja siten se on tärkeää ottaa huomioon.[106]

TSA on EU:n tasoinen säädös, jolla on kaikilta osin jäsenvaltiota velvoittava luonne. Johtuen unionin lainsäädännön ensisijaisesta suhteesta kansallisiin säännöksiin perustuslakivaliokunta on katsonut, ettei ole tarvetta säätää lakia kattavasti ja yksityiskohtaisesti yksilöiden turvasta henkilötietojen käsittelyyn. Sinänsä tälle ei ole estettä. Perustuslakivaliokunta onkin katsonut, että yleisen tietosuoja-asetuksen yksityiskohtainen sääntely, jota tulkitaan ja sovelletaan EU:n perusoikeuskirjassa turvattujen oikeuksien mukaisesti, muodostaa riittävän säädöspohjan perustuslain 10 §:n yksityiselämän ja henkilötietojen suojan kannalta.[107]

2.2.2. Ohjeistukset

Henkilötietojen käsittelyyn liittyy hyvin paljon yleispiirteistä, kansainvälistä sääntelyä, josta ei voida johtaa tarkkoja tulkintoja siitä, miten kyseisessä tilanteessa tulisi aina toimia. Tästä syystä on nähty tarpeelliseksi laatia erilaisia ohjeistuksia tietosuojalainsäädännön noudattamiseen liittyen. EU:ssa ensimmäisenä elimenä näitä ohjeistuksia annettiin tietosuojadirektiivin mukaisen tietosuojatyöryhmän (WP29) toimesta. Tietosuojatyöryhmä antoi lukuisia ohjeita ja kannanottoja sääntelyä selkiyttämään. Kuitenkaan WP 29:n mielipiteet eivät olleet velvoittavia. Tässäkin tutkimuksessa tietosuojatyöryhmän kannanottoihin viitataan järjestelmällisesti. Työryhmän tuloksilla on ollut merkittävä vaikutus eurooppalaisissa tietosuojakäytännöissä. Heidän antamiaan kannanottoja käytetään edelleen niiltä osin, kun ei ole tuoreempaa ohjeistusta saatavilla. Tästä syystä niiden merkitys ei ole poistunut, vaikka toimielin yhdenmukaistamisessa onkin vaihtunut.

[105] Ks. De Terwangne, 2021, s. 3–12.
[106] Ibid., s. 16–17.
[107] PeVL 14/2018, s. 3–4 ja PeVL 51/2014, s. 2.

Yleisellä tietosuoja-asetuksella perustettiin Euroopan tietosuojaneuvosto (EDPB). Kyse on riippumattomasta EU:n elimestä, jolla on oikeushenkilön asema[108] ja joka vastaa tietosuojasääntöjen yhdenmukaisesta soveltamisesta kaikkialla Euroopan unionissa ja edistää EU:n tietosuojaviranomaisten välistä yhteistyötä. Tietosuojaneuvosto koostuu kansallisten tietosuojaviranomaisten ja Euroopan tietosuojavaltuutetun edustajista. Tietosuojaneuvoston tavoitteena on varmistaa yleisen tietosuoja-asetuksen ja ns. rikosasioiden tietosuojadirektiivin ((EU) 2016/680) yhdenmukainen soveltaminen EU:ssa. Tietosuojaneuvosto voi antaa yleisiä ohjeita EU:n tietosuojalainsäädännön käsitteiden selventämiseksi, jotta kaikki voivat saavat yhdenmukaisen tulkinnan oikeuksistaan ja velvoitteistaan. Tietosuojaneuvostolle on lisäksi annettu tietosuoja-asetuksella valtuudet tehdä kansallisia valvontaviranomaisia koskevia sitovia päätöksiä yhdenmukaisen soveltamisen varmistamiseksi. Lisäksi tietosuojaneuvosto voi toimia eräänlaisena riidanratkaisuelimenä rajat ylittävissä tapauksissa, joissa kansalliset valvontaviranomaiset eivät pääse yhteisymmärrykseen asian ratkaisusta.[109] Tietosuoja-asetuksen keskeisenä tehtävänä onkin ollut voimaan tultuaan yhtenäistää eurooppalaista tietosuojakäytäntöä. Tässä mielessä tietosuojaneuvoston merkitys eräänlaisena yhden luukun järjestelmänä on merkittävä yhdessä kansallisten valvontaviranomaisten ohella. Tämä *one-stop-shop* (OSS) -mekanismiksi kutsuttu järjestelmä kehitettiin tilanteisiin, joissa henkilötietoja käsitellään useammassa EU:n jäsenvaltiossa.[110]

Toisaalta tietosuojaneuvoston ohjeistukset eivät ole myöskään velvoittavia, mutta sen kompetenssi sitoviin ratkaisuihin riidanratkaisuelimenä tuo sille aikaisempaa enemmän uskottavuutta. Tietosuojaneuvoston roolia TSA:n soveltamisessa on alleviivattu heti alusta pitäen.[111] Sen tehtävänä ei ole antaa suosituksia tai osoittaa parhaita käytäntöjä vaan antaa ohjeistuksia (*guidelines*). Tällä on mitä ilmeisimmin haluttu korostaa näiden kolmen erityyppisen materiaalin antamista siinä mielessä, että niiden velvoittavuus voidaan erottaa toisistaan, vaikka kaikki näistä voidaan oikeuslähdeopillisesti laskea *soft law*'n alle. Näiden ohjeistuksien oikeudellinen asema ei ole täysin selvä toisin kuin hyväksyttyjen käytännesääntöjen, jotka komissio voi hyväksyä TSA 93 artiklan 2 kohdan mukaisessa komiteamenettelyssä. Myös sertifiointimekanismit edellyttävät muodollista hyväksyntää. Oikeudellisessa mielessä on todennäköistä, että tietosuojaneuvoston ohjeistuksia tulee pitää suosituksina tavalla, jolla Euroopan neuvoston virallisia suosituksia pidetään.[112] Kuitenkaan ei ole mielekästä ajatella asiaa niin, etteivätkö sen linjaukset

[108] TSA artikla 68.
[109] TSA artikla 70.
[110] Ks. Talus, 2016, s. 63–81.
[111] Talus, 2016, s. 80–81.
[112] Jay, ym., 2017, s. 25.

merkitsisi käytännössä juuri mitään. Päinvastoin on todettava, että sen yleinen velvollisuus tuottaa ohjeistuksia ja tulkintasuosituksia on keskeistä ja tässä mielessä erittäin relevanttia myös tämän tutkimuksen osalta. Lisäksi tietosuojaneuvoston ohjeistusten merkitys tulisi saada entistä enemmän selväksi kaikille, jotka toimivat tietosuojalainsäädännön parissa.

Euroopan tietosuojaneuvoston antama ohje oletusarvoisesta ja sisäänrakennetusta tietosuojasta on tämän tutkimuksen kannalta keskeisin. Euroopan tietosuojaneuvosto vahvisti lokakuussa 2020 ohjeistuksensa 4/2019 TSA:n 25 artiklan soveltamisesta eli sisäänrakennetusta ja oletusarvoisesta tietosuojasta. Ohjeistus sisältää tietosuojaneuvoston analyysin 25 artiklan sisällöstä ja yleisten tietosuojaperiaatteiden implementoinnista osaksi sisäänrakennettua ja oletusarvoista tietosuojaa. Ohjeistuksessa todetaan, että periaatteet ovat toisiaan täydentäviä ja että periaatteet ovat osa rekisterinpitäjän velvollisuutta riippumatta sen koosta.[113] Asianmukaisilla toimenpiteillä ja tarvittavilla suojatoimilla pyritään suojaamaan rekisteröidyn oikeuksia ja varmistamaan, että hänen henkilötietojensa riittävä suoja on osa henkilötietojen käsittelyä.[114]

Ohjeistuksessa avataan muun muassa 25 artiklan avainkäsitteitä. Esimerkiksi termillä *state of the art* viitataan rekisterinpitäjien velvollisuuteen ottaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä määrittäessään jatkuvasti huomioon markkinoilla saatavilla oleva teknologian nykyinen kehitys. Lisäksi rekisterinpitäjien on tiedostettava ja pysyttävä ajan tasalla teknologisesta kehityksestä. Velvollisuus ei koske pelkästään teknisiä toimenpiteitä, vaan kyse on myös organisatorisista toimenpiteistä.[115] Ohjeistusta käytetään tässä tutkimuksessa selventämään lainsäätäjän näkemystä 25 artiklan tulkinnasta.

2.3. Yleiset tietosuojaperiaatteet sisäänrakennetun ja oletusarvoisen tietosuojan lähtökohtana

2.3.1. Yleistä

Oikeudellistuvan verkkoyhteiskunnan kehitys on johtanut riskiyhteiskuntaan, jossa digitaalinen toimintaympäristö aiheuttaa riskejä yksilön oikeuksille. Tämän taustalla *Saarenpää* pitää tietämättömyyttä digitalisaation vaaroista tai välinpitämättömyyttä henkilötiedon merkittävyydestä.[116] TSA:n 5 artiklassa määritellään henkilötietojen käsittelyä koskevat yleiset periaatteet.[117] TSA:ssa ei ole pyritty ehdottomiin ja liian tarkkarajaisiin säädöksiin, joilla pyrittäisiin

[113] Tietosuojaneuvoston ohjeistus 4/2019, kohta 5.
[114] Tietosuojaneuvoston ohjeistus 4/2019, kohta 7.
[115] Tietosuojaneuvoston ohjeistus 4/2019, kohdat 19 ja 21.
[116] Ks. Saarenpää, 2016, s. 81–82 ja s. 125–128.
[117] Näistä periaatteista voidaan käyttää toistensa synonyymeinä useita eri variaatioita. Itse käytän termiä yleiset tietosuojaperiaatteet siksi, että käsitteellä ne voidaan erottaa selkeämmin muista tietosuojaan liittyvistä

sääntelemään yksittäisiä asioita liian tarkasti. Tästä syystä periaatteilla on haluttu luoda joustava rakenne, joka mahdollistaa asetuksen soveltamisen kaikkiin tilanteisiin, joissa henkilötietoja käsitellään. Tässä mielessä yksittäiset vaikeat säännökset voivat tulla ymmärretyiksi periaatteiden avulla.[118] Sisäänrakennetun ja oletusarvoisen tietosuojan osalta on keskeistä, että yleiset tietosuojaperiaatteet ja niiden vaatimukset sisällytetään jo varhaisessa vaiheessa osaksi henkilötietojen käsittelyä.[119] Lisäksi rekisterinpitäjän tulee myös TSA 5 artiklan 2 kohdan mukaisesti pystyä osoittamaan, että yleisiä tietosuojaperiaatteita on noudatettu.

Yleiset tietosuojaperiaatteet on jaettu TSA 5 artiklassa seitsemään kohtaan. Periaatteet voidaan jakaa: 1) käsittelyn lainmukaisuuden *(lawfulness)*, kohtuullisuuden *(fairness)* ja läpinäkyvyyden periaatteeseen *(transparency)*, 2) käyttötarkoitussidonnaisuuden periaatteeseen *(purporse limitation)*, 3) tietojen minimoinnin periaatteeseen *(data minimisation),* 4) tietojen täsmällisyyden periaatteeseen *(accuracy),* 5) tietojen säilytyksen rajoittamisen periaatteeseen *(storage limitation)*, 6) tietojen eheyden ja luottamuksellisuuden periaatteeseen *(integrity and confidentiality)* ja 7) rekisterinpitäjän osoitusvelvollisuuteen ja asetuksen noudattamisvaatimukseen *(accountability and compliance)*.[120] Periaatteiden ymmärtäminen jokapäiväisessä ja arkisessa toimintaympäristössä on merkityksellistä. Vaikka TSA:n vastuuasema kohdistuukin rekisterinpitäjään tulisi mielestäni jokaisen pystyä toimimaan myös digitaalisessa ympäristössä henkilötietoja kunnioittaen. Kyse on siten omien rutiinien ja päivittäisten toimintojen riskikartoituksesta, mikä jatkuvana prosessina ennaltaehkäisee vääriä toimintatapoja. Rekisterinpitäjän vastuulla on antaa ohjeita tietojen käsittelystä, mutta on kuitenkin ymmärrettävä, että jokaisella on velvollisuus huolehtia siitä, että myös itse käsittelee tietoja järkevästi ja miettii kunkin toimenpiteen perimmäistä merkitystä tässä ketjussa. Periaatteiden merkitystä ei voida ylikorostaa. Syytä on huomioida, että periaatteiden rikkomisesta voidaan TSA:n 83 artiklan 5 kohdan perusteella määrätä hallinnollinen seuraamusmaksu, joka on enintään 20 miljoonaa euroa tai yritysten kohdalla enintään neljä prosenttia sen maailmanlaajuisesta kokonaisliikevaihdosta. Tämä jos mikä laittaa pohtimaan tietosuojaperiaatteiden noudattamista. Esimerkiksi Italian tietosuojaviranomainen (*Garante per la protezione dei dati personali*) on antanut lähes 17 miljoonan euron seuraamusmaksun tapauksessa, jossa viranomainen katsoi telekommunikaatioyrityksen rikkoneen yleisen tietosuoja-asetuksen 25 artiklaa. [121] Tapauksessa kyse oli muun muassa

periaatteista. Teoksessa Korpisaari, ym., 2018 käytetään termiä *tietosuojaperiaatteet*. Englanniksi puhuttaessa käytetään myös termejä *Data Protection Principles* tai *Data Quality Principles*, ks. Lambert, 2017. Bygrave on käyttänyt lisäksi aikaisemmin ennen yleistä tietosuoja-asetusta tietosuojan ja yksityisyyden ydinperiaatteista termiä *Core Principles of Data Privacy Law*, ks. Bygrave, 2014, s. 163–164.

[118] Korpisaari, ym., 2018, s. 23–24.

[119] Alapuranen, ym., 2020, s. 67.

[120] Ks. IT Governance Privacy Team, 2017, s. 100–119.

[121] Ks. tapaus *Garante v. Wind Tre S.p.A*.

menetelmistä, joilla kerätään ja peruutetaan suostumus. Tietosuojaviranomainen katsoi, että rekisterinpitäjän toimenpiteet olivat virheellisiä, sillä niissä kannustettiin keräämään myynninedistämistarkoituksessa henkilötietoja, vaikka rekisteröidyt vastustivat tietojen keräämistä.

2.3.2. Lainmukaisuus, kohtuullisuus ja läpinäkyvyys

TSA 5 artiklan 1 kohdan a alakohdan mukaan henkilötietoja on käsiteltävä lainmukaisesti, asianmukaisesti ja rekisteröidyn kannalta läpinäkyvästi. Lainmukaisuusperiaatteella viitataan yksiselitteisesti siihen, että käsittelylle on oltava lain mukainen peruste ja *ex analogia* henkilötietojen käsittely on kiellettyä ilman sellaista perustetta.[122] Perusteita ovat suostumus, sopimuksen täytäntöönpano, rekisterinpitäjän lakisääteisen velvoitteen noudattaminen, elintärkeiden etujen suojaaminen, yleistä etua koskevan tehtävän suorittaminen tai rekisterinpitäjälle kuuluvan julkisen vallan käyttäminen sekä oikeutettujen etujen toteuttaminen.[123] Lainmukaisuuden vaatimukseen sisältyy myös lähtökohtainen kielto käsitellä erityisiä henkilötietoryhmiä[124].[125] Kansallisesti jätettyä liikkumisvaraa varten tietosuojalain 2 lukuun on osittain sisällytetty täsmentäviä perusteita esimerkiksi yleistä etua koskevia tilanteita varten. Myös erityislaeista löytyy tarkentavia perusteita.[126] Lainmukaisuusperiaatteen mukaisia arvoja voivat olla merkityksellisyys, eriyttäminen, määritelty tarkoitus, välttämättömyys, autonomia, suostumuksen saaminen, suostumuksen peruuttaminen, etujen tasapainottaminen, käsittelyn ennalta määritteleminen ja mukauttaminen.[127]

Tässä yhteydessä TSA:n asianmukaisuusvaatimus (kohtuullisuus) tarkoittaa eräänlaista reiluutta, varsinkin englanninkielisessä merkityksessä (*fairness*). Sanamuodon voidaan ajatella tarkoittavan sitä, että rekisterinpitäjä ottaa myös huomioon vastapuolen edut ja odotukset. Samalla kyse on reiluudesta siinä mielessä, että rekisteröity saa tiedot henkilötietojen käsittelystä TSA 13 artiklan mukaisesti.[128] Tietoja ei myöskään saa käsitellä epämääräisesti, vaan käsittely vaatii suhteellisuutta ja tietynlaista tasapainoa.[129] Kyse on siten eräänlaisesta lojaliteettivelvoitteesta, joka on bilateraalinen. Siinä missä rekisteröity luottaa reiluuden hengessä tietojaan rekisterinpitäjälle, on tämä velvollinen myös näitä tietoja käsittelemään reilusti. Tässä mielessä

[122] Ks. Voigt – Von dem Bussche, 2017, s. 87.
[123] TSA artiklat 6 ja 9–11. TSA 6 artiklan mukaisesti käsittely on lainmukaista vain ja ainoastaan jos yksi edellytyksistä täyttyy.
[124] Vrt. arkaluonteisten henkilötietojen ryhmä.
[125] Korpisaari, ym., 2018, s. 89–90.
[126] Ibid., s. 89.
[127] Tietosuojaneuvoston ohjeistus 4/2019, kohta 68.
[128] Korpisaari, ym., s. 90. Myös Euroopan unionin tuomioistuin on asiassa C-496/17, Deutche Post AG c Hauptzollant Köln kohdassa 59 todennut asianmukaisuuden vaatimuksen sisältävän velvollisuuden rekisteröidylle ilmoittamisesta.
[129] Bygrave, 2001, s. 1.

henkilötietojen käsittely ei myöskään saa osoittautua rekisteröidyn kannalta ennalta arvaamattomaksi.[130] Keskeisiä elementtejä suunniteltaessa kohtuullisuutta voivat olla riippumattomuus, vuorovaikutus, odotukset, syrjimättömyys, hyödyntämättömyys, kuluttajien valinta, voimatasapaino, eettisyys, totuudenmukaisuus ja oikeudenmukaiset algoritmit.[131]

Läpinäkyvyyden vaatimus on TSA:n tuomia uusia velvoitteita rekisterinpitäjälle.[132] Samalla se on mielenkiintoinen periaate, sillä lähtökohtaisesti rekisteröity ei pysty tosiasiallisesti itse valvomaan henkilötietojen käsittelyä. Läpinäkyvyyden periaatteen myötä rekisteröityä tulee informoida rekisterinpitäjän prosessista henkilötietojen käsittelyssä. Läpinäkyvyydellä pyritään siihen, että rekisteröity saa tietoonsa selvästi ja ymmärrettävästi kaikki häntä koskevat tiedot, joita rekisterinpitäjällä on sekä sen, miten niitä käytetään tai mitä niitä yhdistelemällä tuotetaan. Tämä mahdollistaa luonnollisen henkilön reagointimahdollisuuden.[133] Reagointimahdollisuudessa kyse on esimerkiksi TSA 15 artiklan tarkastusoikeuden käyttämisestä. Läpinäkyvyydessä on kyse siten tietojenkäsittelyn avoimuudesta. Avoimuus on puolestaan yhteydessä yksilön itsemääräämisoikeuteen esimerkiksi juuri rekisteröidyn tarkastusoikeuden näkökulmasta. Tarkastusoikeuden käyttäminen antaa yksilölle vaikuttamismahdollisuuden valvoa itseään koskevien tietojen käsittelyä. Etukäteisellä viestinnällä vältytään siten tilanteilta, joissa rekisteröity vasta myöhemmin saa yllättäen tietää henkilötietojen käsittelyn käytänteistä. Periaate edellyttää myös sitä, että informaatio tietojenkäsittelystä on helposti saatavilla ilman pitkää tiedon etsimistä esimerkiksi siten, että se on asetettu internetsivuille.[134] Läpinäkyvyysperiaatteen keskeisiä suunnitteluelementtejä voivat olla selkeys, semantiikka, saavutettavuus, asiayhteys, merkityksellisyys, universaali suunnittelu, ymmärrettävyys, monikanavaisuus ja kerrostettu rakenne.[135]

Yhtenä tärkeänä elementtinä läpinäkyvyyden olemassaolosta on se, että sekä rekisterinpitäjä ja henkilötietojen käsittelijä käyttää kommunikaatiossa ymmärrettävää kieltä siten, että rekisteröity saa siitä helposti selon.[136] Tämä toteutuu siten, että tietojen prosessointi kuvataan havainnollistavalla tavalla ja tiedot pidetään helposti saatavilla. Kielenkäytössä tulee myös huomioida kohderyhmä – esimerkiksi, kun tietojen käsittelyä kohdistetaan lapsiin, tulee kielenkäytössä huomioida erityisesti ymmärrettävyys.[137] Toisaalta läpinäkyvyys estää valta-asemasta johtuvaa

[130] Tietosuojavaltuutetun toimisto, Lainmukaisuus, asianmukaisuus ja läpinäkyvyys.
[131] Tietosuojaneuvoston ohjeistus 4/2019, kohta 70.
[132] Läpinäkyvyyden vaatimus on täysin uutta eurooppalaisessa yhteydessä. Suomessa periaate omaksuttiin jo henkilötietolaissa henkilötietojen käsittelyä ohjaavaksi esimerkiksi rekisteriselosteen muodossa.
[133] Näin myös TSA:n johdanto-osan 39 perustelukappaleessa.
[134] Korpisaari, ym., 2018, s. 90–91.
[135] Tietosuojaneuvoston ohjeistus 4/2019, kohta 66.
[136] TSA johdanto-osan 58 perustelukappale. Ks. myös Voigt, 2017, s. 88.
[137] Ks. WP 260, s. 10.

epätasapainoa rekisteröidyn ja rekisterinpitäjän välisessä suhteessa. Lisäksi rekisterinpitäjä on velvollinen antamaan luonnolliselle henkilölle tietoja käsittelystä mutta myös käsittelyyn liittyvistä säännöistä, suojatoimista ja oikeuksista sekä niiden käyttämismahdollisuuksista. Samalla kun rekisterinpitäjä toimii näin, se luo itselleen tilannekuvaa omista käsittelytoimistaan ja helpottaa työtaakkaansa osoitusvelvollisuuden suhteen.

Kootusti näen tämän periaatteen olevan se työkalu, josta tietojenkäsittely lähtee liikkeelle. Toisaalta periaatteet ilmentävät myös rekisterinpitäjän mahdollisuutta hyödyntää uusia ja innovatiivisia keinoja viestinnässä. Käsittelyä ei saa toteuttaa niin, että tietoja kerätään sieltä ja täältä, päättyen siihen, että ne kulkevat rutiininomaisen tehdaslinjaston lävitse päätyen tehtaasta ulos. Päinvastoin jokaisen tietoyksikön kohdalla tulisi pysähtyä ja miettiä: 1) Onko tämän tietoyksikön käsittelylle olemassa oleva lainmukainen käsittelyperuste? 2) Onko tämä tieto merkityksellistä ja välttämätöntä kerätä juuri tätä tarkoitusta varten? 3) Vastaako tämän tiedon kerääminen rekisterinpitäjän näkyvää viestintää henkilötietojen käsittelystä? Esimerkiksi tietosuojavaltuutettu on katsonut ratkaisukäytännössään, että työnhakijalta ei ole syytä kerätä toimenhakulomakkeella syntymäkuntaa, seurakuntaa, perhesuhteita, asuntoa, puolison nimeä, puolison ammattia, puolison työpaikkaa, lasten syntymävuosia, terveydentilaa ja mahdollista raskautta koskevia henkilötietoja. Yksiselitteisesti tällaisten tietojen kerääminen on lainvastaista. Tällöin myöskään rekisterinpitäjä ei ole suorittanut asianmukaisia teknisiä ja organisatorisia toimenpiteitä asetuksen noudattamiseksi.[138]

Sisäänrakennetun ja oletusarvoisen tietosuojan kohdalla on tärkeää toteuttaa läpinäkyvyyden, kohtuullisuuden ja lainmukaisuuden periaatteita pintatasoa syvemmällä, toisin sanoen ilman sanahelinää. Esimerkiksi on turhaa viestiä rekisteröidyille, että heidän henkilötietojaan arvostetaan, jos henkilötietoja ei suojata asianmukaisesti. Läpinäkyvyyteen liittyy myös se, että tietojärjestelmät tarjoavat rekisteröidylle mahdollisuuden saada yksinkertaisessa muodossa kaiken informaation. Järjestelmien suunnittelu niin, että ne tarjoavat rekisteröidylle mahdollisuuden saada yksinkertaisessa muodossa kaiken informaation, voi johtaa myös positiiviseen yrityskuvaan. Tässäkin yhteydessä kyse on lopulta hyvin yksinkertaisista seikoista. Rekisterinpitäjän tulee tietää, mitä saa kerätä ja millä edellytyksillä sekä tehdä keräämisen ja tietojen hyödyntämisen välisestä korrelaatiosta dynaaminen kokonaisuus, jossa otetaan myös rekisteröidyn edut huomioon. Kun lisäksi viestitään kohderyhmän tasolla oikeaoppisesti tietojen käsittelystä, on tätä periaatekokonaisuutta noudatettu. On tärkeää ymmärtää, että kaikille henkilötietojen käsittelyn prosessi ei ole selvää.

[138] Tietosuojavaltuutetun ratkaisu TSV 18.5.2020.

2.3.3. Käyttötarkoitussidonnaisuus

Sisäänrakennetun ja oletusarvoisen tietosuojan vaatimus ilmentää eräänlaista suunnitelmallisuutta. Henkilötietojen käsittelyn tulee olla perusteltua rekisterinpitäjän toiminnan kannalta. Käsittelyn tarkoitukset ja periaatteet on määriteltävä etukäteen ennen niiden muodostumista tietojenkäsittelyn kokonaisuudeksi. Tietosuojalainsäädännön keskeinen periaate onkin, että henkilötietoja käsitellään vain ennalta määriteltyjen tarkoitusten mukaisesti, ja käsittelylle tulee olla perusteltu tarve.[139] Kun luonnollisista henkilöistä kerätään tietoja, ne kerätään tiettyyn käyttötarkoitukseen. Tämän käyttötarkoituksen ulkopuolelle näitä tietoja ei saa ilman muuta yhteensopivaa käyttötarkoitusta käsitellä. Käyttötarkoitussidonnaisuus ei siten ole ehdoton, sillä TSA:ssa on tiettyä liikkumavaraa tilanteisiin, joissa käsittelylle on yhteensopiva käyttötarkoitus. Käyttötarkoitussidonnaisuuteen lukeutuu siten henkilötietojen kerääminen tiettyä, nimenomaista ja laillista tarkoitusta[140] varten, ja se, että niitä ei saa käsitellä myöhemmin alkuperäisen tarkoituksen kanssa yhteensopimattomalla tavalla.[141] Sanamuodossa käytetyt ilmaisut tietystä ja nimenomaisesta käyttötarkoituksesta viittaavat pitkälti siihen, että käyttötarkoitus on ennalta selvillä ennen tietojen keräämistä. Käyttötarkoitus onkin ilmaistava viimeistään tietojen keräämishetkellä. Tällä tulkinnalla saavutetaan ainakin TSA:n mukaiset tavoitteet.[142] Käyttötarkoitussidonnaisuus estää keräämästä tietoa muihin kuin ennalta määriteltyihin käyttötarkoituksiin. Tietosuojatyöryhmän ohjeessa pidetään siten tietojen keräämistä yksistään esimerkiksi markkinointitarkoituksiin, IT-turvallisuuden tarkoituksiin tai tulevaisuudentutkimusta varten epätäsmällisinä käyttötarkoituksina.[143] Tällainen määrittely ei ole riittävän täsmällistä käyttötarkoitussidonnaisuuden periaatteen mukaisesti. Keräämisen peruste tulee yksilöidä esimerkiksi uutiskirjeen muodossa.

Käyttötarkoitussidonnaisuus edellyttää tietojen käsittelijältä sitä, että tämä etukäteen määrittää tiedon käyttötarkoituksen ja sittemmin rajoittaa käsittelyn vain tätä tarkoitusta varten ilman laajentavaa tietojen käsittelyä. Etukäteisen käyttötarkoituksen valinnalla voidaan siten myös toteuttaa läpinäkyvyyden vaatimusta ilmoittamalla tietojen käsittelystä tietojen keräämisvaiheessa.[144] Useasti tietoja saatetaan kerätä *varmuuden varalta*, vaikka ne eivät edes liittyisi suoranaisesti käyttötarkoitukseen. Kyse voi olla tilanteesta, jossa tietoja kerätään tarjouksen

[139] Alapuranen, ym., 2020, s. 57.
[140] WP 203, s. 20: ”This includes all forms of written and common laws, primary and secondary legislation, municipal decrees, judicial precedents, constitutional principles, fundamental rights, other legal principle, as well as jurisprudence, as such ‘law’ would be interpreted and taken into account by competent courts”.
[141] TSA 5 artiklan 1 kohdan b alakohta, ks. myös WP 203, s. 3.
[142] Ks. Hanninen, ym., 2017, s. 49.
[143] WP 203, s. 16.
[144] IT Governance Privacy Team, 2017, s. 108.

laskemista varten, mutta tietoja kerätään samalla markkinointitarkoituksiin, mistä rekisteröityä ei ole informoitu. Tällöin ajatellaan, että tähän tilanteeseen annetut tiedot ovat sitten käytettävissä myös tulevaisuutta varten. Tällöin ollaan kuitenkin väärällä tavalla käsittelemässä henkilötietoja, sillä tälle uudelle käyttötarkoitukselle ei rekisteröity ole välttämättä antanut suostumustaan tai muu käsittelyn oikeusperuste ei ole käsillä. Käyttötarkoitussidonnaisuuden osalta kyse on myös tietojen minimoinnista ja tarpeellisuusvaatimuksesta. Kuten jäljempänä käy ilmi, tulee rekisterinpitäjän säilyttää vain käyttötarkoituksen kannalta ja käyttötarkoituksen ajan rekisteröidystä kerättyjä tietoja. Tästä syystä onkin tärkeää muistaa, että jos tietoa kerätään ilmoitettuun käyttötarkoitukseen A, sitä ei silloin saa käyttää tarkoituksiin C ja Y. Kuten voidaan huomata, käyttötarkoitussidonnaisuus on yhteydessä myös tarpeellisuusvaatimukseen ja tietojen minimointiin. Ainoan poikkeuksen henkilötietojen käsittelystä toiseen tarkoitukseen tuo mukanaan tilanne, jossa henkilötietojen käsittely sopii yhteen alkuperäisen tarkoituksen kanssa. Yhteensopivuutta tulee kuitenkin tarkastella aina kulloinkin kyseessä olevassa tilanteessa tapauskohtaisesti.[145] Toistaiseksi tästä ei liiemmin ole tulkintakannanottoja, mutta ainoana selkeänä esimerkkinä voitaneen pitää käsittelyä arkistointia ja historiallista taikka tieteellistä tutkimusta varten.[146]

Käyttötarkoitussidonnaisuuden rikkomisesta on myös oikeuskäytäntöä. Suurin osa tapauksista koskee terveydentilaan liittyvien tietojen tarkastelua ilman hoitosuhdetta potilaaseen. Oikeuskäytäntö on suhteellisen selvää siltä osin, että henkilötietojen katsominen potilasjärjestelmistä ilman merkityksellistä hoidollista tarvetta on käyttötarkoitussidonnaisuuden vastaista.[147] Toisaalta aina kyse ei ole suorista potilaskertomuksista. Oikeuskäytännössä on myös pohdittu terveydenhuollossa käytettävien ajanvarausrekisterien sisältämiä henkilötietoja, jotka sisältävät myös potilastietoja, joita ei tule tarkastella uteliaisuudesta. Vaasan HO:ssa käsiteltiin tapausta, jossa asiakaspalvelija oli tarkastellut puolisonsa entisen kumppanin ajanvaraustietoja ja saanut siten erikoislääkärin erikoistumisalan perusteella tietoonsa mahdollisia terveystietoja.[148]

Oikeuskäytännössä on katsottu, että sillä, onko teon tehnyt työ- tai virkasuhteessa oleva tai esimerkiksi harjoittelija, ei ole käytännössä merkitystä. Tietosuojavaltuutettu on henkilörekisteririkkomusta koskevassa lausunnossaan edellyttänyt rangaistavuudelta sitä, että tekijä on rekisterinpitäjän palveluksessa, teolla loukataan rekisteröidyn yksityisyyden suojaa tai aiheutetaan rekisteröidylle vahinkoa ja lisäksi, että tietojen tulee olla kerätty tai annettu hoitosuhteessa

[145] WP 203, s. 3.
[146] TSA johdanto-osan 50 perustelukappale.
[147] Ks. esimerkiksi Vaasan HO ratkaisu 20/109076, annettu 4.3.2020.
[148] Ks. Vaasan HO ratkaisu 20/150486, annettu 17.12.2020.

luottaen siihen, että niitä käytetään vain siihen, että potilaalle voidaan tarjota tarpeellinen ja hyvä hoito.[149]

Toinen tyyppitapaus liittyy tilanteisiin, joissa virkamies tarkastelee hänen tehtäväkuvaansa liittymättömiä tietoja. Teon moitittavuutta lisää se, että tarkastelu kohdistuu arkaluonteisiin tai salassa pidettäviin tietoihin. Näissä tapauksissa käyttötarkoitussidonnaisuus edellyttää, että tietojen tarkasteluun on jokin perusteltu syy. Pelkästään käyttöoikeuksien saaminen tiettyihin rekistereihin ei mahdollista tietojen tarkastelua, ellei sille ole työhön liittyvää tarkoitusta.[150] Myöskään se, että virkamiehelle kerrotaan kansalaisen tehneen rikoksia, ei oikeuta poliisimiestä ryhtymään hakujen suorittamiseen.[151]

Selvää on myös se, että esimerkiksi terveystietoja sisältävistä tietojärjestelmistä tehtävät kyselyt, joiden perusteena on työtehtävien hoitamiseen liittyvien yhteystietojen hankkiminen ei ole itsessään peruste selata yksilöstä kerättyjä tietoja, ellei niitä ole millään vaihtoehtoisella tavalla saatavilla. Tällöin esimerkiksi asiakaspalvelijan hankkiessa tietojärjestelmästä potilaan yhteystietoja hän käsittelee terveystietoja, jotka on annettu terveydenhuoltoa varten eikä yhteydenpitoa varten. Pelkästään tieto terveydenhuollon yksikössä asiakkaana olemisesta on salassa pidettävää. Myöskään tekstiviestien lähettely tai asiakkaan kotiovella käyminen näin hankituilla tiedoilla ei ole käyttötarkoitussidonnaisuuden periaatteen mukaista.[152] Erityisesti moitittavana menettelyä on pidetty, jos rekistereistä saatavia tietoja käytetään työtehtäviin liittymättömiin tarkoituksiin, kuten biologisten vanhempien osoitetietojen selvittämiseen perinnönjakoa varten.[153]

Sisäänrakennetun ja oletusarvoisen tietosuojan kohdalla on syytä kiinnittää huomiota prosesseihin, kun henkilötietojen käsittelyä suunnitellaan ja arvioidaan. Esimerkiksi, ohjeistuksilla ja prosessikaavioilla voidaan toteuttaa muistilista asioista, jotka tulee huomioida ennen toimenpiteisiin ryhtymistä. Tällöin käsittelyn luonne ja käyttötarkoitus tulevat arvioiduksi. Toisaalta

[149] Ks. Etelä-Savon KO ratkaisu 18/114227, annettu 29.3.2018.
[150] Ks. Satakunnan KO ratkaisu 20/104108, annettu 30.1.2020.
[151] Tapauksessa oli hovioikeudessa kyse virkavelvollisuuden rikkomisesta, mikä edellyttää tahallisuutta. Hovioikeus katsoi, että tapauksessa virkamies ei ollut tietoisesti tai tarkoituksellisesti toiminut laittomasti suorittaessaan virkatoimiaan ja hylkäsi siten syytteen, ks. Turun HO ratkaisu 17/121354, annettu 26.5.2017. Lisäksi oikeuskäytännössä on perinteisesti katsottu, että virkamiehen tulee pystyä arvioimaan käsittelyn kohteena olevien tietojen tarpeellisuutta työtehtävissään tai ammattitaidon ylläpitämiseen. Esimerkiksi ammattitaidon ylläpitämistä ei ole se, että tarkastelee yksittäistä kuolemansyynselvityksestä tehtyä raporttia, ks. Turun HO ratkaisu 14/136034, annettu 4.9.2014.
[152] Ks. Oulun KO ratkaisu 18/142895, annettu 9.10.2018 ja Pohjois-Karjalan KO ratkaisu 19/109031, annettu 28.2.2019, sekä Satakunnan KO ratkaisu 19/106975, annettu 14.2.2019.
[153] Ks. Helsingin KO, ratkaisu 18/119000, annettu 3.5.2018.

teknisten järjestelmien kohdalla tulee mahdollisimman aikaisessa vaiheessa pohtia käyttötarkoitussidonnaisuutta ennen järjestelmän avulla tietojenkeräämiseen ryhtymistä.

2.3.4. Tietojen minimointi

Yhtenä ongelmana pidän erityisesti rekisterinpitäjinä toimivien organisaatioiden tapaa pyrkiä keräämään asiakkaistaan ylimääräisiä tietoja suhteessa käsiteltävään aiheeseen. Hyvin usein esimerkiksi asiakkaalta kerätään henkilötietoja, jotka eivät ole tarpeellisia. Esimerkiksi jos olet halukas saamaan kuluttajana luettavaksi mallikuvaston, joudut täyttämään yhteystietosi ennen katalogin lataamista. Katalogin avulla kuluttaja voi tutustua tarjoajan mallistoon ja on sitä kautta potentiaalinen asiakas yritykselle. Toisaalta yhteystietonsa antaneeseen kuluttajaan tullaan todennäköisesti kohdentamaan mainontaa tarjoajan palveluista.

TSA 5 artiklan 1 kohdan c alakohdan mukaan henkilötietojen on oltava asianmukaisia ja olennaisia sekä rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten tietoja kerätään. Tietoja tulee siten käsitellä aina mahdollisimman vähän. Jos tietoja saa kerätä vain ennalta määrättyyn käyttötarkoitukseen, on kerättävien tietojen oltava käyttötarkoitukseen nähden niin oleellisia, että niitä täytyy kerätä käyttötarkoituksen toteuttamiseksi ja vain siinä määrin, että käyttötarkoitus toteutuu.[154] Kyse on tietojen minimoinnin periaatteesta. Tällä periaatteella on selkeä yhteys edellä esille tulleeseen käyttötarkoitussidonnaisuuteen. Jo tietosuoja-asetuksen johdannossa todetaan, että henkilötietoja saa käsitellä vain, jos käsittelyn tarkoitusta ei voida kohtuullisesti toteuttaa muilla keinoin.[155] Siten sellaisia tietoja ei tule kerätä, joille ei ole osoitettavissa tarvetta. Kerättävät tiedot eivät saa olla liian laajoja suhteessa käyttötarkoitukseen. Kyse ei ole tietenkään siitä, että tietojen käsittelyn määrä minimoidaan mahdollisimman vähäiseksi vaan että tiedon kerääminen sovitetaan käyttötarkoitukseen nähden sopivalle tasolle.[156] Keskeistä on säilyttää rekisteröidystä ainoastaan siinä määrin tietoja, kuin on tarkoitusten toteuttamiseksi tarpeellista. Siten esimerkiksi vanhentuneet tai hyödyttömät tiedot tulee poistaa. Tässä yhteydessä on keskeistä, että kukaan ei kerää tietoja, joita ei tarvita käyttötarkoituksen toteuttamiseksi. Tietosuojavaltuutettu on ratkaisukäytännössään pitänyt esimerkiksi takseissa käytössä olevan kameravalvonnan lisäksi tallennettua ääninauhaa ylimääräisenä henkilötietona, jota ei tarvita käyttötarkoituksen toteuttamiseksi.[157] Toisessa tietosuojavaltuutetun toimiston ratkaisussa TSV 25.06.2020 apulaistietosuojavaltuutettu katsoi, että pysäköintilaitokseen parkkeeratessa näkyville jätettävässä parkkilapussa oleva henkilön osoitetieto ei ollut

[154] Ks. Korpisaari, ym., 2018, s. 93.
[155] TSA johdanto-osan 39 perustelukappale.
[156] Voigt, 2017, s. 90.
[157] Apulaistietosuojavaltuutetun ratkaisu TSV 26.5.2020, perusteluiden kohta 2.

yhteensopiva tietojen minimoinnin periaatteeseen.[158] Tietojen minimointia harjoitetaan organisaation tietosuojariskien kartoituksella ja analysoinnilla *(data mapping)* ja toimintatapojen arvioinnilla.[159] TSA:ssa korostetaan, että tiedosta ja sen käytöstä tulee olla selvillä, jotta tiedon käyttöä voidaan minimoida.[160] Kukin voi omassa roolissaan pohtia henkilötietoja käsitellessään, palveleeko tämä tieto käyttötarkoituksen toteutumista. Jos tiedosta ei ole muuta kuin välillistä hyötyä eikä suoraa vaikutusta käyttötarkoituksen rakentumiseen, sellaista tietoa ei tulisi kerätä. Pelkästään rekisteröidyn suostumus ei laajenna tarpeettomasti tai rajattomasti rekisterinpitäjän oikeutta kerätä henkilötietoja.[161]

2.3.5. Säilytyksen rajoittaminen

TSA:n 5 artiklan 1 kohdan e alakohdan mukaan henkilötiedot on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten. Siten, kun henkilötiedot käyvät tarpeettomaksi, ne tulee lähtökohtaisesti poistaa. Tällä viitataan säilytyksen rajoittamiseen. TSA:n johdannossa todetaan, että rekisterinpitäjän tulisi asettaa määräajat henkilötietojen säilyttämiselle.[162] Tällöin rekisterinpitäjän on syytä tehdä merkintä selvästi ja helposti saatavissa olevassa muodossa, mikä auttaa rekisterinpitäjää tarkastelemaan aika ajoin sitä, onko tietoja syytä poistaa. Merkinnät voidaan tehdä manuaalisesti siten, että rekisterinpitäjällä on mahdollisuus seurata esimerkiksi vuosikelloa, jossa on määritelty ajankohdat, jolloin asiakirjat tuhotaan. Käytettäessä automaattista tietojen käsittelyä on järjestelmiin mahdollista rakentaa mekanismi, joka automaattisesti tietyn ajan kuluttua hävittää tiedot. Tietojen säilytysajasta on myös viestittävä rekisteröidylle siinä kohdin, kun tietoja hänestä kerätään.[163] Tästä johdettuna ja myös sisäänrakennettuun ja oletusarvoiseen tietosuojaan liittyen määräaikoja tietojen säilyttämiseen tulee pohtia jo ennen käsittelytoimiin ryhtymistä. Tietojen säilytystä koskevan suunnitelman kirjaaminen organisaation tietosuojakäytänteisiin auttaa organisaatiota myös myöhemmin nähtävillä olevissa osoitusvelvollisuustilanteissa. Lisäksi se toteuttaa velvollisuutta asianmukaisista teknisistä ja organisatorisista toimenpiteistä.

Kun henkilötiedot käyvät tarpeettomaksi, tulee tiedot lähtökohtaisesti poistaa. Lähtökohtaisuus viittaa siihen, että rekisterinpitäjä voi täyttää tämän velvollisuuden muuttamalla tiedot

[158] Apulaistietosuojavaltuutetun ratkaisu TSV 25.6.2020, perusteluiden kohdat 5–7.
[159] IT Governance Privacy Team, 2017, s. 109–110. Ks. käytännön toteutuksesta Andreasson, ym., 2019, s. 56–67.
[160] TSA artikla 25.
[161] Hanninen, ym., 2017, s. 49.
[162] TSA:n johdanto-osan 39 perustelukappale.
[163] TSA 13 artikla.

sellaiseen muotoon, josta rekisteröity ei enää ole tunnistettavissa. Tällöin kyse on tietojen anonymisoinnista, jota käsitellään tarkemmin kohdassa 4.3.3. Lähtökohdasta voidaan myös poiketa tilanteissa, joissa erityislainsäädännössä asetetaan tarkempia määräyksiä tietojen säilyttämisestä. Yksi tällaisista tilanteista on hotelliasiakkaasta kerättävät matkustajatiedot, jotka on säilytettävä majoitus- ja ravitsemistoiminnasta annetun lain (308/2006) 8 §:n 3 momentin mukaisesti vuoden ajan matkustajailmoituksen allekirjoittamispäivästä. Siten, vaikka henkilötiedot olisivat käyneet rekisterinpitäjälle tarpeettomaksi, on niitä säilytettävä edellä mainitun ajan. Säilyttäminen tulee kuitenkin järjestää siten, että henkilötietoja ei silti käsitellä tarpeettomasti. Viittaan tällä siihen, että säilytettäviä tietoja ei käsitellä arkistointia enempää. Erityislainsäädäntöä tietojen säilyttämisen kestosta tulee arvioida tarkkaan. Tietosuojavaltuutettu on esimerkiksi ratkaisukäytännössään huomioinut, että esimerkiksi kirjanpitolakiin 1336/1997 sisältyy aikamääreitä tietojen säilyttämisestä. Ratkaisussa TSV 19.3.2021 tietosuojavaltuutettu katsoi, että ajoneuvosta otetut valokuvat ja valvontamaksulomake eivät ole kirjanpitolaissa tarkoitettuja tietoja, joita tulisi säilyttää kirjanpidollisista syistä. Samaisessa ratkaisussaan tietosuojavaltuutettu totesi, että tietoja ei voida loputtomiin ja määrittelemättömästi säilyttää sen nojalla, että rekisterinpitäjä mahdollisesti joskus tulevaisuudessa päättää saattaa asian tuomioistuimen ratkaistavaksi.[164] Näinpä rekisterinpitäjän tulee huolellisesti arvioida kussakin tilanteessa säilytyksen rajoittamisen vaatimus.

2.3.6. Eheys ja luottamuksellisuus

TSA 5 artiklan 1 kohdan f alakohdassa edellytetään, että henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus. Henkilötietojen käsittelyssä tietoja tulee suojata luvattomalta ja lainvastaiselta käsittelyltä. Samoin henkilötiedot on suojattava vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta. Suojaaminen tapahtuu käyttäen asianmukaisia teknisiä ja organisatorisia toimia. Eheyden ja luottamuksellisuuden periaate on ehkä kaikista TSA 5 artiklan periaatteista tärkein taloudellisesta näkökulmasta. Kyse on siitä, että muiden periaatteiden kohdalla vahinko syntyy rekisteröityjä kohtaan, kun taas eheys- ja luottamuksellisuusperiaatteen vastainen toiminta johtuu yleensä tietoturvaloukkauksista, jotka voivat olla osoitus tehottomasta toiminnasta eheyden ja luottamuksellisuuden eteen. Periaate edellyttää, että tietoja käsitellään siten, että tietojen eheys ja luottamuksellisuus säilyy eikä asiattomille synny mahdollisuutta päästä käsiksi tietoihin.[165] Toisaalta periaate edellyttää riittävän turvallisuustason järjestämistä, joten aina tietoturvaloukkaukset eivät ole

[164] Tietosuojavaltuutetun ratkaisu TSV 19.3.2021.
[165] IT Governance Privacy Team, 2017, s. 114–-116.

seurausta tehottomista toimista tietoturvallisuudessa. Siten periaate liittyy asetuksen edellyttämään riskiperusteiseen lähestymistapaan.[166] Eheydellä tarkoitetaan sitä, että kerätyt tiedot säilyvät muuttumattomana pois lukien rekisterinpitäjän suostumuksella tapahtuneet muutokset. Luottamuksellisuudella viitataan puolestaan velvollisuuteen turvata tietoihin käsiksi pääseminen siten, ettei kukaan ulkopuolinen niihin pääse käsiksi.[167]

TSA:ssa tämä vaatimus liittyy läheisesti tietoturvallisuuteen, ja sillä on selkeä yhteys TSA:n artikloihin 25, 32 ja 35. Tietoturvallisuusstandardin mukaan luottamuksellisuus nähdään siten, että tietoa ei tuoda saataville eikä luovuteta luvattomille henkilöille tai prosesseille.[168] Kyse on siten myös sisäisistä tarpeista rajoittaa pääsyä tietoon. Näin esimerkiksi kollegoilla, joilla ei ole yhteenliittymää työtehtävään, ei tulisi myöskään olla tarvetta nähdä sellaisesta tietoja. Työpaikalla voi tulla esiin asioita, joihin kollegalla ei edes olisi pääsyä ja näin ollen tietoa pääsee liikkumaan ilman oikeutta siihen. Samaisen standardin mukaan eheys nähdään tiedon tarkkuutena ja täydellisyytenä.[169] Eheyden varmistamisessa yksi keino on pitkän prosessin aikana huolehtia esimerkiksi siitä, että asiakkaan yhteystiedot tarkistetaan itse asiakkaalta säännöllisin väliajoin – tällöin esimerkiksi tieto ei päädy vanhentuneeseen osoitteeseen. Lisäksi kyseeseen tulevat tietoturvatoimenpiteet, joilla erotetaan tietoryhmät toisistaan. Esimerkkinä tällaisesta toimenpiteestä on myöhemmin käsiteltävä pseudonymisointi. Tärkeää on huolehtia esimerkiksi siitä, ettei kukaan tietoja yhdistelemällä pääse henkilötietoihin käsiksi.

TSA 33 artiklan toisen kohdan mukaan henkilötietojen käsittelijän on ilmoitettava ilman aiheetonta viivytystä rekisterinpitäjälle tietoturvaloukkauksesta saatuaan tämän tietoonsa. Tämä pätee varsinaisiin loukkauksiin, joissa on esimerkiksi murtauduttu tietojärjestelmiin. Hyvänä kysymyksenä on kuitenkin se, tulisiko henkilötietojen käsittelijä ilmoittaa havaitsemastaan mahdollisesta uhasta tietoturvaloukkaukseen? Esimerkiksi kyse voisi olla asiakirjojen säilyttämisestä toimiston käytävällä, vaikka laatikot oli tarkoitus siirtää tietosuojattuun tilaan iltapäivällä. Tällaisen ilmoituksen vuoksi voidaan ryhtyä toimenpiteisiin vastaisuuden varalta. Toisaalta tällaisten uhkien universaali ilmoittaminen johtaisi raskaaseen prosessiin. Ilmoitusmenettelystä sovitaan yleensä tarkemmin rekisterinpitäjän ja henkilötietojen käsittelijän välisellä sopimuksella. Sopimuksen laatimisessa usein erimielisyyttä syntyy juuri siitä, milloin ilmoitus tulee tehdä. Tämä on seurausta siitä, että henkilötietojen käsittelijä ei halua ilmoittaa kaikista uhkakuvista, mutta rekisterinpitäjä puolestaan haluaisi näistä tietää. Käytännön toteutus onkin haastavaa, enkä näe ilmoituksen rakentamista myös uhkakuviin perustelluksi yksilön suojaamisen

[166] Korpisaari, ym., 2018, s. 94.
[167] Ibid., s. 94.
[168] ISO/IEC 27000:2018, kohta 3.10.
[169] ISO/IEC 27000:2018, kohta 3.36.

kannalta. Jos tällainen ilmoitus kaikista uhkista tulisi tehdä, se johtaa tilanteeseen, jossa resursseja käytetään liikaa preventiiviseen suojaamiseen, milloin reagointikyky mahdollisiin loukkauksiin heikkenee. Yksilön kannalta keskeisempää on se, että mahdollisiin tietoturvaloukkauksiin pystytään puuttumaan, sillä vaikka preventiiviseen suojaamiseen panostetaan, on aina tietoturvamurron riski olemassa.

Yksi mielenkiintoinen asia liike-elämässä on, että toimittaessa erinäisissä tilanteissa voi syntyä kysymyksiä todennuksesta *(authenticity)*. Käsiteltäessä henkilötietoja pitää muistaa, että kuka tahansa voi esiintyä jonkin tahon edustajana, ja on aina muistettava huolehtia siitä, että pystyy todentamaan kyseessä olevan henkilön. Lisäksi on hyvä muistaa, että TSA 28 artiklan 2 kohdan mukaan henkilötietojen käsittelijä ei saa käyttää toisen käsittelijän palveluksia ilman rekisterinpitäjän (kirjallista) lupaa.

Tietoturvallisuuteen liittyen on oikeuskäytännössä katsottu, että tiedot tulee tuhota asianmukaisesti.[170] Samaisessa tapauksessa kyse oli myös siitä, oliko henkilörekisterin tulostamiselle paperiversiona tarvetta. Yrityksen osaomistaja oli tulostanut henkilörekisterin tiedot, jotta kykenisi arvioimaan yhtiön asiakasmäärän kehitystä. Henkilötietoja käsiteltyään hän oli hävittänyt tiedot siten, että tulostetut asiakastiedot oli laitettu ei-lukittavaan paperinkeräyssäiliöön, josta sivullinen on rekisteritiedot löytänyt. Oikeus katsoi, että henkilötietojen tietoturvallista hävittämistä koskevien sääntöjen rikkominen aiheuttaa rekisterissä olevien henkilöiden tietoturvallisuudelle vakavan vaaran ja osaomistajan oli siten katsottava syyllistyneen tietosuojarikokseen.

2.3.7. Täsmällisyys

Täsmällisyysvaatimuksella pyritään tietojen paikkansapitävyyteen. TSA edellyttää, että henkilötietojen tulee olla täsmällisiä ja tarvittaessa päivitettyjä.[171] Tämä puolestaan tarkoittaa käytännössä sitä, että rekisterinpitäjän vastuulla on huolehtia kohtuullisin toimenpitein tietojen oikeellisuudesta ja poistaa epätarkat ja virheelliset tiedot viipymättä.[172] Tällä pyritään suojaamaan rekisteröityä muun muassa identiteettivarkaudelta. Se myös pitää huolen siitä, että automaattisia profilointipäätöksiä tehdään perustuen täsmällisiin tietoihin päätöksen kohteesta.[173] Tietojen säilytysaika tulee myös sovittaa oikein. Kyse on säilytyksen rajoittamisesta siten, että tietojen säilyttämisajan tulee olla mahdollisimman lyhyt. Voi tietysti olla, että joitain tietoja joudutaan säilyttämään pidemmänkin aikaan jonkin muualla laissa säännellyn seikan vuoksi. TSA 5 artiklan 1 e kohdan mukaan tällöin edellytetään, että tietoja tulee säilyttää sellaisessa

[170] Ks. Pirkanmaan KO ratkaisu 21/100862, annettu 11.1.2021.
[171] TSA 5 artiklan 1 kohdan d alakohta.
[172] Korpisaari, ym., 2018, s. 93.
[173] IT Governance Privacy Team, 2017, s. 110–113.

muodossa, että ne eivät paljasta tiedon kohdetta ja että tiedot on helppo poistaa. Tällöin kyseeseen tulee tietojärjestelmien hallinta esimerkiksi tietoja hajauttamalla ja pseudonymisoimalla.[174]

Virheellinen henkilötieto ei anna oikeaa kuvaa seikasta, jota sillä halutaan kuvata. Samoin jos tieto ei kyseisessä tilanteessa ole asianmukainen, on kyse virheellisestä tiedosta.[175] Epätäydellinen, kokonaan tai osittain puutteellinen tieto voi johtaa sitä käytettäessä toisenlaiseen lopputulokseen verrattuna siihen, mitä olisi tapahtunut, jos käytettävissä olisi ollut täydelliset tiedot. Yksilöllä on oikeus tulla arvioiduksi oikeiden tietojen valossa.[176] Siten on keskeistä, että rekisterinpitäjän on oikaistava rekisteröityä koskevat virheelliset tiedot mahdollisimman pian, ettei yksilölle tapahdu oikeudenloukkauksia. TSA ei kuitenkaan edellytä sitä, että rekisterinpitäjä aktiivisesti pyrkii selvittämään uusia yhteystietoja. Yleensä kuitenkin tietojen päivittäminen lähtee kuitenkin rekisteröidyn aloitteesta.

Täsmällisyysvaatimuksen mukaan jokaisen tulee huolehtia siitä, että hän ei itse säilytä vanhentuneita tietoja. Aika ajoin tulee myös käydä läpi olemassa olevat yhteystiedot ja muut henkilötiedot virheellisten tietojen oikaisemiseksi. Tämän voi tehdä esimerkiksi väestötietojärjestelmän avulla.[177] Kyse on kohtuullisista toimista. Nähdäkseni kohtuullisia keinoja ovat esimerkiksi sellaiset, joita suoritetaan valvontasyklien tai vuosikellon mukaisesti säännöllisin väliajoin. Kohtuullisia eivät siten olisi esimerkiksi päivittäiset tarkastukset. Kohtuullisena toimenpiteenä tulee ehdottomasti pitää sitä, jos rekisteröity haluaa oikaista itseään koskevat tiedot. Tällaisessa tilanteessa tulee tiedot päivittää viipymättä. Samalla on hyvä olla myös perillä tietojen säilytysajoista. Moni ajattelee varmasti, että on mukava säilyttää malliksi pohjia ja sopimuksia sekä muita tietoja tulevaisuutta varten. Sinällään pohjia tietysti saa ja kannattaa säilyttää, mutta ne on tyhjennettävä henkilötiedoista. Kun tietojen säilytysaika minimoidaan, myös tilaa säästyy. Tästä syystä on mielestäni tärkeää, että jokaisen rutiineihin kuuluu myös säännöllisin väliajoin tarkastella tietojen säilytysajan merkitystä. Yhtenä käytännön toimenpiteenä voi olla tiedostojen nimeäminen päivämäärin, milloin tieto tulee poistaa.

2.3.8. Osoitusvelvollisuus

Edellä on käsitelty yleisiä tietosuojaperiaatteita. Osoitusvelvollisuus ei ole sinänsä periaate, vaikka tässä yhteydessä kuvaankin sitä seitsemäntenä periaatteena. Osoitusvelvollisuus

[174] IT Governance Privacy Team, 2017, s. 113–114.
[175] Wallin – Nurmi, 1991, s. 95.
[176] Alapuranen, ym., 2020, s. 62
[177] Korpisaari, ym., 2018, s. 93–94.

merkitsee kahta asiaa: 1) rekisterinpitäjä on velvollinen noudattamaan yleisiä tietosuojaperiaatteita ja lisäksi 2) rekisterinpitäjä pystyy osoittamaan noudattamisen toteutuksen. Rekisterinpitäjän osoittamisvelvollisuus kohdistuu kaikkiin henkilötietojen käsittelyn vaiheisiin ja kaikkeen rekisterinpitäjän toimesta tehtyyn käsittelyyn – myös suhteessa kolmanteen.[178] Osoitusvaatimus on TSA:n mukanaan tuoma uudistus. Enää ei riitä, että henkilötietoja käsitellään sellaisenaan tietosuojavaatimusten mukaisesti, vaan noudattaminen pitää myös pystyä osoittamaan.[179] Osoitusvelvollisuusvaatimuksella pyritään siihen, että se vähentämään epätasa-arvoa rekisteröidyn ja rekisterinpitäjän välillä – nähdäkseni siitä syystä, että se asettaa uhan suurista sakoista ja dokumentoinnista. Dokumentointia on puolestaan vaikea toteuttaa, jos toimintamallit eivät vastaa näitä vaatimuksia.[180] Tämä onkin keskeistä tietää, sillä käsitellessä henkilötietoja tulee muistaa, että toimenpiteet tulee pystyä osoittamaan myöhemmin.

Ajantasaisesta dokumentoinnista tietoja käsiteltäessä tulee pitää huolta. Tämä helpottaa myös huomattavasti esimerkiksi valvontaviranomaisen valvontakäyntiä tai tilannetta, jossa epäillään TSA:n noudattamatta jättämistä. Toisaalta jo itse dokumentointi ja kyky tietosuojaperiaatteiden noudattamisen osoittamiseen osoittaa hyvää tietojenkäsittelytapaa. Kun rekisterinpitäjä pystyy osoittamaan käsittelyn lainmukaisuuden ja hyvän tietojenkäsittelytavan noudattamisen pitämällä arkistot turhasta tiedosta vapaana, ei ole huolta myöskään TSA;n mukaisista sanktioista.[181]

Tietosuojavaltuutettu on julkaissut listauksen toimenpiteistä ja erilaisista dokumenteista, joilla osoitusvelvollisuutta voidaan osoittaa. Listaus sisältää dokumentoinnin seuraavista asioista: seloste käsittelytoimista, tietosuojaperiaatteiden sisäänrakennettu toteutuminen omassa toiminnassa, mahdolliset tietosuojaa koskevat laajemmat toimintaperiaatteet, informointikäytännöt, käsittelyn oikeusperustetta koskevat arviot, muut sisäiset ja ulkoiset ohjeistukset, vaikutustenarviointeja ja ennakkokuulemista koskeva dokumentaatio, tietoturvaloukkausten dokumentointi, tietosuojavastaavan asema ja tehtävien dokumentointi, henkilötietojen käsittelyyn liittyvät sopimukset, kolmansiin maihin tehtävät henkilötietojen siirtoja koskevat dokumentit sekä yhteisrekisteripitäjien vastuualueet. Osoitusvelvollisuutta osana rekisterinpitäjän organisatorisia toimenpiteitä tarkastellaan tarkemmin luvussa 4.4.

Olisikin hyvä, jos jokainen tietoja käsittelevä pitäisi kunnian asianaan omaa, tietosuojaystävällistä tietojenkäsittelytapaansa ja veisi tätä esimerkiksi laajalti myös työympäristöönsä.

[178] IT Governance Privacy Team, 2017, s. 116–118.
[179] Vrt. aikaan ennen tietosuoja-asetusta Hanninen, ym, 2017, s. 51.
[180] Korpisaari, ym., 2018, s. 95–97.
[181] Hallinnollisen seuraamusmaksun suuruus riippuu rikotusta oikeushyvästä. Korvausten enimmäismäärät ovat suuret, ks. TSA 83 artikla 2–6 kohdat.

Loppujen lopuksi tässä on kyse erityisen tärkeästä asiasta, jolla on myös vaikutusta yrityskuvaan.[182] Koko henkilöstön riittävällä tietosuojaosaamisella on merkitystä myös yritystoiminnan yleiseen toimintaan ja rekisterinpitäjän tietosuojavelvoitteiden noudattamiseen. Tietosuojatyön organisointi ja asiakkaan luottamus toimintaan ovat merkityksellisiä valttikortteja. Tästä syystä ei pidäkään enää ajatella, että tietosuoja estää jotain, vaan se mahdollistaa paremmat tulokset.[183] Kuten myöhemmin ilmenee, osana sisäänrakennettua ja oletusarvoista tietosuojaa tulee henkilötietojen käsittelyssä ja käsittelyn suunnittelussa katsoa näiden yleisten tietosuojaperiaatteiden lävitse ja noudattaa niitä.

3. SISÄÄNRAKENNETTU JA OLETUSARVOINEN TIETOSUOJA

3.1. Sisäänrakennettu tietosuoja

Sisäänrakennetusta tietosuojasta käytetään useita termejä, joilla on hieman eri merkitys. Yleisin on englanninkielinen termi *Privacy by Design (PbD)*, mutta varsinkin eurooppalaisessa kontekstissa käytetään termiä *Data Protection by Design (DPbD)*. Vaikka edellä mainittuja käsitteitä käytetään usein synonyymeinä, on niillä kuitenkin eroja. Niitä tulee käyttää varovaisesti sekoittumisvaaran vuoksi, sillä käsitteiden laajuus eroaa eurooppalaisen ja yhdysvaltalaisen käsityksen valossa.[184] Käsite tuo esiin laajempaa poikkitieteistä pyrkimystä, jonka tavoitteena on upottaa keskeiset inhimilliset arvot – erityisesti hyve-etiikan keskeiset arvot – teknologian suunnitteluprosessiin.[185] Itsessään käsitettä on heikosti avattu, ikään kuin se hyväksyttäisiin sellaisenaan samoin kuin yksityisyyden käsite.[186] Ajatuksena on tunnustaa tietojärjestelmäarkkitehtuurin kyky muokata ihmisen käyttäytymistä kuten lait tai sopimukset, ja siten muokata yksilöiden käyttäytymistä tehokkaammin. Samalla kyse on pyrkimyksestä parantaa tietosuojaa koskevia oikeudellisia normeja rakentamalla normit osaksi tietojärjestelmäarkkitehtuuria. Tällaisen upottamisen avulla arkkitehtuurin automatisoidut prosessit auttavat automatisoimaan ja muokkaamaan myös oikeudellisia normeja. Oletuksena on lupaus normien soveltamisen

[182] Ks. Korpisaari, ym., 2018, s. 277–281 ja ks. myös Andreasson, ym., 2019, s. 30.
[183] Tietosuojan merkityksestä organisaatioille ks. Andreasson, ym., 2019, s. 48–56.
[184] Eroavuudet liittyvät lähinnä käsitykseen suojan kohteesta. Eurooppalaisessa kontekstissa suoja kohdistuu henkilön oikeuteen kontrolloida omia tietojaan. Sen sijaan, yhdysvaltalaisessa kontekstissa kyse on suojasta yksilön yksityisiä tietoja kohtaan. Ks. Bygrave, 2017, s. 757 ja s. 761.
[185] Ks. esimerkiksi Wiener, 1954, ks. myös Friedman, 1997 ja Spiekermann, 2015.
[186] Sisäänrakennetun tietosuojan käsite unionin kontekstissa on jäänyt jokseenkin vaisuksi. Esimerkiksi Euroopan komission suosituksessa 2014/724/EU todetaan varsin ylimalkaisesti sisäänrakennetun tietosuojasta seuraavaa*: 'data protection by design' requires to implement, having regard to the state of the art and the cost of implementation, both at the time of the determination of the means for processing and at the time of the processing itself, appropriate technical and organisational measures and procedures in such a way that the processing will meet the requirements of Directive 95/46/EC and ensure the protection of the rights of the data subject*.

merkittävästä lisääntymisestä *ex ante* ja vastaavasta vähennyksestä niiden soveltamisessa *ex post facto*. Toiveena on, että tämä sääntelyn uudelleenjärjestely parantaa teknologisen kehityksen saavuttamisen ongelmaa, joka perinteisesti vaivaa lainsäätämistavoitteitamme.[187]

Terminä sisäänrakennettu tietosuoja ei ole syntynyt vastikään. Kyse on sisäänrakennetun tietosuojan pioneerin Ann Cavoukianin[188] kehittämästä ajatuksesta, jossa organisaatioita kehotetaan suojaamaan yksilöiden yksityisyyttä upottamalla se tekniikoiden, liiketoimintakäytäntöjen ja fyysisten infrastruktuurien suunnitelmiin. Euroopan tietosuojaneuvosto sisällytti 32. vuosittaisessa täysistunnossaan päätöslauselmaansa Ann Cavoukianin kehittämän holistisen konseptin, *Privacy by Designin* käsitteellistämisen kansainväliseksi standardiksi.[189]

Cavoukianin ajatus sisäänrakennetusta tietosuojasta sisältää seitsemän periaatetta, joiden muotoilut voidaan paremmin ajatella retorisina iskulauseina kuin analyyttisinä tai toiminnallisina välineinä. Cavoukianin seitsemän periaatteen mukaisesti sisäänrakennettu tietosuoja on:

1) Proaktiivista, ei reaktiivista; ennaltaehkäisevää, ei hoitavaa: tietosuoja tulee ottaa huomioon ennakoivasti eikä jälkikäteisesti. Riskit tulee tunnistaa samoin etukäteisesti kuten myös ennalta ehkäistä yksityisyyden loukkaukset ja muut tietosuojariskit.
2) Oletusasetus: rekisteröidyn ei tarvitse tehdä mitään suojatakseen yksityisyyttään, vaan yksityisyyden suoja on järjestelmissä oletusarvona sisäänrakennetusti. Jos yksilö ei toimi yksityisyytensä turvaamiseksi, hänen yksityisyytensä tulee edelleen olla turvattu.
3) Yksityisyyden sisällyttämisestä suunnitteluun: palvelut tulee suunnitella niin, että tietosuoja on luonnollinen ja keskeinen osa järjestelmää heikentämättä kuitenkaan sen toiminnallisia ominaisuuksia.
4) Täyttä toiminnallisuutta; lisäarvoa eikä nollasummapeliä: kaikki oikeutetut edut pyritään saavuttamaan ilman tarpeettomia kompromisseja. Harhaanjohtavia vastakkainasetteluja tulee välttää.
5) Päästä päähän -turvallisuutta *(end-to-end security*); yksityisyyden suoja ja tietoturva tulee varmistaa koko henkilötiedon elinkaaren ajan alkaen ajasta, jolloin henkilötietoa ei ole vielä edes syötetty mihinkään, kestäen aina siihen, kun henkilötieto on tosiasiallisesti tuhottu.

[187] Bygrave, 2017, s. 755.
[188] Ann Cavoukian on entinen Ontarion osavaltion tietosuojavaltuutettu.
[189] Resolution on Privacy by Design, Euroopan tietosuojaneuvoston 32. täysistunto, Jerusalem, Lokakuu 27–29 2010, https://edps.europa.eu/sites/edp/files/publication/10-10-27_jerusalem_resolutionon_privacy-bydesign_en.pdf, käytetty 5.3.2021.

6) Näkyvyyttä, läpinäkyvyyttä ja avoimuutta: toimenpiteiden, joita suoritetaan tietosuojaan liittyen, tulee olla kaikille osapuolille (käyttäjille, käsittelijöille, yhteistyökumppaneille jne.) dokumentoituja, läpinäkyviä ja saatavilla.
7) Yksityisyyden kunnioittamista ja käyttäjäkeskeisyyttä: yksilön tarpeet ovat keskeisimpiä. Tietosuoja tulee toteuttaa käyttäjäkeskeisesti, yksilön oikeudet edellä. Käyttäjillä tulee olla riittävästi vaihtoehtoja esimerkiksi asetuksissa, joiden tulee lisäksi olla oletuksena yksityisyyttä kunnioittavia. Järjestelmien tulee tarjota käyttäjälleen riittävät ja oikeat tiedot vaihtoehtojen tueksi, jotta käyttäjä pystyy valitsemaan häntä tyydyttävän vaihtoehdon.[190]

Sisäänrakennettu tietosuoja määrittää sen, että rekisterinpitäjien on sovellettava ohjelmistosuunnitteluperiaatteita sekä organisatorisia toimenpiteitä yksityisyyden suojan suunnitteluun koko tietojärjestelmien kehityksen sekä tiedonkeruun ja käsittelyprosessien ajan. Näihin käytänteisiin voidaan sisällyttää esimerkiksi tietojen pseudonymisointi ja tiedonkeruun minimointi. Samaan kategoriaan lukeutuvat vaikutustenarviointi, kryptaus ja muut tekniset toimet. Sisäänrakennetun tietosuojan puolestapuhujille on itsestään selvää, että yksityisyys on oletusasetus; se ei ole vain ylimääräistä jargonia, vaan yksityisyyden tulee muodostaa valtavirta, ja sen kunnioittamisen ei pitäisi myöskään olla vain sääntöjen noudattamista (*compliance*) vaan asia, joka on sisäistettävä täysimääräisesti. Tällaisen strategian toteuttamista voi olla jonkinlainen teknologinen toimenpide, kuten yksityisyyden suojaa edistävien teknologioiden käyttöönotto, mutta yksityisyyden suojan toteutus ei ole täysimittaisesti teknologiasta riippuvaa.[191]

Tässä yhteydessä lienee syytä todeta, että sisäänrakennetun ja oletusarvoisen tietosuojan avulla järjestetyssä henkilötietojen suojassa ei ole kyse mistään superperusoikeudesta. Monissa yhteyksissä tätä korostetaan liikaa, sillä TSA edellyttää riittävää henkilötietojen suojaa. Jos henkilötietojen suoja viedään äärirajoille se loisi täydellisen henkilötietojen käsittelykiellon. Vaikka tällöin tietysti yksilön yksityisyys toteutuisi täysimääräisesti, tilanne johtaisi kuitenkin ylitsepääsemättömiin ongelmiin yhteiskunnassa. Jos kaikennäköinen henkilötietojen käsittely olisi kiellettyä tai se olisi hyvin tarkkaan rajoitettua, eivät yksilöt pystyisi nauttimaan yhteiskunnan tarjoamista mahdollisuuksista. Sisäänrakennetussa ja oletusarvoisessa tietosuojassa kysymys on yksilön suojaamisesta tarpeettomalta henkilötietojen käsittelyltä, ja sen lisäksi rekisterinpitäjien ohjaamisesta kohti henkilötietojen suojaa kunnioittavaa kulttuuria.

[190] Cavoukian, 2009, s. 2.
[191] Cavoukian, 2009.

Sisäänrakennetun- ja oletusarvoisen tietosuojan noudattamisen velvollisuus on sisällytetty TSA:n 25 artiklaan, jonka sisältö on seuraava:

> *1. Ottaen huomioon uusimman tekniikan ja toteuttamiskustannukset sekä käsittelyn luonteen, laajuuden, asiayhteyden ja tarkoitukset sekä käsittelyn aiheuttamat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit luonnollisten henkilöiden oikeuksille ja vapauksille rekisterinpitäjän on -- toteutettava tehokkaasti tietosuojaperiaatteiden, kuten tietojen minimoinnin, täytäntöönpanoa varten asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten tietojen pseudonymisointi ja tarvittavat suojatoimet--.*
>
> *2. Rekisterinpitäjän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. -- Näiden toimenpiteiden avulla on varmistettava etenkin se, että henkilötietoja oletusarvoisesti ei saateta rajoittamattoman henkilömäärän saataville ilman luonnollisen henkilön myötävaikutusta --.*

Sisäänrakennetun ja oletusarvoisen tietosuojan vaatimus on muodostettu artiklan pohjalta. Artiklalla on pyritty selkeästi lisäämään rekisterinpitäjän velvollisuutta huolehtia omatoimisesti rekisteröityjen yksityisyydestä henkilötietoja käsiteltäessä verrattuna aikaan ennen TSA:ta. Tietosuojadirektiiviin ei vastaavaa ajatusta sisäänrakennetusta ja oletusarvoisesta vielä sisältynyt. TSA:n johdanto-osan 78 perustelukappale noudattelee pitkälti edellä esitetyn TSA:n 25 artiklan sisältöä mutta korostaa erityisesti asetuksen toteuttamisen tarkoitusta sisäänrakennetun ja oletusarvoisen tietosuojan avulla. Sekä TSA 25 artikla että johdanto-osan 78 perustelukappale edellyttävät myös, että vaatimusten täyttämiseksi toteutetaan tekniset ja organisatoriset toimenpiteet. TSA:n artiklan 5 kohdan 2 mukaan periaatteiden noudattaminen on rekisterinpitäjän vastuulla, ja rekisterinpitäjän on pystyttävä osoittamaan vaatimustenmukaisuus, johon voidaan viitata vastuuvelvollisuuden käsitteenä. Edellä mainitun toteutuksessa rekisterinpitäjän tulee säännöllisesti arvioida periaatteiden noudattamista ja tietoturvatoimenpiteiden asianmukaisuutta. Velvollisuus on yhteydessä TSA 35 artiklan vaatimukseen toteuttaa vaikutustenarviointi silloin, kun henkilötietojen käsittelyyn kohdistuu korkea riski. Tietosuojavaltuutettu on antanut ratkaisun, jossa huomioidaan sekä TSA 5, 25 että 35 artiklan noudattamatta jättämisen. Kyse oli lainvastaisesta tietojen keräämisestä. Ratkaisussa katsottiin, että tällainen rikkomus on vakava ja edellyttää tästä syystä seuraamusmaksun määräämistä.[192]

Toisaalta jos oletettaisiin, että teknologisia hallintatoimenpiteitä voidaan myös käyttää ihmisten tiedonintressin loukkaamisen, kuten järjestelmien tietojen luvattoman käytön, henkilötietojen

[192] Ks. Tietosuojavaltuutetun ratkaisu TSV 18.5.2020.

luvattoman säilyttämisen tai väärinkäytön suunnitteluun, herää kysymys siitä, voidaanko niillä tosiasiallisesti loukata toisen yksilön suojattuja yksityisyyden etuja. *Brownsword* kysyy, mitä meidän pitäisi ajatella tällaisesta sisäänrakennetusta tietosuojasta, kun on kyse toimenpiteiden mahdollisesta vaikutuksesta käytännön vapausoikeuksiin. Mitä syitä sääntelyn epäröintiin voisi olla?[193]

Yhtenä huolenaiheena on, että poistamalla käytännön vaihtoehdot tehdä väärin ei olisi enää moraalista hyvettä muiden yksityisyyden etujen kunnioittamiseen. Toisin sanoen moraalisen yhteisön konteksti voisi heikentyä. Toiseksi, kun otetaan huomioon, että yksityisyyden suojan luonne, laajuus ja painoarvo on usein kiistelty aihe niin etiikassa kuin oikeudellisessa kontekstissa, on olemassa todellinen vaara, että toimijat joutuvat joko toimimaan omaatuntoaan vastaan tai heitä rajoitetaan tekemästä sitä, mitä he pitävät oikeana asiana. Kolmanneksi, vaikka kansalaiset ovat olleet laajasti mukana, ennen kuin teknologiaan liittyvät oikeudelliset suuntaviivat hyväksytään, saatamme kyseenalaistaa sen, onko mahdollisuus itsesääntelyyn säilytettävä. Luotamme tiettyihin oikeudenaloihin, kuten vahingonkorvaus- ja sopimusoikeuteen. Niillä emme ainoastaan yritä suojella yksityisyyttä vaan pyrimme jatkuvasti vaikuttamaan muiden suojattujen intressiemme laajuuteen. Tyypillisesti näiden erityisintressien olemassaolo ja laajuus kiistetään ja ratkaisu annetaan sen perusteella, mitä voimme kontekstissa kohtuudella odottaa[194]. Tietenkin silloin, kun kohtuulliset odotuksemme viittaavat siihen, mitä voimme käytännössä odottaa, on olemassa vaara, että kohtuullisuuden linjat muodostetaan uudelleen niin, että yksityisyyden suojamme laajuus ja vahvuus heikkenevät. Neljänneksi ja jokseenkin samalla tavalla liberaalit toimijat saattaisivat arvostaa sitä, että "paikallisille" ryhmille ja tietyille yhteisöille varataan mahdollisuus asettaa omat norminsa. Liberaalit voivat olla huolissaan myös siitä, että sisäänrakennettua tietosuojaa voidaan pitää holhoavan teknologisen johtamisen välineenä, sillä siinä ei ole opt-out-mahdollisuutta.[195]

Lisäksi on olemassa vahva väite siitä, että sisäänrakennettu tietosuoja on ristiriidassa yhden hallitsevan ohjelmistokehitysmallin kanssa. Niin sanotussa ketterässä ohjelmistokehityksessä ohjelmisto rakennetaan iteroivilla[196] prosesseilla mieluummin kuin ylhäältä alas ennalta mietittyjen suunnitelmien perusteella.[197] Toisaalta 25 artikla on luonteeltaan suostutteleva: siinä tunnustetaan, että pyrkimyksiä siirtyä kohti sisäänrakennettua tietosuojaa rajoittavat tekniikan taso, täytäntöönpanokustannukset ja kyseessä olevan käsittelyn luonne. Toisaalta ei ole

[193] Brownsword, 2017, s. 62.
[194] Koops – Leenes, 2005, s. 115.
[195] Brownsword, 2017, s. 63–64.
[196] Iterointi on yleinen nimitys menetelmille, joissa työvaiheita toistetaan, kunnes saavutetaan haluttu tulos.
[197] Ks. Gürses – van Hoboken, 2017, s. 18.

epäilystäkään siitä, että siinä kannustetaan käyttämään kehittyvää tietosuojatekniikkaa ja kiinnittämään huomiota ajatukseen, että käyttäjät omistavat henkilötietonsa.[198]

Sisäänrakennettua tietosuojaa voidaan käyttää sekä positiivisessa että negatiivisessa mielessä. Positiivisena elementtinä se toimii toden teolla eräänlaisena yrityskuvan parantajana antaen potentiaalisille rekisteröidyille ja organisaation yhteistyökumppaneille kuvan hyvästä tietojenkäsittelytavasta, ja yritys saa näin heidän luottamuksensa. Toisaalta negatiivisessa mielessä sitä voidaan käyttää myös markkinointikikkana, jonka ajatuksena on viestiä organisaatiosta positiiviseen sävyyn, eikä kyse ole niinkään tarkoituksenmukaisesta suunnitelmasta hallita yksityisyyttä. Negatiivista voi olla myös se, että teknologiat saattavat sumentaa käsitystämme esimerkiksi suostumuksen antamisesta. Tämä johtuu siitä, että ohjelmistoratkaisuilla voidaan nykyään tehdä ainakin kaksi asiaa: 1) tarjota parempia tai mielekkäämpiä tapoja antaa (ja peruuttaa) suostumus ja 2) ennustaa ja ehkä korvata väitetty suostumus, jos aiemmat kokemukset osoittavat, että käyttäjä todennäköisesti olisi suostunut (tai ei).[199]

Sisäänrakennetun tietosuojan vaatimukset tulee suhteuttaa käytettävissä olevan tekniikan tasoon, toteuttamiskustannuksiin ja käsiteltävänä olevien tietojen laatuun. Lisäksi käsittelyssä tulee ottaa huomioon käsittelyn luonne, asiayhteys, laajuus sekä tarkoitus. Samalla asetus velvoittaa ottamaan huomioon käsittelystä mahdollisesti aiheutuvat riskit, niiden vakavuus ja todennäköisyys. Vaatimuksia voidaan selvittää TSA 35 artiklan mukaisella vaikutuksenarvioinnilla.[200]

Vaikka käsite on laaja, sisäänrakennettua tietosuojaa käytetään usein viittaamaan yritysten itsesääntelytoimenpiteisiin. Muissa tilanteissa se rinnastetaan enemmänkin hyvään tietoturvaan kuin holistisempaan lähestymistapaan, jota *Ann Cavoukian* on kutsunut yksityisyyden leipomiseksi osaksi organisaation ja tekniikan suunnittelun kaikkia osa-alueita.[201]

3.2. Oletusarvoinen tietosuoja

Oletusarvoisen tietosuojan osalta TSA edellyttää, että teknisillä ja organisatorisilla toimenpiteillä varmistetaan, että kulloinkin käsitellään vain tarpeellisia henkilötietoja. Toimenpiteillä tuleekin varmistua siitä, että henkilötiedot eivät päädy ennalta rajoittamattoman henkilöjoukon saataville.[202] Samalla oletusarvoisen tietosuojan käsitteeseen voidaan lukea ajatus siitä, että

[198] Ks. ENISA – Privacy and Data Protection by Design - from policy to engineering, 2014, s. 52–53.
[199] Edwards, 2019, s. 161–164.
[200] WP 248, s. 4.
[201] Hartzog, 2018, s. 5.
[202] Korpisaari, ym., 2018, s. 280.

sillä pyritään suojaamaan luonnollisia henkilöitä ylimääräisten tietojen keräämiseltä. TSA pyrkii tällä tavoin vaikuttamaan erityisesti sellaisten luonnollisten henkilöiden oikeuksiin, joilta puuttuvat riittävät tekniset tietotaidot itsensä suojelemiseen.[203]

Keskeistä onkin, että tietojen minimointi lähtee oletusarvosta kehitettäessä erilaisia järjestelmiä ja toteutettaessa tietojen keräämistä. Tämä ajatus tulee olla rekisterinpitäjällä ja käsittelijällä sisäistettynä ennen toimenpiteisiin ryhtymistä. Tällä puolestaan saavutetaan tavanomaisena liiketoimintana turha tietojen kerääminen esimerkiksi tiedonlouhintaa varten tai kohdennettua mainontaa. Ajatuksena onkin, että käytännön toteutus lähtee alhaalta ylöspäin eikä ylhäältä alas. Ajatus ei niinkään ole siten se, että ensin suunnitellaan ja arvioidaan myöhemmin tietosuojan toteutusta vaan päinvastoin, ennen suunnitteluun lähtemistä tulee jo ottaa ensimmäisenä huomioon tietosuojan toteutuminen.[204] Ajatuksen tasolla oletusarvoista tietosuojaa voi miettiä käytännönläheisesti siten, että kun yövyt hotellissa ja haluat aamulla nukkua rauhassa pitkään, perinteisesti olet laittanut oveen kyltin, jonka mukaan sinua ei saa häiritä. Oletusarvoisesti tämän tulisi kuitenkin olla tavallaan toisinpäin. Sinun tulisi laittaa oveen kyltti, jonka mukaan sinua saa häiritä. Tällöin henkilökunta olettaa, että haluat olla rauhassa eikä ryntää herättämään sinua. Samoin tietosuojan toteutuksen tulee toimia. Käytössä tulee olla lähtökohtaisesti keinoja, joiden avulla pystyy helposti ilmoittamaan, ettei minua saa häiritä. Aina se ei ole mahdollista, mutta tärkeintä on oletuksena tarkastella, voisiko tilanteessa järjestää tällainen vaikutusmahdollisuus. Tietyissä tilanteissa puolestaan tämä vaikutusmahdollisuus estyy jo lain tasolla. Näitä esimerkkejä on käsitelty jo aikaisemmin.

Suositeltuihin toimenpiteisiin sisäänrakennetun tietosuojan mahdollistamiseksi sisältyy TSA:n 25 artiklan perusteella tietojen pseudonymisointi sekä tiedonkeruun minimointi. Erityisesti 25 artiklassa suositellaan, että oletusarvoisesti sovellukset ja järjestelmät keräävät vain käyttäjien ilmoittamien tarkoitusten saavuttamiseksi tarvittavat tiedot. Tietojen minimointi on tietysti nyt myös erillinen tietosuojaperiaate, mutta liiketoimintakäytäntönä tämä säännös merkitsee huomattavaa muutosta normeissa, etenkin yrityksille, jotka ovat riippuvaisia tiedonlouhinnasta ja kohdennetusta mainonnasta.

Oletusarvon vaatimus tarkoittaa, että yritysten olisi toteutettava toimenpiteitä keräämiensä henkilötietojen rajoittamisen tai minimoinnin lisäksi myös paremmasta valvonnasta niiden käsittelyn laajuudessa. Säilytysaika tarkoittaa, että yritysten tulisi oletusarvoisesti käsitellä henkilötietoja vain siinä määrin kuin se on tarpeen niiden tarkoituksiin. Tietoja ei pitäisi tallentaa

[203] Korpisaari, ym., 2018, s. 280.
[204] Edwards, 2019, s. 110–111.

kauemmin kuin on tarpeen näihin tarkoituksiin. Henkilötietoja on oletusarvoisesti säilytettävä vain tuotteen tai palvelun toimittamiseen tarvittavan ajan. Siinä missä aikaisempi direktiivi pyrki rajoittamaan ylimääräisen tiedon käsittelyä, TSA:n 25 artikla asettaa tämän velvollisuuden, jonka laiminlyönnistä voi seurata hallinnollinen seuraamusmaksu.[205]

Oletusarvoinen tietosuoja vaikuttaa suunnitteluprosessiin eräänlaisen pakollisen tarkastuksen muodossa. Se voidaan myös tulkita tiukemmin suunnitteluvaatimukseksi, jossa oletusarvoisesti on tarjottava ja aktivoitava suojaavimmat yksityisyyden suoja-asetukset käyttäjän saataville.[206] Esimerkiksi yksi sosiaalisen median palveluiden ensisijaisista ongelmista on se, että ne on suunniteltu kannustamaan ihmisiä paljastamaan mahdollisimman paljon tietoja itsestään antaen tilaa vain hyvin vähän miettiä mahdollisia seurauksia. Monien sosiaalisen median palveluiden oletusasetukset painottavat avoimuutta yksityisyyttä enemmän. Pelkkä oletusasetusten muuttaminen saattaa siten suojata monia ihmisiä. Eri verkkosivustojen asetukset tai selainten asetukset voivat olla yksi tärkeimmistä vaikutuksista yksityisyyteen tulevaisuudessa.[207] Siksi TSA kannustaa yrityksiä miettimään, miten niiden verkkosivustojen suunnittelu vaikuttaa yksityisyyteen.

4. REKISTERINPITÄJÄN TEKNISET JA ORGANISATORISET TOIMENPITEET

4.1. Yleistä

Tutkimuksen aiheena on tarkastella TSA:ssa rekisterinpitäjälle asetettua velvollisuutta suorittaa tekniset ja organisatoriset toimenpiteet osana sisäänrakennettua ja oletusarvoista tietosuojaa. Sisäänrakennettu tietosuoja edellyttää TSA:n mukaan sitä, että rekisterinpitäjä toteuttaa sekä tietojärjestelmän suunnittelun että noudattaa itse käsittelyn yhteydessä tietosuojaperiaatteita niin teknisesti kuin organisatorisestikin.[208] Rekisterinpitäjällä tarkoitetaan TSA 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. Henkilötietojen käsittelijällä tarkoitetaan TSA 4 artiklan 8 kohdan perusteella luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.

[205] Pothos, 2018 s. 203
[206] Ks. Bygrave, 2017, s. 754–775.
[207] Solove, 2007, s. 201.
[208] Korpisaari, ym., 2018, s. 279. Esimerkkejä sisäänrakennetusta tietosuojasta ks. esim. Romanou, 2017, s. 104–108.

Keskeisenä kysymyksenä on selvittää ensinnäkin se, mitkä ovat tekniset ja organisatoriset toimenpiteet sekä mikä on asetuksen tekstin mukaisesti asianmukaista kulloisessa tilanteessa. Ensinnäkin jako voidaan tehdä teknisiin toimenpiteisiin sekä hallinnollisiin eli organisatorisiin toimenpiteisiin. Teknisillä ja organisatorisilla toimenpiteillä tarkoitetaan esimerkiksi tietoturvatoimenpiteitä, henkilöstön koulutusta, henkilöstölle annettuja ohjeita ja määräyksiä, salassapitosopimuksia, tilavalvontaa, tietojen salausta, tietojen anonymisointia ja pseudonymisointia, auditointeja, etäkäyttöyhteyksiä, teknisiä rajoituksia, tarkastus- ja valvontajärjestelmiä, tietotilinpäätösprosessia, käytännesääntöjä ja sertifikaattien käyttöönottoa.[209] Tutkimuksessa käsittelen näitä toimenpiteitä irrallaan toisistaan. Koska TSA edellyttää sitä, että toimenpiteet tulee myös pystyä näyttämään toteen, käsittelen erillisenä osana osoitusvelvollisuutta, sillä rekisterinpitäjän tulee osoittaa toimenpiteiden suorittaminen.

Rekisteripitäjän tulee tehdä asianmukaiset tekniset (suoja)toimenpiteet, joilla rekisteröidylle aiheutuvaa riskiä voidaan vähentää hyväksyttävälle tasolle. Tässä yhteydessä puhutaankin usein tietoturvallisuuden toteuttamisesta, milloin se mielletään osaksi TSA:n 32 artiklaa. Näinhän asia käytännössä onkin. TSA 32 artiklassa luetellaan joukko erityisiä turvatoimenpiteitä, joita voidaan käyttää. Näitä ovat esimerkiksi henkilötietojen pseudonymisointi ja salaus, järjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa.[210] Tietoturva on osa asianmukaisia teknisiä ja organisatorisia toimenpiteitä ja samalla keino toteuttaa sisäänrakennettua ja oletusarvoista tietosuojaa. Yksilön näkökulmasta on tärkeää, että tietoturva otetaan huomioon kaikissa henkilötietojen käsittelyn prosesseissa. Siksi on relevanttia käsitellä myös tietoturvakysymyksiä osana tätä tutkimusta. On selvää, että henkilötietojen käsittely tässä yhteydessä riittävän tietoturvallisuuden varmistamiseksi on rekisterinpitäjän oikeutettu etu, kunhan käsittely on ehdottoman välttämätöntä ja oikeassa suhteessa sillä tavoiteltuun tarkoitukseen. Hallinnollisiin eli organisatorisiin toimenpiteisiin puolestaan kuuluvat toimintalinjaukset, periaatteet, organisaatiojärjestelyt, henkilöstön tehtävien ja vastuiden määrittelyt sekä ohjeistus, koulutus ja valvonta.[211]

Toteuttaessaan asianmukaisia teknisiä ja organisatorisia toimenpiteitä kuten TSA 25 artiklassa odotetaan, rekisterinpitäjien on otettava huomioon muut tekijät, mukaan lukien *tekniikan taso, toteutuskustannukset ja käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset samoin kuin [siitä aiheutuvat] riskit*. Riskipositiona pidetään lähtökohtaisesti läpi TSA:n yksilöön eli

[209] Alapuranen, ym., 2020, s. 67.
[210] TSA 32 artiklan 1 kohdan a–c alakohdat.
[211] Jay, ym., 2017, s. 134.

rekisteröityyn kohdistuvia riskejä. Termi *asianmukainen* toimenpide merkitsee sitä, että asetus ei edellytä absoluuttista turvallisuutta ja rajoittamattomia hallinnollisia järjestelyjä. Siten rekisterinpitäjä voi selvitä ilman sanktioita esimerkiksi tietoturvamurrosta, jos toimenpiteet ovat olleet riittäviä tietojen suojaamiseksi. Tämä johtunee siitä, että lainsäätäjä ei voi pitää organisaation epäonnistumista tietoturvatoimen-piteissä suoraan myös oikeudellisena virheenä. TSA:n 32 artikla edellyttääkin rekisterinpitäjältä riskiperusteista lähestymistapaa, jolla voidaan määrittää mikä on tai ei ole riittävä toimenpide.

Aikaisemmin tutkielmassa olen pyrkinyt esittämään mahdollisimman suoraviivaisesti TSA:n sisältöä. Läpi asetuksen rekisterinpitäjältä edellytetään kuitenkin tilannesidonnaista arviointia käsittelyn sisältämistä (potentiaalisista) riskeistä. Tilannesidonnaisuudesta johtuu, että riskiperusteisen lähestymistavan seurauksena ei ole mahdollista esittää ehdottomia ja tarkkarajaisia tulkintoja. Riskiarvioinnissa tulee huomioida lisäksi ns. *state-of-the-art*-vaatimus, jossa rekisterinpitäjän edellytetään käyttävän uusinta teknologiaa tietoturvallisuudesta ja rekisteröityjen yksityisyyden turvaamiseksi ottaen kuitenkin huomioon tällaisen teknologian käyttämisestä aiheutuvat kustannukset. TSA:n 25 artiklassa annetaan rekisterinpitäjälle mahdollisuus ottaa huomioon toimenpiteiden aiheuttamat kustannukset. Tietosuojaneuvoston ohjeistuksessa todetaan, että rekisterinpitäjältä ei edellytetä kohtuuttoman paljon resursseja käytettäväksi, kun vaihtoehtoisia, vähemmän resursseja vaativia mutta tehokkaita toimenpiteitä on olemassa. Täytäntöönpanokustannukset ovat kuitenkin tekijä, joka on otettava huomioon sisäänrakennetussa tietosuojassa eivätkä ole syy sen toteuttamatta jättämiselle. Valituilla toimenpiteillä on varmistettava, että rekisterinpitäjän ennakoiman käsittelyn seurauksena ei käsitellä henkilötietoja periaatteiden vastaisesti kustannuksista riippumatta.[212] Tällä tarkoitetaan sitä, että rekisterinpitäjiä ja käsittelijöitä vaaditaan pohtimaan tietoturvallisuuden ammatillista mielipidettä. Tämä johtaa siihen, että jos kohtuullisen tietoisten tietoturvallisuusalan ammattilaisten joukko katsoo, että tietty turvaamistoimenpide on tarkoituksenmukaista kyseisissä olosuhteissa, rekisterinpitäjän tulisi ottaa se huomioon tehdessään päätöstä tietoturvatoimenpiteen soveltamisesta käyttöympäristöön.[213] TSA:n johdanto-osan 78 perustelukappaleessa todetaan asianmukaisista toimenpiteistä seuraavaa:

> *Luonnollisten henkilöiden oikeuksien ja vapauksien suoja henkilötietojen käsittelyssä edellyttää, että toteutetaan asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla varmistetaan, että asetuksessa säädetyt vaatimukset täyttyvät -- rekisterinpitäjän olisi hyväksyttävä sisäisiä menettelyjä ja toteutettava toimenpiteet, jotka vastaavat erityisesti sisäänrakennetun ja oletusarvoisen tietosuojan periaatteita. Tällaisia toimenpiteitä [ovat] henkilötietojen käsittelyn minimointi, henkilötietojen pseudonymisointi mahdollisimman*

[212] Tietosuojaneuvoston ohjeistus, kohdat 24 ja 25.
[213] Room, 2018, s. 173.

> *pian, tehtävien ja henkilötietojen käsittelyn läpinäkyvyys, sen mahdollistaminen, että rekisteröity voi valvoa tietojenkäsittelyä ja että rekisterinpitäjä voi luoda ja parantaa turvaominaisuuksia. -- tuotteiden, palvelujen ja sovellusten tuottajia olisi kannustettava ottamaan huomioon oikeus tietosuojaan niiden kehittäessä ja suunnitellessa tällaisia tuotteita, palveluja ja sovelluksia ja varmistamaan uusin tekniikka asianmukaisesti huomioon ottaen --.*[214]

Teknisiä toimenpiteitä, joihin johdannon perusteella tulee ryhtyä, ovat 1) käsiteltävien henkilötietojen määrän minimointi, 2) pseudonymisointi ja 3) yksilöille annettavat paremmat mahdollisuudet hallita henkilötietojaan ja 4) lisäämällä näkyvyyttä siihen, miten tietoja käsitellään. Toisin sanoen kyse on läpinäkyvyydestä, joka on yksi yleisistä tietosuojaperiaatteista TSA:n 5 artiklassa. Muita toimenpiteitä ovat asianmukaisten turvallisuusstandardien soveltaminen hallussa oleviin henkilötietoihin. TSA:n 25 artiklan noudattamisen varmistamiseksi yritysten olisi tarkasteltava ja arvioitava huolellisesti tietojenkäsittelyjärjestelmiään ja toimintaansa yleensä selvittääkseen, onko 1) henkilötiedot koottu, luokiteltu, merkitty, säilytetty ja niihin pääsy järjestetty helpoksi, jos rekisteröity pyytää joko toimittamaan henkilötietoja tai oikaisemaan tai poistamaan henkilötietoja, 2) järjestelmät valmisteltu henkilötietojen automaattista poistamista varten, 3) paperipohjaiset lomakkeet ja hakemukset tai muut tiedonkeruulomakkeet laadittu asianmukaisesti sen varmistamiseksi, ettei liiallisia henkilötietoja kerätä, 4) henkilötiedot salattu, sikäli kuin se on mahdollista, 5) henkilötiedot erotettu siten, että suoramarkkinointiviestien vastaanottamista vastustaneiden henkilöiden henkilötiedot voidaan poistaa ja 6) henkilötiedot järjestetty yleisesti käytettyyn, koneellisesti luettavaan ja yhteen toimivaan muotoon, jotta yritys voi täyttää tiedonsiirron vaatimukset.[215]

Tekniset ja organisatoriset toimenpiteet ja tarvittavat suojatoimet voidaan ymmärtää laajassa merkityksessä tavaksi tai keinoksi, jota rekisterinpitäjä voi käyttää henkilötietojen käsittelyssä. Tarkoituksenmukaisuus tarkoittaa, että toimenpiteiden ja tarvittavien suojatoimien olisi sovelluttava aiotun tarkoituksen saavuttamiseen eli niiden on pantava tietosuojaperiaatteet tehokkaasti täytäntöön. Tekninen, organisatorinen tai suojatoimenpide voi olla mitä tahansa kehittyneiden teknisten ratkaisujen käytöstä henkilöstön peruskouluttamiseen.

Kun asianmukaisia teknisiä ja organisatorisia toimenpiteitä pannaan täytäntöön, toimenpiteet ja suojatoimet olisi suunniteltava yleisten tietosuojaperiaatteiden tehokasta täytäntöönpanoa ja siitä seurauksena olevaa oikeuksien suojelua silmällä pitäen. Tehokkuus on osa sisäänrakennetun tietosuojan käsitteen ydintä. Vaatimus periaatteiden tehokkaasta täytäntöönpanosta tarkoittaa, että rekisterinpitäjien on toteutettava tarvittavat (suoja)toimenpiteet yleisten tietosuojaperiaatteiden kanssa rekisteröidyn oikeuksien turvaamiseksi. Kunkin toteutetun toimenpiteen olisi

[214] TSA johdanto-osan 78 perustelukappale.
[215] Pothos, 2018, s. 204.

tuotettava odotetut tulokset rekisterinpitäjän ennakoimaan käsittelyyn, millä on kahdenlaisia seurauksia. Ensinnäkään 25 artiklassa ei edellytetä minkään erityisen teknisen tai organisatorisen toimenpiteen täytäntöönpanoa vaan että valittujen toimenpiteiden ja suojatoimien olisi oltava erityisiä tietosuojaperiaatteiden täytäntöönpanossa kyseistä käsittelyä varten. Näin toimenpiteet ja suojatoimet olisi suunniteltava vahvoiksi, ja rekisterinpitäjän olisi voitava toteuttaa lisätoimenpiteitä riskien mahdollisen kasvun seurauksena. Se, ovatko toimenpiteet tehokkaita, riippuu näin ollen käsittelyn asiayhteydestä ja tiettyjen elementtien arvioinnista, jotka olisi otettava huomioon käsittelykeinoja määriteltäessä. Lisäksi rekisterinpitäjän tulee pystyä näyttämään, että periaatteita on noudatettu. Tehokkuutta voidaan ohjeistusten mukaisesti arvioida esimerkiksi käyttäen KP-indikaattoria[216] (Key Performance Indicator).

Rajan asettaminen siihen, mikä on kulloinkin asianmukaista ei ole yksinkertaista. Oikeuskäytäntöä on asiasta suhteellisen vähän erityisesti EU:ssa. Samoin kansallisissa yhteyksissä ei ole vielä ehditty käsittelemään aihetta TSA:n tuoreuden vuoksi. Yhdysvalloissa taas on paljonkin käsitelty asianmukaisuutta tietosuojakäytännöissä. Keskeistä on kuitenkin huomata, ettei seuraavista tapauksista voida suoraan tehdä johtopäätöksiä EU-oikeudesta. Tämä siitä syystä, että sääntelypohja on EU:ssa erilainen. Tapauksessa *FTC v. Wyndham Worldwide Corp.* tuomioistuin katsoi, että tietovuodot johtuivat riittämättömistä turvatoimista, ja yrityksen epäonnistuminen kohtuullisen ja asianmukaisen tietoturvan ylläpitämisessä oli epäreilua käytäntöä.[217] Samoin myös tapauksessa *In re: Facebook Inc., v. FTC* arvioitiin rekisterinpitäjän käytäntöjen asianmukaisuutta. Facebookin tietosuojakäytännön muutokset johtivat siihen, että sen käyttäjien tiedot paljastuivat julkisuuteen. FTC:n mielestä kyse oli hämäämisestä (ilmoittamatta jättäminen ihmisille asianmukaisesti) sekä epäoikeudenmukaisuudesta (aineellisen muutoksen tekeminen taannehtivasti yksityisyyden suojaan ilman kuluttajan suostumusta). Facebook ei ollut noudattanut Safe Harbor -periaatteita[218] ilmoituksen ja valinnan suhteen.[219] On ehkä selvää, että tapauksessa *In re: DesignerWare LLC., v. FTC* kyse ei ollut asianmukaisesta toiminnasta, kun asiakkaan tietämättä tietokoneella ollut ohjelmisto nimeltään *Detective Mode* otti

[216] KP-indikaattorilla tarkoitetaan suorituskykyyn perustuvaa mittaustyyppiä. Suorituskykyilmaisimet arvioivat organisaation tai tietyn toiminnan (kuten projektien, ohjelmien, tuotteiden ja muiden aloitteiden) onnistumista. Tällaisten indikaattoreiden merkitys näkyy tyypillisesti päätöksentekoprosessissa. Suorituskykyilmaisin antaa valmiudet analysoida vallitsevaa tilannetta tulevien toimien seurausten ennustamiseksi. Suorituskykyilmaisimen asianmukainen käyttö vähentää virheitä ja minimoi riskejä.
[217] FTC v. Wyndham Worldwide Corp. No. 13-1887 F.3d 236 (3d Cir. 2015).
[218] Vuonna 2015 EUT tulkitsi, että *Safe Harbour* -järjestely on pätemätön. Myöhemmin se korvattiin ns. *Privacy Shield* järjestelyllä vuonna 2016, minkä EUT kumosi ns. *Schrems II* -ratkaisussaan (C-311/18). Nykyisin henkilötietojen siirto EU:n talousalueen ulkopuolelle on mahdollista lähtökohtaisesti vain, jos henkilötietojen käsittely on sallittua kansallisesti ja siirrolle on olemassa TSA V luvussa määritelty siirtoperuste.
[219] In re: Facebook, FTC No. 092-3184, Docket No. C-4365, (2012).

kuvakaappauksia luottamuksellisista ja henkilökohtaisista tiedoista, kirjasi asiakkaiden tietokoneiden näppäilyä ja otti tietyissä tapauksissa verkkokamerakuvia ihmisistä omissa taloissaan.[220]

Näistä ja muista tapauksista voidaan tehdä eräänlaisia johtopäätöksiä asianmukaisuuden vaatimuksesta Yhdysvalloissa.[221] Tietosuojakäytännöistä FTC:lle tehdyt kantelut johtuvat 1) puutteellisesta tietoturvallisuudesta, jossa erityisesti luvataan mutta ei tarjota tosiasiallisesti riittävää tietoturvaa, 2) tietoturvavirheistä ja kouluttamatta jättämisestä, 3) tietosuojaselosteessa annettujen lupausten noudattamatta jättämisestä, 4) tietosuojakäytännön taannehtivista muutoksista, joilla mahdollistetaan esimerkiksi henkilötietojen luovuttaminen aikaisempaan nähden ilman, että yksilöiltä pyydetään suostumusta muutokseen, 5) hämäävästä tiedonkeruusta, jossa rekisteröidyt eivät edes käy yrityksen verkkosivustolla tai käytä sitä ja 6) tietojen keräämisen laajuuden puutteellisesta ilmaisemisesta, jonka puitteissa rekisteröidylle ei ilmoiteta selkeästi ja näkyvästi internetselaimen seurannan laajamittaisuudesta. Mielestäni on varsin selvää, että Yhdysvalloissa käydyt keskustelut asianmukaisuudesta liittyvät hyvin perustavaa laatua oleviin kysymyksiin. Edellä mainitut esimerkit ovat selkeästi vastoin eurooppalaista tietosuojakäytäntöä. Yhdysvalloissa asianmukaisuuden kohdalla puhutaan epäreiluudesta, mikä osaltaan kuvaa hyvin tietoturvaloukkauksia. Kyse on rekisteröidyn kannalta epäreilusta tilanteesta. TSA edellyttää selkeästi korkeampaa turvallisuusstandardia, joka Yhdysvalloissa on hyväksytty. Tästä syystä lieneekin, että tietojen siirtoa kolmansiin maihin pidetään arveluttavana.

4.2. Organisatoriset toimenpiteet

4.2.1. Riskiperusteinen lähestymistapa

Henkilötietojen käsittelystä aiheutuu aina jonkin verran riskiä, mikä ei aiheuta käytännön huolta. On selvää, että kaikkia riskejä on mahdotonta poistaa. Riskien täydellinen poistaminen on melkein yhtä mahdotonta kuin tulevien luonnonmullistusten estäminen. TSA edellyttää rekisterinpitäjältä tästä syystä riskiperusteista lähestymistapaa. Riskiperusteinen lähestymistapa on johdettavissa erityisesti TSA:n 24 artiklan sisällöstä. Lisäksi TSA:n 32 artiklan 2 kohdassa edellytetään kiinnitettävän huomiota erityisesti käsittelyn sisältämiin riskeihin. Kuten on huomattu, termiä *riski* käytetään asetuksessa hyvin laajasti, ja se voi helposti aiheuttaa epäselvyyttä. Riski liittyy kaikkeen henkilötietojen käsittelyyn. Rekisterinpitäjä joutuu jopa ottamaan tietoisesti riskiä henkilötietojen käsittelyssä tilanteissa, joihin ei ole selkeää vastausta.

[220] In re: DesignerWare, LLC, No. 112 3151, Docket No. C-4390, (2013).
[221] Ks. esimerkiksi In re: Microsoft Corp., FTC, Docket No. C-4069, (2002); In re: Eli Lilly & Co., FTC Docket No. C-4047, (2002); In re: Liberty Fin. Cos., FTC Docket No. C-3891, (1999); In re: Sears Holdings Mgmt. Corp., FTC No C-4264 (2009).

Riskiperusteisessa lähestymistavassa riskejä tulee pohtia suhteessa rekisterinpitäjän käytettävissä oleviin resursseihin. Tästä syystä on tärkeää suorittaa *riskienarviointi* huolella.

Tietoturvariskit, jotka tulee arvioida TSA:n mukaisesti, ovat sellaisia, jotka kohdistuvat luonnollisen henkilön oikeuksiin ja vapauksiin henkilötietojen käsittelyn yhteydessä. TSA:n lähtökohta on minimoida yksilölle aiheutuvia riskejä. Riskejä, jotka voivat aiheutua siten yritykselle itselleen tai henkilötietojen käsittelijälle, ei tule tässä yhteydessä arvioida. Mikään ei tietysti estä arvioimasta omalle organisaatiolle aiheutuvia riskejä, mutta asetus ei sitä edellytä. Rekisterinpitäjän valitessa esimerkiksi henkilötietojen käsittelijää voi tällainen arviointi olla paikallaan, sillä huolimattomasti toteutettu käsittelijän valinta voi johtaa huonoon tulokseen. Riskejä voi syntyä tietoturvallisuusstandardeista joustamisesta, jos luonnollisen henkilön tietoja säilytetään esimerkiksi virheellisesti tai jos tiedot eivät ole ajan tasalla. Riskien arvioinnissa on hyvä pitää lisäksi mielessä, että sekä rekisterinpitäjän että käsittelijän tulee arvioida, mitä voi mennä pieleen tietoturvaloukkauksen yhteydessä. Arvioinnissa tulee ottaa lisäksi huomioon käsittelyn luonne, laajuus, konteksti ja käsittelyn tarkoitus sekä käsittelyn potentiaaliset riskit.[222]

Rekisteröidyn oikeuksiin ja vapauksiin kohdistuvan riskin todennäköisyys ja vakavuus on määriteltävä tietojenkäsittelyn luonteen, laajuuden, asiayhteyden ja tarkoituksen mukaan. Riski on arvioitava objektiivisesti ja pohdittava, liittyykö tietojen käsittelytoimiin riski tai korkea riski.[223] Tämä edellyttää, että rekisterinpitäjä tuntee henkilötietojen käsittelyn tavat ja prosessit organisaatiossa. Riskienarvioinnissa hyväksyttyjen käytännesääntöjen ja sertifiointien tai tietosuojaneuvoston suuntaviivojen avulla taikka tietosuojavastaavan tiedotteilla voidaan hakea vastauksia siihen, onko rekisterinpitäjä tai henkilötietojen käsittelijä täyttänyt asianmukaisesti vaaditut toimenpiteet ja ovatko toimenpiteet toteutuneet.[224]

Asetuksessa ei ole mainittu sitä, milloin riskienarviointi tulee tehdä toisin kuin vaikutuksenarviointiin liittyen. Vaikutustenarviointia käsitellään lähemmin kappaleessa 4.4.1. Tutkimuksen kannalta keskeisenä lähtökohtana voitaneen pitää sitä, että sisäänrakennettu ja oletusarvoinen tietosuoja edellyttää riskien arvioinnin suorittamista mahdollisimman aikaisessa vaiheessa, kun henkilötietojen käsittelyä suunnitellaan. Tässä yhteydessä mielestäni voisi todeta, että arvioinnin suhteen voidaan antaa tilaa myös taiteelliselle luovuudelle. Tarkoitan tällä sitä, että koska tietoturvaloukkauksia on monenlaisia, myös seuraukset voivat olla moninaisia. Tällöin arvioinnissa tulisi kiinnittää huomiota myös täysin utopistisiin mahdollisuuksiin, jotka kuitenkin ovat potentiaalisia. Monet tietoturvaloukkaukset ovatkin johtaneet seurauksiin, kun ei ole

[222] Jay, ym., 2017, s. 133.
[223] TSA johdanto-osan 75 perustelukappale.
[224] Korpisaari, ym., 2018 s. 272.

ymmärretty uskoa potentiaalisiin uhkakuviin, joita yleensä kyberhyökkäysten toteuttajat hyödyntävät. Jos riskejä havaitaan, tulee rekisterinpitäjän ja henkilötietojen käsittelijän ryhtyä riittäviin toimenpiteisiin riskien poistamiseksi tai ainakin niiden minimoimiseksi. Toisaalta toimenpiteisiin ryhtymisessä tarvitaan myös punnintaa sen suhteen, onko järkevämpää kohdistaa toimenpiteet ennakollisiin ratkaisuihin vai reagointikyvyn kehittämiseen. Vaikka riskeihin voidaankin varautua ennakolta, niitä ei voida kuitenkaan täydellisesti poistaa. Siten reagointikykyyn tulee myös panostaa, sillä rekisteröidyn henkilötietojen suojan kannalta jopa keskeisemmässä asemassa on se, että tietoturvaloukkaustilanteissa yksilön tiedoille aiheutuvaa vahinkoa kyetään minimoimaan.

4.2.2. Koulutukset

TSA:n 32 artiklan 4 kohdan mukaan *[r]ekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava toimenpiteet sen varmistamiseksi, että jokainen rekisterinpitäjän tai henkilötietojen käsittelijän alaisuudessa toimiva luonnollinen henkilö, jolla on pääsy henkilötietoihin, käsittelee niitä ainoastaan rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita.*

On hyvä huomata, että kaikkiin työntekijöihin, joilla on pääsy henkilötietoihin sovelletaan tätä artiklaa. Tässä on hyvä huomioida kuitenkin se, että työntekijöiden täytyy toimia heille annettujen ohjeiden rajoissa eikä ylittää toimintavaltuuksiaan. Näin ollen artiklan puitteissa rekisterinpitäjän tulee huolehtia ohjeiden antamisesta. Vaikka henkilökunnan jäsen voikin syyllistyä rikokseen, on rekisterinpitäjä silti velvollinen noudattamaan TSA:ta. Näin ollen on työnantajan huolehdittava esimerkiksi siitä, ettei kukaan epätietoisena hyödynnä henkilötietoja omaksi tai jonkun kolmannen hyväksi sekä luotava henkilökunnalleen selvät ohjeistukset ja roolitukset. Rekisterinpitäjän kannattaa myös rakentaa työoikeuden säännöksiin perustuva seurausjärjestelmä mahdollisten väärinkäytösten käsittelemiseksi.[225] Huomiota on kiinnitettävä myös tilanteisiin, kun työsuhde päättyy irtisanomisen, eläkkeelle siirtymisen tai muun syyn vuoksi. Fyysinen omaisuus on tällöin palautettava, työntekijän henkilökohtaiset laitteet on puhdistettava organisaation tiedoista ja käyttöoikeudet on lopetettava ja riittävät työsuhteen päättymisen jälkeiset rajoitukset jatkuvan turvallisuuden ja luottamuksellisuuden takaamiseksi on aktivoitava. [226] Rikosoikeudellisista seuraamuksista kyseeseen voivat tulla esimerkiksi rikoslain (39/1889) 38 luvun tekomuodot, kuten 9 §:n tietosuojarikos, 3–4 §:ien (törkeä)

[225] Ks. Room, 2018, s. 175.
[226] Ibid., s. 185.

viestintäsalaisuuden loukkaus tai 8 § ja 8a §:n (törkeä) tietomurto. Lisäksi on huomioitava, että kyseeseen voi tulla vahingonkorvaus, josta säädetään TSA 82 artiklassa. Rekisterinpitäjä on velvollinen korvaamaan lainvastaisella henkilötietojen käsittelyllä aiheuttamansa vahingon. Lainvastaisella käsittelyllä tarkoitetaan henkilötietojen käsittelyä, jossa jätetään noudattamasta tietosuoja-asetusta, tietosuojalakia (1050/2018) sekä henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettua lakia (1054/2018). Sama koskee myös muuta erityislakia, jossa säädetään henkilötietojen käsittelystä. Vahingon lajilla ei ole niinkään väliä, sillä korvattavaksi tulevat niin aineelliset kuin aineettomat vahingot.

Työnantajan tulee muovata organisaatiota kokonaisuutena kohti riskitietoisuuden ja henkilötietojen kunnioittamisen kulttuuria osana sisäänrakennettua ja oletusarvoista tietosuojaa. Erityisesti tämä pätee työantajiin, joilla on direktio-oikeus työntekijöihinsä. Tämä siitä syystä, että rekisterinpitäjä on saattanut ulkoistaa henkilötietojen käsittelyn toiselle työnantajalle, jonka palveluksessa oleviin työntekijöihin varsinaisella rekisterinpitäjällä ei ole suoraa valtaa. Rekisterinpitäjä voi toki välillisesti esimerkiksi rekisterinpitäjän ja käsittelijän välisellä sopimuksella määritellä tarkempia ohjeita. Asianmukaiset organisatoriset toimenpiteet edellyttävät ohjelmaa, jolla upotetaan ja vahvistetaan oikeaa kulttuuriprofiilia ja käyttäytymistä työyhteisössä. Oikean kulttuurin saavuttamisessa keskeistä on pätevien ja luotettavien työntekijöiden valinta. *Room* pitää hyvän turvallisuuskulttuurin avainkomponentteina seuraavia asioita:

1) Ymmärretään ihmisriskit. Prosessi alkaa tunnistamalla työpaikan turvallisuusriskit ja se, miten niihin puututaan. Riskinarviointiprosessi tällä mikrotasolla asettaa riskien vähentämisen tien siitä eteenpäin.
2) Rekrytointiprosessilla suunnitellaan oikean henkilön saaminen työhön. Tapa, jolla tietoja ehdokkaista kerätään ja käsitellään, välittää arvon, jonka organisaatio asettaa turvallisuudelle ja luottamuksellisuudelle.
3) Työtarjouksessa ja työsopimuksessa rekrytointiprosessi tarjoaa ennakollisesti mahdollisuuden sisällyttää organisaation kulttuuri osaksi prosessia ja saattaa se hakijan tietoon. Näiden tulisi sisältää oikeat sanamuodot, jotka selittävät, mitä organisaatio odottaa ja miten sen odotukset saavutetaan.
4) Organisaatiolla on loistava tilaisuus esitellä uudelle tekijälle organisaation tietoturvakäytänteet työtarjouksen hyväksymisen jälkeen.
5) Perehdytyspäivä tarjoaa mahdollisuuden sisällyttää organisaation luottamuksellisuuden ja turvallisuuden puitteet perehdytykseen ja esimerkiksi kouluttaa roolikohtaisia tietosuojavelvoitteita.

6) Organisaatioiden on tarjottava jatkuvaa ja roolipohjaista koulutusta. Koulutus ei pääty aloituspäivään. Koulutus pitää työntekijät ajan tasalla käytänteistä, turvallisuusuhista ja heidän roolistaan niiden lieventämisessä.[227]

Organisaatiossa voidaan myös ohjeistuksilla huolehtia henkilötietojen suojasta ja turvallisuudesta. Voidaan sanoa, että kyberturvallisuus on yhtä riippuvainen yhteisistä pelisäännöistä kuin liikenneturvallisuus. Jos organisaatiossa huolehditaan siitä, että henkilökunta ymmärtää ja tiedostaa yleisimmät riskit, hallitsee perusperiaatteet ja käyttää tervettä järkeä, päästään jo pitkälle. Ainakin seuraavien seikkojen pohjalta organisaatio voi luoda ohjeistuksia henkilökunnalle:

1) Varmuuskopiointi ja tiedostojen salaus.[228]
2) Riittävän vahvat salasanavaatimukset ja salasanojen säännöllinen vaihtaminen.[229]
3) Käyttäjillä tulee olla eri salasanat eri järjestelmiin.[230]
4) Sähköpostiohjeistukset, joissa tunnistetaan epäilyttävät linkit sekä liitteet.[231]
5) Laitteisiin, joita organisaatiossa käytetään, ei tule liittää ulkopuolisia laitteita tai tuntemattomia järjestelmiä. Esim. muistitikut[232] ja sovellusten lataaminen.
6) Työsuhdepuhelinten suojaaminen.[233]
7) Tietokoneen päivittäminen aina uusimpaan versioon ja ohjelmistopäivitysten suorittaminen.[234]
8) Lisäksi terve maalaisjärki – jos jokin on epäilyttävää, ei sitä kannata tehdä.[235]
9) Jos työvälineitä käytetään myös työpaikan ulkopuolella, on syytä laatia etätyöskentelyyn ohjeistukset, joissa huomioidaan tietoturvan ja tietosuojan vaatimukset.

Lisäksi organisaatiossa on syytä ottaa huomioon laajemmin alaan vaikuttavat yksittäiset ohjeistukset tietosuojaan liittyen, ja niiden käytännön toteutukseen edellytetään ohjeistuksia myös

[227] Room, 2018, s. 184–185.
[228] Ks. Järvinen, 2012, s. 225–228.
[229] Ks. Ibid., s. 114–127 vrt. kuitenkin Järvinen, 2018, s. 306, missä Järvinen on uudistanut näkökulmaansa siinä, että käyttäjien pakottaminen alituisesti vaihtaman salasanoja johtaa siihen, että käyttäjät valitsevat huonoja ja helposti muistettavia salasanoja, mikä johtaa tietoturvan heikkenemiseen.
[230] Ks. Järvinen, 2012, s. 118.
[231] Sähköpostit saattavat tunnistaa roskapostin, mutta petolliset linkit saattavat johtaa käyttäjän sivustolle, jossa varsinainen haittaohjelma aktivoituu, ks. Ibid., s. 182.
[232] Potentiaalisen hyökkääjän kannalta USB-tikuilla on mahdollista saastuttaa todella hyvin suojattuja kohteita, sillä vaikka järjestelmä ei ole internetissä, muistitikulla haittaohjelma voi sekoittaa esimerkiksi ilmavoimien tukikohdan, ks. Järvinen, 2012, s. 188.
[233] Ks. Ibid., s. 52–55
[234] Erityisen tärkeää on huolehtia esimerkiksi palomuurin ja virustentorjunnan, sekä käyttöjärjestelmän päivityksistä, ks. Ibid., s. 189–194, 202–203 ja 241–244.
[235] Ks. Limnéll, ym., 2014, s. 50–52.

henkilökunnalle. Mainittakoon, että rekisterinpitäjän tulee – riippuen alasta – tutustua EU:n verkko- ja tietoturvadirektiiviin ((EU) 2016/1148) eli niin sanottuun kyberturvallisuusdirektiiviin[236], sähköisen viestinnän tietosuojadirektiiviin (2002/58/EY), kyberrikollisuusdirektiiviin ((EU) 2013/40) ja maksupalveludirektiiviin ((EU) 2015/2366). Lisäksi rekisterinpitäjän tulee tutustua sekä tietosuojaneuvoston ohjeisiin että tietosuojatyöryhmän antamiin ohjeistuksiin. Muita tietosuojaan vaikuttavia elimiä ovat Euroopan unionin verkko- ja tietoturvavirasto ENISA sekä kansalliset tietosuoja- ja kyberturvayksiköt. Lisäksi on olemassa erilaisia standardeja tietosuojaan liittyen, kuten ISO 27000. Kuten tästäkin voidaan huomata, kyse ei ole pelkästään tietosuoja-asetuksen tarkastelusta. Sisäänrakennettuun ja oletusarvoiseen tietosuojaan liittyy vahvasti muita sääntelyinstrumentteja ja toisaalta kansainvälisiä toimijoita ja ohjeita. Kaikki edellä mainitut eivät ole sitovia säännöksiä. Tärkeämpää on ymmärtää niiden ohjaava ja täydentävä vaikutus, kun suoritetaan teknisiä ja organisatorisia toimenpiteitä. Nämä tulee ottaa huomioon ohjeistuksia laadittaessa kuten muussakin tietosuojatyössä.

4.2.3. Auditoinnit ja työryhmät

Ongelmia tietosuojatyöskentelyssä nousee usein esiin, kun tarkastuksia tehdään sisäisesti, sillä niiden merkitys saatetaan aliarvioida. Hyvä asiantuntija voi luoda hyvät puitteet tarkastuksille, mutta yhtenä parempana tapana on käyttää ulkopuolista ja siten objektiivista näkökulmaa. Tilanteet, joissa sisäisesti kerrotaan ehdotuksista johdolle, voivat johtaa puutteellisiin toimiin organisaatiossa. Ulkopuolisen mielipide taas saatetaan ottaa herkemmin huomioon.[237]

Yhtenä keskeisenä välineenä sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamisessa näen kaikenlaisen tietosuojatyöskentelyn. Kyse voi olla niin ulkoisesta kuin sisäisistä asiantuntijapalveluista. Kuten edellä on huomattu, osa ratkaisuista, jotka palvelevat TSA:n velvoitteita, saattaa vaatia organisaatiolta toimenpiteitä, joiden täysimääräiseen toteutukseen riittäviä resursseja ei löydy valmiina omasta organisaatiosta. Tällöin on hyvä kysyä, onko liiketaloudellisesti järkevämpää hyödyntää satunnaisesti ulkoisia palveluita vai onko liiketoiminta niin laajaa, että erilaisia digiajan osaajia kannattaisi palkata organisaatioon. Ainakin tällä hetkellä trendinä on pidetty sitä, että asiantuntijoiden käytöllä saavutetaan liiketaloudellista etua, sillä siihen panostetaan aikaisempaa enemmän yrityksissä. Tässä suhteessa ei liene väärin todeta, että asiantuntevasta yhteistyökumppanista on paljon hyötyä oman liiketoiminnan toteuttamisessa ja

[236] Euroopan komissio ehdotti joulukuussa 2020 tarkistettua verkko- ja tietoturvadirektiiviä. Uusilla säännöillä tiukennetaan yritysten velvoitteita turvallisuuden suhteen, käsitellään toimitusketjujen turvallisuutta, otetaan käyttöön tiukemmat valvontatoimenpiteet kansallisille viranomaisille ja lisätään tietojenvaihtoa ja yhteistyötä entisestään. Ehdotusta käsitellään parhaillaan neuvostossa.
[237] Schneier, 2015, s. 170.

kehittämisessä.[238] Toisaalta ulkopuolisen avun hankkimisessa täytyy kiinnittää huomiota siihen, että organisaatiossa täytyy olla itselläänkin riittävä tietosuojaosaaminen avun kohdistamiseksi oikeaan paikkaan. Jos itse ei tiedetä mihin apua tarvitaan, ei asiantuntijan käyttö tuota etua. Tärkeämpää on tunnistaa omat rajat ja käyttää omien rajojen ulkopuolelle tarjolla olevaa osaamista. Rekisterinpitäjän ei tule ryhtyä sellaisiin toimenpiteisiin, joiden vaikutusta tämä ei ymmärrä.

Ehkä yhtenä tyypillisistä ongelmista asiantuntijoiden käytössä tietosuojaan liittyen on tietosuoja-asioiden pitäminen ylimääräisenä taakkana, joka ei kasvata tai tehosta liiketoimintaa vaan päinvastoin aiheuttaa kuluja. Yleisesti ottaen esimerkiksi kilpailuoikeudessa mielletään kaiken ratkaisijana kysymystä rahasta näin taloustieteellisenä määrittäjänä. Arvostus määrittyy rahallisena tuloksena, mutta arvon määrityksessä ei oteta huomioon muita tekijöitä. Kuten todettu, on tietojen kerääminen käynyt yhä suuremmaksi markkinoiden kasvattajaksi. Miksi tietosuojaa ei sitten arvosteta samalla tavalla? Arvokas ja laadukas voi olla yhtä kuin tietosuojamyönteinen.[239] Mielestäni tietosuojavaatimusten noudattamisen aliarviointi on harhaluulo, sillä yksilöt arvostavat sitä, että heidän yksityisyyttään kunnioitetaan. Otetaan esimerkiksi tilanne, jossa kuluttajalla on keittiöremontin kohdalla kaksi vaihtoehtoista toimijaa, X ja Y. Toimija X haluaa kerätä sinusta kaikenlaisia tietoja ja tallentaa tiedot omiin tietojärjestelmiinsä mutta toimijalle Y riittää vain takuukuitille tuleva nimi sekä toimitusosoite. Kumpaan suuntaan kuluttaja tässä kallistuisi ajatellen pelkästään yksityisyyden suojaa? Kilpailussa markkinoista voitaisiin ottaa siten käyttöön kuluttajan valintaan ja markkinoiden reiluuteen nojaava lähestymistapa, joka sisältää yksityisyyden ulottuvuuden kuluttajan hyvinvointia lisäävänä seikkana perinteisen talouspainotteisen lähestymistavan lisäksi.[240]

Siinä missä sisäänrakennetun ja oletusarvoisen tietosuojan käytännön toteuttamiseen liittyy myös teknisiä ratkaisuja, yhtenä varteenotettavana mittapuuna on käyttää asiantuntijoita, jotka ovat alalla kansainvälisesti tunnetun sertifioinnin saaneita. Tästä hyvänä esimerkkinä on *The International Association of Privacy Professionals (IAPP)*, joka myöntää tällä hetkellä globaalisti ainutta tunnustettua sertifiointia, joka liittyy yksityisyyden hallintaan. IAPP:n pitämiin koulutuksiin ja sertifiointiin ovat osallistuneet useat tietosuoja-alan ammattilaiset saadakseen

[238] Ks. Pyyhtiä, 2019 s. 40–41.
[239] Ks. mielenkiintoinen väitöskirja liittyen kilpailuoikeuteen, missä testataan nykyisiä tietosuojakehityksiä ja pyritään haastamaan ajattelua kohti yksityisyyden turvaamista yhtenä kilpailun etuina ja lisäämällä tiedon arvostusta, sekä osoittamaan yksityisyyden merkitys laadun merkkinä, Wasastjerna, 2019, s. 154–159 ja 167–172.
[240] Ibid., s. 204–205.

täydennystä osaamiseensa liittyen yksityisyyden suojaamiseen[241]. Edellä esitettyjen sertifiointien haltijoiden voidaan ymmärrettävästi lukeutua alansa osaajiin, kun kyse on teknologian käyttämisestä organisaatioissa yksityisyyden ja henkilötietojen suojan nimissä. Osaamisen laajuus on luonnollisesti rinnasteinen haltijan sertifikaattiin.

4.2.4. Tietosuoja- ja tietoturvasuunnittelu

Tietoturvallisuus käsitteenä ja ilmiönä on vaikeasti ymmärrettävissä, ja sen merkitys oikeusperiaatteena odottaa osin selkeytymistä.[242] Oikeudellisessa mielessä tietoturvallisuudella viitataan tietojen luottamuksellisuuteen, eheyteen ja käytettävyyteen sekä niiden ylläpitämiseen ja suojaamiseen oikeudellisena velvollisuutena, vaatimuksena ja kriteerinä.[243]

Psykologi *Don Norman* on esittänyt, että hyvin suunnitellut esineet on helppo tulkita ja ymmärtää. Hyvin suunnitellut esineet sisältävät näkyviä vihjeitä niiden toiminnasta. Huonosti suunniteltuja esineitä voi olla vaikea ja turhauttavaa käyttää. Hän teorioi, että suunnittelun perusperiaatteena on 1) tarjota hyvä käsitteellinen malli, jonka avulla käyttäjät voivat henkisesti simuloida kohteen toimintaa, ja siten 2) tehdä asioista näkyviä. Näiden periaatteiden avaimet ovat erityisesti niiden käyttömahdollisuuksissa, rajoitteissa ja kartoituksissa. Käyttömahdollisuudet ovat asian havaittavissa oleva ja todellinen ominaisuus. Ensisijaisesti käyttömahdollisuudet ovat perusominaisuuksia, jotka määräävät, miten asiaa voidaan käyttää. Kartoitukset tarkoittavat kahden asian suhdetta, kuten hallintalaitteet ja niiden liikkeet sekä tulokset maailmassa. Rajoitteet ovat puolestaan esineiden fyysisiä ominaisuuksia, jotka rajoittavat mahdollisia toimintoja, kuten järjestystä, jossa osat voivat kulkea yhdessä ja tapoja, joilla esinettä voidaan siirtää, noutaa tai muuten käsitellä.[244] Norman esittää seitsemän periaatetta suunnittelun käyttämisestä tehtävien yksinkertaistamiseksi ja vaistonvaraisemmaksi:

1) Käytä sekä maailman että pääsi tietoa.
2) Yksinkertaista tehtävien rakennetta.
3) Tee asioista näkyviä (tee kohteen käyttö ilmeiseksi visuaalisilla elementeillä ja tee tärkeät suunnitteluelementit ilmeisiksi).
4) Tee kartoitukset oikein.
5) Hyödynnä sekä luonnollisten että keinotekoisten rajoitusten mahdollisuuksia.

[241] Mainittakoon, että IAPP myöntää mm. seuraavia sertifiointeja: the Certified Information Privacy Professional (CIPP), the Certified Information Manager (CIPM) ja the Certified Information Privacy Technologist (CIPT), ks. Ustaran, 2018, johdanto kohta ix.
[242] Ks. Råman, 2006a, s. 6 ja Råman, 2006b, s. 818–824 sekä Voutilainen, 2012, s. 196–202.
[243] Ks. Pöysti, 2002, s. 64.
[244] Norman, 1988, s. 2–13.

6) Suunnittele inhimillisiä virheitä varten.
7) Jos jokin epäonnistuu, standardisoi järjestelmät käyttämällä yleisesti tunnistettavia menetelmiä.[245]

Kyse ei siten tarvitse olla hirveän monimutkaisesta tavasta ajatella tai toteuttaa sisäänrakennettua ja oletusarvoista tietosuojaa. Kyse voi olla täysin silmien avaamisesta esimerkiksi työpaikalla. Avokonttorit ovat osaltaan johtaneet siihen, että työpaikoilla itse asiassa yksityisyys ja tietoturvallisuus on heikentynyt. Kun työntekijä jättää työpöytänsä esimerkiksi kahvitauon ajaksi, jäävät näkyville kaikki paperit ja pahimmassa tilanteessa jopa henkilötiedot tietokoneen näytölle. Yksityisyyden ja henkilötietosuojan tarve sisäänrakennetun ja oletusarvoisen tietosuojan toteuttamiseksi tulee yhtä lailla ottaa huomioon myös työpisteillä ja niiden käytössä. Esimerkiksi toimiston tilojen käytössä voidaan hyödyntää alan osaamista työpisteiden sijoittamisella oikein ja käyttäen erinäisiä ratkaisuja tietosuojan ja yksityisyyden parantamisessa.[246] Tätä varten käyttäytymistieteissä on kehitetty tilojen suunnittelijoille jopa tieteellinen malli *The Designing for Privacy model*, jonka puitteissa yksityisyyden suoja (ja samalla tietosuoja) tulee huomioiduksi.[247] Samalla kun työpisteitä muokataan, tulee myös huolehtia esimerkiksi tilojen äänieristyksestä, mikä lisää tilaturvallisuutta. Vaikka ulkopuoliset eivät kuulisikaan toimistokeskusteluita, on äänieristyksestä silti huolehdittava asianmukaisesti. Esimerkiksi esimiehen ja alaisen välillä käytävät kehityskeskustelut ovat luottamuksellisia, eikä niitä siten ole tarkoitettu muiden, edes työyhteisön, tietoon.[248] Edellä mainituissa toimissa hyvänä vaihtoehtona on käyttää ulkopuolisia asiantuntijoita mutta myös kuunnella työntekijöitä. Sisäiset työryhmät, jotka tietävät käytännön tasolla tietojenkäsittelystä organisaatiossa, voivat antaa paljon uusia näkemyksiä tietosuojatyöhön.

Jos edellä käsiteltyä tilojen suunnittelua pohditaan tarkemmin, voidaan se erottaa omaksi osa-alueeksi liittyen tietoturvan toteuttamiseen. Samalla kun tietoturvaa toteutetaan, myös tietosuojan tasoa voidaan kasvattaa. Tietoturva voidaan jakaa eri osa-alueisiin monella tapaa. Perinteinen tapa on jakaa tietoturvallisuus kahdeksaan osaan: 1) hallinnolliseen, 2) fyysiseen, 3) henkilöstö-, 4) tietoliikenne-, 5) laitteisto-, 6) ohjelmisto-, 7) tietoaineisto- ja 8) käyttöturvallisuuteen.[249] Sisäänrakennetun ja oletusarvoisen tietosuojan kohdalla kyse on organisaation sisäänrakennetusta mallista, jossa tietojen suojaaminen otetaan huomioon kaikessa toiminnassa oletusarvoisesti. Esimerkiksi kun suojataan tietoturvaa fyysisessä ympäristössä, voidaan käyttää

[245] Norman, 1988, s. 188–189, tietoa sisältävät järjestelmät on hyvä suunnitella niin, että niiden kaatuessa ne kaatuvat ennakoidulla tavalla, näin myös Schneier, 2015, s. 191–192.
[246] Ks. Stewart-Pollack – Menconi, 2005, s. 97–117.
[247] Ks. Ibid., s. 225–228.
[248] Andreasson – Koivisto, 2013, s. 64.
[249] Ibid., s. 52.

kulunvalvontaa. Samoin, kun otetaan huomioon esimerkiksi tietoaineistoturvallisuus, esimerkiksi käyttöoikeuksilla[250] voidaan rajata tietojen käsittelyä siten, että vain ne, joilla on varsinainen tarve käsitellä tietoja, pystyvät siihen. Valtiohallinnon tietoturvasanaston (VAHTI 8/2008) mukaan fyysisellä turvallisuudella tarkoitetaan henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamista tuhoja ja vahinkoja vastaan. Samalla kun organisaatiossa suojataan tietoturvanäkökulmista pääsyä tiloihin, toteutetaan toimenpiteitä, joilla vähennetään riskiä tietojen luvattomasta paljastumisesta sivullisille. Tällöin myös rekisterinpitäjänä toimivan organisaation asiakkaiden tietosuoja toteutuu. Tietosuojan toteutuminen täysimääräisesti edellyttää kuitenkin myös muita toimenpiteitä.

Verkkosivustojen teknisellä suunnittelulla on myös valtava vaikutus ihmisten yksityisyyteen. *Lawrence Lessig* ja *Joel Reidenberg* korostavat internetin *arkkitehtuurin* merkitystä.[251] Arkkitehtuuri voi muokata ihmisten käyttäytymistä.[252] Fyysinen arkkitehtuuri, kuten rakennukset, voi vaikuttaa siihen, miten elämme ja olemme vuorovaikutuksessa vertaistemme kanssa. Tilat voidaan suunnitella kannustamaan ihmisiä olemaan avoimempia sekä kommunikoimaan keskenään useammin. Toisaalta tilat voidaan suunnitella kannustamaan yksinäisyyteen. Fyysisten tilojen ohella myös internetin virtuaalitilat, kuten sosiaalisen median verkkoalustat, ovat suunniteltuja ympäristöjä. Sosiaalisen verkoston verkkosivustojen suunnitteluvalinnoilla on syvällisiä vaikutuksia siihen, miten niiden käyttäjät ovat vuorovaikutuksessa keskenään.[253]

Kuten tästä voidaan huomata, kulkevat tietosuoja ja tietoturvatoimenpiteet käsi kädessä keskenään. Samoin rekisterinpitäjän velvollisuus toteuttaa organisatorisia ja teknisiä toimenpiteitä asianmukaisen turvallisuuden saavuttamiseksi sisältää velvoitteen huolehtia tietoturvan tasosta. Koska tilanne on hyvin monisyinen, ei näitä velvoitteita tule missään nimessä ajatella irrallisina toisistaan. Kaiken keskiössä on selkeästi otettava huomioon yhtäältä yrityksen omat intressit suojata omia järjestelmiään ja samalla toteuttaa toimenpiteitä rekisteröityjen suojaamiseksi.

4.3. Tekniset toimenpiteet

4.3.1. Yksityisyyden suojaa edistävät teknologiat

Teknologiasta riippuvassa verkkoyhteiskunnassa keskeisenä tekijänä on ollut jo pitkään vastata teknologian aiheuttamiin ongelmiin lisäämällä teknologisia ratkaisuja. Tällaisia menetelmiä

[250] On myös syytä huomioida, että käyttövaltuuksien hallintaan liittyvinä periaatteina ja lähtökohtina voivat olla asiaa koskevaa lainsäädäntö tai organisaatioiden ohjeistukset ja määräykset, sekä tietojen käsittelyyn liittyvät sopimukset, ks. Andreasson – Koivisto, 2013, s. 106–116.
[251] Ks. Lessig, 1999, s. 5–6 ja s. 236, näin myös Reidenberg, 1993, s. 296.
[252] Lessig, 1999, s. 236.
[253] Solove, 2007, s. 200.

tietosuojan osalta on nimitetty yksityisyyden suojaa parantaviksi teknologioiksi, joista englanniksi puhuttaessa käytetään termiä *Privacy-Enhancing Technologies* tai lyhennettä *PET*. Käsitteen on yleensä ajateltu sisältävän tekniset mekanismit, joita kehitetään tarkoituksellisesti yksityisyyden vahvistamiseksi. Myös yleinen mielipide erityisesti erinäisten paljastusten, kuten *Edward Snowdenin* tapauksen, seurauksena on kääntynyt sille kannalle, että henkilötietojen suojaa tulee parantaa, sillä on vihdoin ymmärretty henkilötietojen suojaamisen tärkeys ja arvo. Myös unionin tasolla on jo varhain tuettu yksityisyyden suojaa parantavien teknologioiden käyttöä.[254] PET-järjestelmien merkitys on erityisen suuri estettäessä massavalvontaa. Niiden avulla voidaan estää sivustoja valvomasta ja seuraamasta käyttäjää, mitä voidaan pitää keskeisenä toimenpiteenä yksityisyyden ja henkilötietojen suojan näkökulmasta. Tärkein näistä teknologioista on kuitenkin salausteknologian käyttäminen. Senkin osalta on hyvä huomata, että vaikka salaus tapahtuu sähköpostisovelluksessa tai sosiaalisessa mediassa, kuten WhatsAppissa, saattaa siitä jäädä kopio kyseiselle alustalle salausavainten kanssa, mikä mahdollistaa pääsyn viesteihin.[255] PET:n mahdollisuuksia ovat muun muassa henkilötietojen jäljittämisen, linkittämisen ja konsolidoinnin estäminen yli organisaatio- tai kontekstuaalisten rajojen. Lisäksi niillä voidaan varmistaa, että tietojärjestelmät toimivat rekisteröidyille ja järjestelmien käyttäjille läpinäkyvillä ja ymmärrettävillä tavoilla ja että niiden käyttäjät ja rekisteröidyt voivat asianmukaisesti valvoa ja ohjata tällaisia järjestelmiä.[256] PET:iden käytössä on hyvä muistaa se, että TSA:n vaatimukset tulee suhteuttaa käytettävissä olevan tekniikan tasoon, toteuttamiskustannuksiin ja käsiteltävänä olevien tietojen laatuun. Lisäksi käsittelyssä tulee ottaa huomioon käsittelyn luonne, asiayhteys, laajuus sekä tarkoitus. Samalla asetus velvoittaa ottamaan huomioon käsittelystä mahdollisesti aiheutuvat riskit mukaan lukien niiden vakavuuden ja todennäköisyyden. Riskejä voidaan selvittää TSA 35 artiklan mukaisella vaikutuksenarvioinnilla (DPIA).[257]

McDonald esittää käyttäjien PET:n omaksumiseen monia esteitä:

1) PET:n käyttöön ei ole ilmeisiä kannustimia, mikä johtuu esimerkiksi virheellisestä uskomuksesta, että vahvat lait suojaavat yksityisyyttä verkossa tai että yritykset eivät koskaan keräisi sellaista tietoa, joka muodostaa niiden liiketoimintamallien selkärangan tai ei tajuta, että näkymätön tiedonkeruu jatkuu.
2) Tiedon puute yksityisyyden suojaa parantavien työkalujen olemassaolosta.

[254] Ks. Komission tiedonanto Euroopan parlamentille ja Neuvostolle tietosuojan vahvistamisesta yksityisyyden suojaa parantavilla tekniikoilla, s. 4–5.
[255] Schneier, 2015, s. 252.
[256] Ks. esimerkiksi Rost – Pfitzmann, 2009, s. 353.
[257] WP 248, s. 4.

3) Teknisesti vaikeat asennusmenetelmät.
4) Teknologioiden käyttöönotosta on syntynyt kauheita käyttökokemuksia, joita jaetaan eteenpäin ilman varsinaisia perusteita.[258]

4.3.2. Hide and Seek Technologies

Edellä käsitellyt PET-järjestelmät ovat yksi keino ”piilottaa” yksilöistä tietoja. Itse piilottamisen menetelmät voidaan jakaa kahteen lähestymistapaan: anonymisoiviin ja monimutkaistaviin.[259] Tavalliset PET:t kuuluvat näistä usein ensimmäiseen kategoriaan. *Hartzog* kutsuu keksintöjä, jotka on suunniteltu löytämään, tunnistamaan, valvomaan tai piilottamaan yksilöiden toimimista, piilota ja etsi -teknologioiksi (*hide and seek technologies*). Tähän luokkaan kuuluvat muun muassa kamerat, internetselaimet, kasvojentunnistustekniikat, rekisterikilpien lukijat, droonit, seurantamajakat ja vakoiluohjelmat. Erityisesti tällaiset tekniikat pyrkivät monimutkaisuudellaan suojelemaan yksityisyyttä. Toisaalta tällaisia teknologisia välineitä voidaan käyttää yksityisyyttä rapauttavasti mutta myös yksityisyyttä parantavina teknologisina välineinä. Piilota ja etsi -teknologiat pystyvät aiheuttamaan dramaattisia yksityisyyden haittoja, kuten paljastamaan syvästi arkaluontoisia, salaisia tietoja, kuten alastonkuvia, seksuaalisia mieltymyksiä, terveystietoja ja poliittista toimintaa.[260] Piilota ja etsi -teknologiat ovat myös petollisen huomaamattomia. Ne pystyvät heikentämään epäselvyyden vaatimusta niin hitaasti ja tasaisesti ajan myötä, että emme huomaa prosessia.[261] *Hartzog* määrittelee *epäselvyyden* tiedon tilaksi tai ihmisten vaikeudeksi tai epätodennäköisyydeksi olla löydettävissä tai ymmärrettävissä. Epäselvyys toimii teoreettisena yhteisenä perustana ja sääntelyn keskipisteenä piilota ja etsi -teknologioiden suunnittelun aiheuttamille ongelmille. On olemassa laaja valikoima teknologioita, joita voidaan hyödyntää piilottamaan asioita näkyvistä ja käytännössä pitämään asioita epäselvyyden varjolla tavoittamattomissa.[262] *Hartzog* argumentoi, että kaikki PET:t eivät ole piiloteknologioita, jotka suoraan edistävät epäselvyyttä ja vastustavat valvontaa. Päinvastoin hän näkee, että jotkin yksityisyysystävälliset PET:t, kuten läpinäkyvyys tai ilmoitukset, kuuluvat muihin tietojen reilun käsittelyn käytänteisiin eli FIPiin (Fair Information Practices).[263] Epäselvyys voi näkyä esimerkiksi siinä, että käytetään paikkatiedon verhoamista eri häivytysmenetelmillä.[264]

[258] McDonald, 2015, s. 127.
[259] Heino, 2016, s. 37.
[260] Hartzog, 2018, s. 230–231.
[261] Ks. Cohen, 2008, s. 190.
[262] Hartzog, 2018, s. 234–237.
[263] Ibid., s. 237.
[264] Heino, 2016, s. 37.

Ira Rubinstein on esittänyt, että on olemassa kahdenlaisia PET-järjestelmiä: korvaavia ja toisiaan täydentäviä. Korvaavat PET:t ovat suunniteltu siten, että henkilötietoja ei voi kerätä. Onnistuessaan ne voivat lieventää joidenkin yksityisyyden suojan tarvetta tai jopa poistaa sen. Toisiaan täydentävillä PET:illä on kuitenkin hieman erilainen tavoite olla joko yksityisyysystävällisiä PET-järjestelmiä tai yksityisyyttä muuten suojaavia. Rubinstein määrittelee yksityisyysystävälliset PET-järjestelmät käytännöiksi, jotka helpottavat *henkilökohtaisten tietojen yksilöllistä hallintaa, lähinnä tehostettujen ilmoitusten, valinnanvapauden ja pääsyn kautta*. Hän määrittelee muut yksityisyyttä suojaavat PET:t *yksityisyyden suojaksi, joka tarjoaa todennettavissa olevia yksityisyyden takeita pääasiassa salausprotokollien tai muiden kehittyneiden toimenpiteiden avulla*.[265]

Esimerkiksi epävarmuutta mahdollistavana piiloteknologian käyttötarkoituksena ovat erilaiset salausmenetelmät. Salaamisella on mahdollista säilyttää ne tiedot, joita ei ole tarkoitettu kolmansien tietoon. Kyky varmistaa salaisuuksien säilyminen on tärkeä väline yksityisyyden takaamiseksi yhä tehokkaampien valvontateknologioiden ja -tekniikoiden edessä.[266] Muita tekniikoita, jotka on suunniteltu piilottamaan tietoja, ovat *Hartzogin* mukaan esimerkiksi älykkäät hyperlinkit, joissa tekniikka sallii pyynnöt käyttää henkilökohtaisia tietoja sisältäviä linkkejä vain, jos ne ovat peräisin tietyistä luotettavista lähteistä. Älykkäät hyperlinkit voivat auttaa varmistamaan, että vain suojatun yhteisön jäsenet tai muut vahvistetut käyttäjät voivat käyttää tietoja. Esimerkkeinä voidaan käyttää myös teknologiaa, jonka avulla voidaan luoda ns. "maksumuuri". Lisäksi yleisimmät työkalut, joiden avulla käyttäjät voivat lisätä *Hartzogin* epäselvyyden vaatimusta, ovat yksityisyysasetukset. Näiden asetusten avulla käyttäjät voivat piiloutua hakukoneilta ja hallita henkilökohtaisia tietojaan. Lisäksi hakuestoteknologiat, jotka kieltävät verkkosivustoja indeksoimasta hakukoneita käyttämästä käyttäjän tietoja, ovat siksi erittäin tehokkaita tapoja lisätä yksilöiden toiminnan epäselvyyttä ja monimutkaistaa yksilöistä saatavaa tietoa. Tunnistamisen mahdollisuuden poistaminen kokonaan luo myös epäselvyyttä. Esimerkiksi kasvojen sumentamistyökaluja tulisi käyttää yhä enemmän, milloin yksilö ei ole tunnistettavissa.[267]

VPN-työkalut ovat yksityisyyttä parantava trendi, ja niillä voidaan muodostaa näennäinen virtuaalinen erillisverkko varsinaisen käytetyn verkkoyhteyden ylitse. VPN:ää käytetään yhä enemmän käyttäjien yksityisyyden suojaamiseen ja ylläpitämiseen verkossa. Todennuksen, tunneloinnin ja salausvaiheiden avulla käyttäjät voivat käyttää suojattuja yhteyksiä. VPN-

[265] Rubinstein, 2011, s. 1413.
[266] Hartzog, 2018, s. 241.
[267] Ibid., s. 237–240.

tekniikka kehittyy edelleen samalla kun salaus kehittyy entistä kehittyneemmäksi. Internetin ja sen vuoksi, miten ihmiset jakavat yhä enemmän tietoja, virtuaalisen yksityisen verkon kaltaisen turvallisuusvälineen ymmärtäminen on olennaisen tärkeää tasapainoisten oikeudellisten sääntelykehysten luomiseksi.[268]

London School of Economics on tutkinut PET-järjestelmien hyötyjä taloudelliselta kannalta. Tutkimusten tuloksena voidaan nähdä selviä viitteitä siitä, että yleisesti ottaen järjestelmät voidaan nähdä hyödyllisinä niin käyttäjien kuin viranomaisten taholta. Ongelmallisiksi ovat vain koituneet niistä aiheutuvat kustannukset ja todellisten käyttäjien tai järjestelmistä hyötyjien vähäisyys. Toisaalta tutkimuksessa nähtiin, että yritykset, jotka järjestelmiin panostavat, voivat saada siitä kilpailuetua erityisesti yritysmarkkinoilla mutta miksei myös kuluttajamarkkinoilla.[269]

4.3.3. Pseudonymisointi ja anonymisointi

Henkilötietoja ovat TSA:n mukaan *kaikki tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevat tiedot*.[270] Tunnistettavissa oleva henkilö on henkilö, joka voidaan tunnistaa kyseisistä tiedoista suoraan tai epäsuorasti. Tietosuojasääntöjen soveltamisen kannalta määritelmä on ratkaiseva. Tutkimukset ovat kuitenkin osoittaneet, että määritelmän tulkinta sekä laissa että käytännössä vaihtelee EU:n alueella suuresti.[271]

Henkilötietojen määrittelyn problematiikassa kyse ei ole *biologisten* tietojen erottamisesta muunlaisista tiedoista, kuten tietoteknisesti luoduista tiedoista. Kyse on pikemminkin tilanteesta, jossa henkilötietojen käsittelyssä tulee erottaa toisistaan sellainen tieto, jolla on potentiaalista vaikutusta käyttäjien henkilökohtaiseen yksityisyyteen, taloudellisiin seikkoihin tai emotionaaliseen hyvinvointiin sekä tieto, jolla ei ole tällaista vaikutusta. Yhä useammin tätä eroa ei ole nähtävissä yhtä helposti kuin tavanomaisessa tai biologisessa tiedossa, joka liittyy nimeen tai tunnisteeseen. Riippuen kontekstista, mutta erityisesti isoille korporaatioille kaikista arvokkainta tietoa markkinoilla ovat sähköisesti kerätyt yksilöintitiedot, kuten evästeet ja IP-osoitteet sekä puhelimiin linkittyvät MAC-osoitteet. Näitä tietoja keräämällä käyttäjä voidaankin yhdistää henkilöön ja tarjota tälle profiloinnin avulla tuotteita ja palveluita. Evästeitä ja IP-osoitteita keräämällä ne voidaan yhdistää henkilöön epäsuorasti, sillä niiden avulla voidaan osoittaa käyttäjä. Yhdistäminen on mahdollista siten, että esimerkiksi käyttäjälle, joka selailee

[268] Ks. VPN-teknologiasta esimerkiksi Park, 2017, s. 135.
[269] London School of Economics: Study on the economic benefits of privacy-enhancing technologies (PETs), 2010, s. 153–155.
[270] TSA 4 artiklan 1 kohta.
[271] Ks. C-582/14, Breyer v. Saksa 19.10.2016, kohdat 32–49.

internetissä käytettyjä tavaroita ei markkinoida luksusmerkkejä. Seurauksena tästä yksilöä voidaan jopa syrjiä varallisuuden mukaan. Toisaalta kyse ei välttämättä ole syrjinnästä, jos yksilö ei edes halua luksusmerkkien mainontaa. Problematiikkaan siitä, milloin henkilötieto on yhdistettävissä henkilöön, tietosuojatyöryhmä antoi ratkaisun, joka sittemmin vaikuttaa osana TSA:ta. Jos tietoja voidaan käyttää henkilön tunnistamiseen suoraan tai epäsuorasti *keinoin, joita rekisterinpitäjä tai jokin muu luonnollinen henkilö tai oikeushenkilö voi kohtuudella käyttää*, niitä on pidettävä henkilökohtaisina henkilötietoina.[272]

Anonymisoidulla tiedolla tarkoitetaan dataa, josta on poistettu kaikki ihmiseen liittyvät tiedot. Tämän seurauksena tieto ei ole suorasti tai epäsuorasti yhdistettävissä luonnolliseen henkilöön, milloin anonymisoitu tieto ei ole TSA:n mukainen henkilötieto.[273] Anonymisointi tarkoittaa käytännössä sitä, että datasta poistetaan kaikki yksilöön viittaavat tiedot, eikä niitä voida enää yhdistää tähän yksilöön. Täydellinen anonymisointi johtaa siihen, että organisaatio menettää myös tietoaineksen.

Pseudonymisoitu tieto on sellaista henkilötietoa, jota ei voida enää yhdistää tiettyyn rekisteröityyn ilman lisätietojen käyttöä edellyttäen, että tällaiset lisätiedot pidetään erillään ja että niihin sovelletaan kaikkia mahdollisia teknisiä ja organisatorisia toimenpiteitä sen varmistamiseksi, etteivät henkilötiedot liity tunnistettavissa olevaan eikä tunnistettuun luonnolliseen henkilöön.[274] Käytännössä tämä tarkoittaa sitä, että liityntä ihmiseen katkaistaan ja piilotetaan mutta tietoa ei poisteta kokonaan. Tällöin ilman lisätietojen käyttämistä henkilötietoa ei voida yhdistää luonnolliseen henkilöön.[275] Lisätietona voidaan pitää tässä yhteydessä esimerkiksi koodiavainta. Koska henkilötieto voidaan muuttaa takaisin luonnolliseen henkilöön liittyväksi, kyseessä on edelleen henkilötieto, mutta sen voidaan nähdä muodostavan pienemmän riskin rekisteröidylle, ja näin ollen pseudonymisoidulle henkilötiedolle voidaan antaa erilainen asema. Pseudonymisoidun tiedon säilyttäminen on tavallisessa muodossa olevan henkilötiedon säilyttämistä parempi ratkaisu. Samoin pseudonymisointi voi olla merkki rekisterinpitäjän osoituksesta tietosuojavelvoitteiden noudattamisesta. Erityisesti kyseeseen voivat tulla yleisten tietosuojaperiaatteiden turvallisuusvelvoitteiden hoitaminen sekä sisäänrakennetun ja oletusarvoisen tietosuojan vaatimus.[276]

Toisaalta pseudonymisointi ei tehokkaasti suojaa yksilön henkilötietojen suojaa kaikissa tilanteissa. Esimerkiksi DNA:ta keräävät yritykset viittaavat tietosuojakäytännöissään tietojen

[272] TSA johdanto-osan 29 perustelukappale ja ks. WP 136, s.15–17.
[273] Korpisaari, ym., 2018, s. 612.
[274] TSA:n johdanto-osan 60 perustelukappale.
[275] Korpisaari, ym., 2018, s. 612.
[276] Edwards, 2019, s. 88.

pseudonymisointiin vakuuttaakseen asiakkaansa. Myöskään geneettinen tieto ei ole helposti muutettavissa tunnistamattomaksi, sillä geneettinen tieto on juuri sellaista, jolla yksilö voidaan tehokkaasti tunnistaa ja erottaa muista. Jos asiakkaiden nimet muutetaan geneerisesti tuotetuiksi tunnisteiksi, on heidät silti mahdollista tunnistaa.[277] Tutkimuksessa vuodelta 2000 tutkijat onnistuivat uudelleen tunnistamaan vähintään 98 % yksilöistä, jotka olivat ”anonymisoituja”.[278]

Anonymisoinnin ja pseudonymisoinnin eroa ei ollut selvästi määritelty vielä henkilötietodirektiivin 29 artiklan mukaisen työryhmän lausunnossa 05/2014. Sen sijaan, että piilotettaisiin linkki tietojen ja rekisteröidyn välillä, pseudonymisointi käsittää yhden tietueessa olevan ominaisuuden korvaamisen toisella. Henkilö on tällöin tunnistettavissa edelleen epäsuorasti ja TSA:n johdanto-osan 26 perustelukappaleen mukaisesti tällaiset tiedot on luettava henkilötiedoiksi. On syytä huomata, että pseudonymisoitujen henkilötietojen osalta tiedot on mahdollista palauttaa henkilötiedoiksi käyttäen lisätietoja, kuten koodiavainta. Vasta lisätiedon jälkeen ne voidaan yhdistää jälleen luonnolliseen henkilöön.[279]

4.3.4. Kryptaus

Nykyään tuntuu olevan mahdotonta säilyttää anonymiteetti verkossa liikuttaessa. Tässä yhteydessä on toki syytä erottaa anonymiteetti tilanteissa, joissa halutaan tulla tunnistetuksi. On eri asia ladata materiaalia uteliaisuuttaan, kuin tunnistautua pankkiin omien tilitietojen näkemiseksi.[280] Tiedon luottamuksellisuus ei koske vain kansalaisia, jotka haluavat suojella yksityisyyttään. Se koskee myös yrityksiä, joiden on pidettävä strategiansa luottamuksellisina, aktivisteja, joiden on raportoitava turvallisesti ahdistavista epäkohdista, toimittajia, joiden on suojeltava lähteitään sekä puolustusvoimia ja lainvalvontaviranomaisia, jotka suojaavat arkaluontoista informaatiota. Kaikki nämä toimijat käyttävät erilaisia menetelmiä piilottaakseen itsensä tai tietonsa. Toisaalta myös rikoksentekijät käyttävät näitä tekniikoita välttääkseen paljastumisen, tutkinnan tai syytteeseen joutumisen. Ns. Darknetin käyttö on suosittua, ja rikolliset kehittävät omia salausohjelmiaan pysyäkseen tutkan ulkopuolella. Kaikki nämä kehitelmät ja haasteet luovat ristiriidan lainvalvontaviranomaiselle. Toisaalta on suojeltava kansalaisten yksityisyyttä, tarjottava teollisuudelle turvallinen verkkoympäristö ja luotava turvallinen kybermaailma kaikille nautittavaksi. Toisaalta lainvalvontaviranomaisten on pystyttävä tutkimaan rikollista toimintaa verkossa, mukaan lukien salaus- ja anonymisointipalvelujen rikollinen väärinkäyttö. Ilmaisua *kaksoiskäyttö* (*Dual-Use*) käytetään usein kansainvälisessä humanitaarisessa

[277] Véliz, 2020, s. 13.
[278] Ks. Malin – Sweeney, 2000, s. 4.
[279] Ks. Korpisaari, ym., 2018, s. 64.
[280] Ks. Schneier, 2015, s. 154–157.

oikeudessa kuvaamaan tuotteita ja teknologioita, joilla voi olla sekä yksityis- että sotilastarkoituksia. Tässä tapauksessa teknologiaa voidaan käyttää sekä yksityisiin että rikollisiin tarkoituksiin. Vaikka internetistä on suurta hyötyä lainkuuliaisille kansalaisille ja yrityksille, se hyödyttää myös rikollisia, jotka aikovat tehdä rikoksia ja terrorismiin liittyvissä tapauksissa edistää väkivaltaisia ääriliikkeitä.[281]

On olemassa monia tekniikoita, joilla varmistetaan käytännön suoja tunkeutumiselta (salaus) ja tarjotaan keino piilottaa osapuolten identiteetti (anonyymisyys, pseudonymisointi, satunnaistaminen ja yleistäminen). Teknisestä näkökulmasta anonymisoinnin ja salauksen tavoitteet ovat radikaalisti erilaiset. Salaus pyrkii tarjoamaan tunnistettujen osapuolten välisen viestintäkanavan luottamuksellisuuden salakuuntelun tai tahattoman paljastamisen välttämiseksi, mutta anonymisoinnin tarkoituksena on välttää yksilöiden tunnistaminen estämällä ominaisuuksien linkittäminen rekisteröityihin.[282] Salaus viittaa prosessiin, jolla *viestit, tiedot tai informaatio muunnetaan toiseen muotoon, jota kukaan muu paitsi tarkoitettu vastaanottaja ei pysty lukemaan.*[283] Salaus ei pyri tekemään siten käyttäjistä anonyymejä, koska haltijan käsissä raaka sisältö on edelleen saatavilla tai pääteltävissä. Salaus suojaa ainoastaan minkä tahansa sisällön luottamuksellisuutta ja eheyttä, mikä estää kolmannen osapuolen pääsyn tai manipuloinnin.

Sähköisen ratkaisun luomisen ongelmaan on tunnettuja teknisiä ratkaisuja, jotka voivat antaa vahvan näytön siitä, että asiakirja on peräisin tietyltä yksilöltä. Kryptografiassa nämä tunnetaan nimellä *digitaaliset allekirjoitukset*. Nämä ratkaisut perustuvat "yksisuuntaisiin" matemaattisiin toimintoihin.[284] Matemaattisissa funktioissa on esimerkiksi se hyvä puoli, että ne hidastavat hyökkääjän pääsyä käsiksi tietoihin. Esimerkiksi 64 merkkiä pitkän salausavaimen purkaminen saattaa viedä hyökkääjältä päivän, mutta 65-merkkinen salausavain vie kaksinkertaisen ajan. Tästä syystä tietoja kannattaa suojata salausavaimilla, sillä se pakottaa hyökkääjän tekemään murtautumisen eteen enemmän töitä – toisin kuin silloin, kun ne jätetään avoimeksi.[285] Tässä mielessä salausavainten käytöllä ei välttämättä saavuteta täyttä turvallisuuta siitä, etteikö tietoihin päästäisi käsiksi. Toisaalta täydellistä turvallisuutta ei kaiketi saavuteta millään teknologialla. Turvallisuuden taso tulee suhteuttaa oikein ja TSA:ssa edellytetään riittävää turvallisuustasoa. On kuitenkin muistettava, että tietoverkkorikollisuus kulkee rahan perässä, jolloin potentiaaliset uhrit pyritään etsimään helpoimmasta päästä. Salauksen osalta yhtenä hyvänä esimerkkinä voidaan käyttää sähköpostin välityksellä tapahtuvaa viestien vaihtoa. Tavallisella

[281] Cocq, 2016, s. 179–181.
[282] Ibid., s. 181–182.
[283] Melis, 2001, s. 2.
[284] Edwards, 2019, s. 349.
[285] Schneier, 2015, s. 168–169.

sähköpostilla toteutettu viestintä on teknisesti erittäin yksinkertaista, mikä mahdollistaa lähettäjätietojen helpon väärentämisen. Lähettäjänimeen ei siten voi luottaa, vaan lähettäjän henkilöllisyys on varmistettava jollain toisella tavalla.[286] Yhtenä keinona tähän on ns. kaksivaiheinen todennus[287] tai muu varmenteen käyttö.

Teknologiset ratkaisut ovat kaikkein keskeisimmässä roolissa riittävän turvallisuustason saavuttamiseksi. Kyse ei ole pelkästään salauksesta vaan *de facto* kaikkien teknologisten järjestelmien saattamisesta käyttöön, milloin niille on perusteltua tarvetta. Tietojenkäsittely järjestetään suurimmilta osin erilaisissa sähköisissä tietojärjestelmissä. Näitä tietojärjestelmiä ei pystytä suojaamaan esimerkiksi fyysisillä lukoilla, vaan niihin pääsy järjestetään teknologian avulla. Tästä syystä teknologia vaikuttaa siihen, miten tietojärjestelmiä suojataan. Jos teknologiaa ei käytetä, jäävät tiedot suojaamatta. Toisaalta teknologian kääntöpuolena on erilaisten sovellusten käytettävyys. Sovelluksia tulee tosiasiallisesti osata käyttää, jotta ne saavuttavat niillä tavoitellut päämäärät. Teknologiaa tuleekin käyttää ja kehittää siten, että esimerkiksi salausjärjestelmät riittävällä tavalla pitävät tiedot turvassa. Vaikka tältä osin kyseessä näyttäisi olevan teknologiatulva, ei asia ole näin yksinkertainen. Lisäksi yhtenä osana sisäänrakennettua ja oletusarvoista tietosuojaa on se, että toteutuksessa huomioidaan ns. *state-of-the-art*[288]-vaatimus. Tällöin kyse on kulloiseenkin tilanteeseen parhaimpien järjestelmien hyödyntämisestä niiden kustannukset huomioiden.[289]

4.3.5. Tietoturvaratkaisut

Tietoturvallisuus on kaikkien perustarve. Kyse ei ole pelkästään yhden joukon tarpeesta, vaan kyse on yksilöiden, yritysten, yhteiskuntien ja valtioiden tarpeesta. Teknologian kehittyessä jokaisen on pakko kiinnittää enemmän huomiota turvallisuuteen, eikä esimerkiksi kyberturvallisuus ole minkään pienen asiantuntijajoukon keksintö. Se koskettaa meitä kaikkia, ja jokainen on vastuussa turvallisuuden (tunteen) onnistumisesta. Merkittävimmät puutteet liittyvätkin siihen, että tietoturvallisuutta pidetään vain teknologisena asiana, vaikka digitalisoituneessa maailmassa kyberturvallisuus on strateginen ja poliittinen asia, joka koskee sekä poliittisia päättäjiä että yrityselämän johtohenkilöitä. Turvallisuuden tulee olla organisaatioiden prioriteettilistalla korkealla, eikä organisaation tulisi toimia niin, että ensin kehitetään prosesseja, infrastruktuuria, tuotteita tai palveluita ja vasta tämän jälkeen pohditaan niiden turvallisuutta. Ketterä ja paras

[286] Järvinen, 2012, s. 78.
[287] Ks. Järvinen, 2018, s. 307.
[288] Ks. määritelmästä esim. TeleTrusT – ENISA: IT Security Act (Germany) and EU General Data Protection Regulation: Guideline "State of the art", Technical and organizational measures, 2021, s. 15–17.
[289] TSA 32 artiklan 1 kohta.

kyberturvallisuus mahdollistetaan rakentamalla se sisään eri järjestelmiin, tuotteisiin ja ratkaisuihin.[290] TSA:n oletusarvoinen ja sisäänrakennettu tietosuoja edellyttää organisaatioita ottamaan huomioon turvallisuuden tason jo suunniteltaessa järjestelmiä. Tässä mielessä organisaatioiden tulee kiinnittää huomiota vahvasti myös kybermaailman uhkiin.

Yleisesti organisaatioissa ei puhuta kyberturvallisuudesta vaan tietoturvasta. Tietoturvan kohde on yrityksen tietopääoma, joka kattaa aineettomat oikeudet, tietokannat, sopimukset, kontaktit, asiakastiedot, prosessikuvaukset ja niin edelleen. Tavoitteena tällöin on, että turvataan tiedon säilyminen, saatavuus ja liikuteltavuus sekä tiedon eheys ja luottamuksellisuus.[291] Tietoturva ja tietosuoja ovat kaksi eri asiaa, vaikka molemmissa on kyse tietojen suojaamisesta. Tietojen sisältö ja suojaamisen tarkoitus ovat erilaiset. Tietoturvassa suojataan itse tietoja ja tietojärjestelmiä sekä varmistetaan järjestelmien toiminta ja käytön turvallisuus kaikissa olosuhteissa. Tietosuojassa suojauksen kohteena ovat ihmisten henkilötiedot. Tällaisia tietoja ovat ilmeisten perustietojen lisäksi kaikki ihmisten ominaisuuksia ja toimintaa kuvaavat merkinnät. Siten tietosuojalla pyritään takaamaan yksilöille perusoikeutena turvattu oikeus yksityisyyteen sekä estää tämän tietojen tarpeeton ja epäasiallinen käyttö.[292] Tietosuoja on puolestaan käsitteenä monipuolisempi kuin yksityisyyden suoja. Esimerkiksi *Konstari* pitää tietosuojan käsitettä rekisterinpitoon ja tietojenkäsittelyn toiminnalliseen puoleen liittyvänä.[293] Asianmukaisella tietojen salassapidolla suojataan organisaation toimintaympäristön lisäksi asiakkaiden liike- ja ammattisalaisuuksia sekä turvataan yksilöiden yksityisyyden suojaa.[294] Kyberturvallisuutta voidaan pitää tietoturvaa laajempana kokonaisuutena, joka tuo turvallisuuden kohteeksi ihmisten ja bittien maailman yhdessä muodostaman kokonaisuuden. Kyberturvallisuutta ei voi rajata vain yrityksen omiin prosesseihin, vaan siihen täytyy sisällyttää koko yhteysverkosto. Organisaatioilla onkin vastuu teknologiaan pohjaavien toimintojen ylläpitämisestä ja oikeellisuuden varmistamisesta.[295]

Kyber tarkoittaa digitaalista maailmaa, ts. kaikessa laajuudessaan sitä bittien maailmaa, joka ympärillämme on ja joka vaikuttaa päivittäiseen elämäämme voimakkaammin kuin aina edes osaamme ajatella. Tämä maailma voidaan erottaa fyysisestä eli atomien muodostamasta maailmasta. Fyysinen atomien maailma ja digitaalinen bittien maailma eivät olet toisistaan

[290] Limnéll, ym., 2014, s. 13–14.
[291] Ibid., s. 55–56.
[292] Järvinen, 2012, s. 12.
[293] Konstari, 1992, s. 1–15.
[294] Andreasson – Koivisto, 2013, s. 32.
[295] Limnéll, ym., 2014, s. 55–56.

riippumattomia ja erillisiä. Päinvastoin ne kietoutuvat toisiinsa yhä tiukemmin, mikä puolestaan korostaa lisääntynyttä tarvetta varmistaa digitaalisen maailman toimivuutta sekä turvallisuutta.[296]

Turvallisuutta voi kuvata tavoitetilaksi, johon pyritään tekemällä erilaisia turvallisuutta lisääviä toimia. Tavoitetilaan pääsemisen vastapainona ovat uhkat, joiden arviointi on turvallisuuden vahvistamisen alku. Turvallisuudessa yhdistyvät tunne, todellisuus, opitut mallit sekä kykymme sietää erilaisia häiriö- ja kriisitilanteita. Turvallisuus on aina tunnetta siitä, miten turvalliseksi tunnemme itsemme siinä ympäristössä, jossa olemme. Uhkana voidaan pitää mitä tahansa toiminnan kannalta kielteistä asiaa, joka saattaa aiheuttaa vahinkoa tai muilla tavoin estää tai vaikeuttaa toimintaa. Turvallisuus on aina suhteellista, ja sen taso pitää suhteuttaa uhkaan. Esimerkiksi kyberuhkana voidaan pitää tahallisesti tai tahattomasti digitaalisessa maailmassa tapahtuvaa turvattavan kohteen turvallisuutta heikentävää tekijää. Suurin osa toteutuneista kyberuhkista on muita kuin tarkoituksella aiheutettuja, kuten erilaiset ohjelmistovirheet tai tekniset viat. Kun turvallisuutta toteutetaan, on sillä kolme ulottuvuutta. Ensinnäkin tulee pohtia sitä, mitä turvataan eli mikä on turvaamisen kohde. Toisekseen tulee pohtia mahdollisia uhkia eli sitä, miltä turvataan. Lopuksi näistä voidaan muodostaa käsitys siitä, miten kohdetta voidaan turvata eli mitkä ovat ne keinot, joilla uhkat torjutaan.[297]

Kyberturvallisuudesta huolehtiminen on jatkuva prosessi, jonka menetelmät tunnetaan huonosti. Ellei kybermaailman ja sen turvallisuuden suoria vaikutuksia tunneta organisaation sisällä, saattavat päätökset johtaa yllättäviin seurauksiin. Toisaalta näin monimutkaisessa maailmassa ei aina voida välttyä epäsuorilta vaikutuksilta.[298] Teknisiä tietoturvatoimia ovat esimerkiksi laitteille ja järjestelmiin pääsyn valvonta, tietojen ja järjestelmien luvattoman käytön esto, tapahtumien kirjaaminen, tietoliikenteen kybervalvonta ja reititysvalvonta, järjestelmien käyttöoikeuksien määrittely, ylläpitotoimien asianmukainen järjestäminen, tietojen ja järjestelmien suojaaminen tietoturvaa vaarantavilta teoilta tai tapahtumilta sekä tietoliikenteen häirinnän valvonta ja sen estäminen.[299] Tietojen ja järjestelmien suojaamisen ratkaisuja ovat muun muassa virustorjuntaohjelmistot, palomuurit, roskapostin suodatusohjelmistot, pääsynhallintatyökalut, vikatilanteiden osoituslaitteistot, tietovuotojen ehkäisytyökalut, kaksiosainen varmentaminen ja IP-lokijärjestelmät.[300]

[296] Limnéll, ym, 2014, s. 29–32.
[297] Ibid., s. 34–38.
[298] Ibid., s. 47–48.
[299] Pitkänen, ym., 2013, s. 215–216.
[300] Room, 2018, s. 188.

Tietoturva on laaja aihe, mutta yhteistä sille on pyrkimys kolmeen tavoitteeseen. 1) Tiedon tulee säilyä luottamuksellisena. Keskeisessä roolissa ovat tietoihin pääsyn rajoittaminen eri välineillä, kuten salasanoilla ja käyttäjäoikeuksien rajoittamisella. 2) Tietojen täytyy säilyä eheinä, millä tarkoitetaan sitä, että tietojen käsittelyn ja käytön aikana niihin tulee kohdistua vain oikeutettuja muutoksia. 3) Tietojen tulee olla saatavissa, koneiden käytettävissä, ja palveluiden tulee olla toimivia silloin, kun niiden käyttö on tarpeellista.[301] Tietoturvan tavoitteiden saavuttaminen edellyttää osapuolten todentamista.[302]

Organisatorisiin ja teknisiin toimenpiteisiin liittyen on tärkeää huomata, että kyse on prosesseista, jotka tulee tehdä TSA:n noudattamiseksi. Välineitä prosesseihin on monia. Kun puhutaan esimerkiksi vaaditun turvallisuustason toteuttamisesta, on kaiken lähtökohta strateginen toimintatapa organisaatiossa. Turvallisuuden rakentaminen lähtee strategiselta tasolta, jossa abstrakti visio muunnetaan operatiivisella tasolla toimintaohjeiksi. Kyse on oletusarvoisesta ajattelusta, sillä pyrkimyksenä täytyy olla turvallinen ympäristö. Strategian tekninen toteutus tapahtuu suorittavalla teknisten kyvykkyyksien tasolla. Suorittamisessa tulee jatkuvasti huolehtia sisäänrakennetusta tietosuojasta. Pelkän tietoturvan toteuttaminen ei siten välttämättä riitä. Kyberturvallisuuden näkeminen organisaatiossa strategisen tason kysymyksenä sitouttaa yrityksen johdon turvallisuusprosessiin. Tällöin tavoite tehokkaasta turvallisuuden tuottamisesta, inhimillisten virheiden vähentämisestä ja tuotannon laadun varmistamisesta onnistuu kokonaisuutena. Hyvänä vaihtoehtona on lähteä tavoittelemaan tietoturvaa laajempaa turvallisuuden tasoa laatimalla organisaatiossa kyberstrategia, jolla pyritään turvaamaan laajemmin organisaation toimintaa uhkia vastaan.[303]

4.4. Osoitusvelvollisuus

4.4.1. Yleistä

Osoitusvelvollisuuteen viitataan englanniksi termillä *accountability*. Termi esiintyy usein organisaatioiden sisäisen valvonnan toiminnassa. Vaikka usein osoitusvelvollisuuden ajatellaan syntyneen TSA:n tuloksena, on sillä kansainvälisesti pidemmät juuret. Kuten edellä käsiteltäessä oikeudellista viitekehystä kappaleessa 2.2.1. huomattiin, kansainvälisessä kontekstissa on jo aikaisemmin viitattu siihen, että rekisterinpitäjän tulisi olla vastuussa tietojen käsittelyssä, mutta toisaalta pohjalla on mielestäni ollut ajatus siitä, että pelkkä noudattaminen ei ole riittävää – sääntelyn noudattaminen tulisi myös pystyä osoittamaan. TSA:n myötä rekisterinpitäjä on

[301] Järvinen, 2012, s. 10.
[302] Ibid., s. 12.
[303] Ks. kyberstrategian rakentamisesta Limnéll, ym., 2014, s. 157–212.

suoraan vastuussa henkilötietojen käsittelystä. Pelkkä henkilötietojen käsittelyn oikeaoppisuus ei kuitenkaan riitä, vaan se pitää myös näyttää toteen. Ensimmäistä kertaa osoitusvelvollisuuden käsite ilmeni OECD:n yksityisyyden suojaa koskevien ohjeiden 14 artiklassa, jonka mukaan rekisterinpitäjän tulisi olla vastuussa ohjeiden ja toimenpiteiden noudattamisesta.[304] Ohje edellyttää, että rekisterinpitäjällä tulisi olla käytössään sen toimintaan liittyvä yksityisyyden hallintaohjelma, joka sisältää tietojen suojaamisen, tehokkaan hallintorakenteen ja valvontamekanismit. Ohjelman tulisi olla reagoiva, ja se tulisi päivittää säännöllisesti. Rekisterinpitäjän on myös oltava valmis osoittamaan ohjelman toiminta sääntelyviranomaisille ja muille asianmukaisille elimille. Lisäksi rekisterinpitäjän on ilmoitettava sääntelyviranomaisille tai muille asiaankuuluville viranomaisille, jos merkittäviä tietoturvaloukkauksia on tapahtunut, sekä ilmoitettava rekisteröidyille tällaisista rikkomuksista.[305] Osoitusvelvollisuudella ei asetettu vielä tällöin varsinaisesti uusia velvoitteita, vaan sillä tehostetaan tietosuojaperiaatteiden vaikutusta.[306]

Osoitusvelvollisuus käsitteenä siinä muodossa, jossa sen nykyisin ymmärrämme, on kehittynyt TSA:n tuloksena. TSA:n 5 artiklan 2 kohdan mukaan rekisterinpitäjä vastaa siitä, että edellä mainittuja tietosuoja-asetuksen yleisiä tietosuojaperiaatteita noudatetaan. Tämän ohella TSA:n 24 artiklan 1 kohdassa edellytetään, että rekisterinpitäjän on toteutettava tarvittavat tekniset ja organisatoriset toimenpiteet, joilla voidaan varmistaa ja osoittaa, että käsittelyssä noudatetaan tätä asetusta. Osoitusvelvollisuuden käsitteellä on laaja ulottuvuus, eikä ole vakiintunutta yhteistä näkemystä siitä, mitkä sen vaatimukset ovat tietosuojan näkökulmasta. Suomessa tietosuojavaltuutettu on koonnut sivuilleen listauksen toimenpiteistä ja dokumenteista osoitusvelvollisuuden toteuttamiseksi.[307] Myös monia TSA:n säännöksiä voidaan pitää osoitusvelvollisuutta koskevina säännöksinä: ilmoitukset rekisteröidyille, rikkomuksista ilmoittaminen, rekisterinpitäjien ja henkilötietojen käsittelijöiden väliset sopimukset, tietosuojavastaavan nimittäminen ja turvallisuusstandardien soveltaminen – kaikkia voidaan pitää vastuuvelvollisuuden mekanismeina. Lisäksi osoitusvelvollisuudella voidaan nähdä liittymäkohtia TSA:n 26 artiklan yhteisrekisterinpitäjiin, 29 artiklan mukaiseen tietojenkäsittelyyn rekisterinpitäjän ja henkilötietojen käsittelijän alaisuudessa, 30 artiklan edellytykseen käsittelytoimien selosteesta, 35 artiklan tietosuojaa koskevaan vaikutustenarviointiin ja 36 artiklan ennakkokuulemiseen.[308]

[304] OECD:n neuvosto hyväksyi 11. heinäkuuta 2013 tarkistetun suosituksen yksityisyyden suojaa ja henkilötietojen yli rajojen suuntautuvaa suojaa koskevista suuntaviivoista vuoden 2008 Soulin julistuksen seurauksena Internet-talouden tulevaisuudesta, missä arvioidaan yksityisyyden suojaa koskevat suuntaviivat *tekniikan, markkinoiden ja käyttäjien käyttäytymisen muutosten ja digitaalisten identiteettien kasvavan merkityksen* valossa.
[305] Ks. OECD Tietosuojasuositus artikla 15.
[306] WP 173, s. 2–4.
[307] Ks. Tietosuojavaltuutetun verkkosivut: https://tietosuoja.fi/osoitusvelvollisuus. Käytetty 2.5.2021
[308] Jay, ym., 2017, s. 170.

Tämän ohella osoitusvelvollisuudella on myös yhteys TSA:n 25 artiklan mukaiseen sisäänrakennettuun ja oletusarvoiseen tietosuojaan.

Osoitusvelvollisuuden käsite liittyy läheisesti henkilötietojen käsittelyyn liittyvän riskin arviointiin. Jotta rekisterinpitäjä voi päättää asianmukaisista strategioista vaatimusten noudattamisen toteuttamiseksi, hänen on kyettävä arvioimaan erityisesti käsittelyyn liittyvät riskit. Tämä käy ilmi TSA:sta, jossa vastuuvelvollisuutta määrittelevät artiklat edellyttävät myös rekisterinpitäjän suorittavan riskinarviointeja.[309] Tämä kokonaisuus muodostaa yhden, koherentin kokonaisuuden, jota jokaisen tulisi kyetä käsittelemään yhdessä eikä pitää velvollisuuksia irrallisina tietosuojaa koskevassa päätöksenteossa.

Rekisterinpitäjän velvollisuutena on toteuttaa asianmukaiset toimenpiteet. Päättäessään, mikä on tarkoituksenmukaista, rekisterinpitäjän on otettava huomioon käsittelyn *luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit*.[310] Luettelo asioista, jotka on otettava huomioon, on tuttu. Samaa lausetta käytetään sisäänrakennettua ja oletusarvoista tietosuojaa koskevassa TSA 25 artiklassa sekä TSA 32 artiklassa, joka koskee henkilötietojen käsittelyn turvallisuutta ja asianmukaisten turvallisuustasojen valintaa. Mielenkiintoista on kuitenkin se, että TSA:n 25 ja 32 artiklassa otetaan huomioon myös täytäntöönpanokustannukset ja turvatoimien nykytaso, kun taas asianmukaisten vastuutoimien kustannuksia ei sisällytetä 25 artiklaan. Tietosuojaa koskevan vaikutusten arvioinnin TSA 35 artiklassa käytetään myös lausetta *käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset* tietosuojaa arvioitaessa. Kyse on hyvin laajasta muotoilusta. Jayn mukaan kyse näyttää olevan siitä, että rekisterinpitäjän olisi tarkasteltava kaikkia tekijöitä, jotka vaikuttavat tietojen käsittelyyn, sosiaaliseen ja muuhun kontekstiin ja tietojen käyttöön tässä yhteydessä. Ilmaisulle olisi siten annettava sama laaja merkitys jokaisessa artiklassa, jossa sitä käytetään. Näiden tekijöiden arvioimiseksi on selvää, että rekisterinpitäjän on oltava täysin tietoinen käsiteltävän tiedon luonteesta ja muista käsittelyyn vaikuttavista tekijöistä. Velvollisuus pitää asianmukaista kirjanpitoa tehdystä käsittelystä auttaa täyttämään tämän velvoitteen. Jos rekisterinpitäjällä ei ole riittäviä tietoja, riskinarvioinnit ovat

[309] Jay, ym., 2017, s. 170.
[310] TSA 24 artiklan 1 kohta, ks. myös Jay, ym., 2017, s. 174–175, missä Jay katsoo, että lause kattaa selvästi rekisteröidyn oikeuksia ja vapauksia vahingoittavien tapahtumien todennäköisyyden, tällaisten tapahtumien esiintymisen sekä vaikutukset, jos sellaista tapahtuu. Sen arvioiminen, liittyykö tiettyyn käsittelyyn riski ja missä määrin, on erittäin tärkeää myös koskien sisäänrakennettua ja oletusarvoista tietosuojaa. Hän toteaa, että riskienhallinta on hyvin kehittynyt ala, ja riskien arviointiin ja hallintaan on olemassa erilaisia menetelmiä, vaikka useimmat eivät keskity yksityisyyden suojaan tai tietosuojariskiin. Hän ehdottaa myös, että rekisterinpitäjien ja henkilötietojen käsittelijöiden on sovellettava johdonmukaista lähestymistapaa asetuksen mukaisesti riskien arviointiin, ja hyötyä voi olla tutustumisesta esimerkiksi valmispohjiin, joita ovat tuottaneet ainakin CNIL, Norsk Regnesscentral sekä ICO.

todennäköisesti osittaisia ja mahdollisesti riittämättömiä. On huomattava, että asiaa koskevat johdanto-osan perustelukappaleet eivät lisää ilmaisuun tulkinta-apua, vaikka niissä annetaankin joitakin ohjeita siitä, mitä olisi pidettävä riskinä rekisteröidylle.[311] Tällaisia ohjeita ovat muun muassa se, että rekisterinpitäjän tulisi käyttää vain sellaisia henkilötietojen käsittelijöitä, joilla on riittävä asiantuntemus, luotettavuus sekä resurssit tietosuoja-asetuksen noudattamiseksi.[312]

Osoitusvelvollisuuden kohdalla on hyvä muistaa se, että lainsäädännön velvoitteiden noudattaminen ei sellaisenaan kuulu osoitusvelvollisuuteen, vaan velvollisuuden tosiasiallinen sisältö kohdistuu toiminnan lainmukaisuuden osoittamiseen.[313] Tässä yhteydessä osoitusvelvollisuudella on yllättävänkin tuttu merkitys organisaatioiden sisäisen tarkastuksen menetelmissä, joita suoritetaan liittyen esimerkiksi taloudellisten kysymysten tai yrityslainsäädännön noudattamiseksi. Tietosuojatyöryhmän lausunnossa (WP 173) on löydettävissä tekijöitä, joita yleisesti ottaen osoitusvelvollisuuden katsotaan sisältävän. Näitä ovat 1) jaetut ja molemminpuolisesti ymmärretyt standardit sekä selkeät tavoitteet, joita sovelletaan ja jotka kaikki toimijat hyväksyvät 2) selkeys eri toimijoiden vastuusta 3) läpinäkyvyys ja avoimuus kyseisten toimijoiden asiaankuuluvissa toimissa 4) todistettavissa olevien vaatimusten noudattaminen asianmukaisten käytänteiden, prosessien ja ihmisten kautta ja 4) tehokas oikeussuoja, seuraamukset ja oikaisumahdollisuus, jos prosessit, käytänteet tai henkilöt eivät ole toimineet asianmukaisesti.[314]

Osoitusvelvollisuus on itsessään näin ymmärrettynä itsenäinen, iso kokonaisuus osana TSA:ta. Tämän tutkimuksen kannalta on keskeistä huomata sen nivoutuminen myös osaksi sisäänrakennettua ja oletusarvoista tietosuojaa, sillä sen noudattaminen edellyttää sitä, että rekisterinpitäjä pystyy tämän myös osoittamaan. Tässä mielessä on syytä ymmärtää, että vaikka organisaatio suorittaa sisäistä valvontaa vastaavilla metodeilla muissa asioissa kuin tietosuojakysymyksissä, jälkimmäisissä tilanteissa se tulee pystyä myös osoittamaan. Tästä syystä myös sisäänrakennetun ja oletusarvoisen tietosuojan ottaminen jokapäiväiseksi aiheeksi edesauttaa osoitusvelvollisuuden täyttymistä, kun tulokset kirjataan. Katson osoitusvelvollisuuden olevan eräänlainen asianmukaisia organisatorisia ja teknisiä toimenpiteitä täydentävä (ja mahdollistava) väline. Tärkeimmät välineet, joilla osoitusvelvollisuutta puolestaan toteutetaan, ovat vaikutustenarviointi sekä käytänne- ja sertifiointimekanismit. Näiden lisäksi on tietysti dokumentoitava itse toimenpiteet. Dokumentointi on osa osoitusvelvollisuutta, ja sen avulla rekisterinpitäjä voi havainnoida käyttämiään asianmukaisia teknisiä ja organisatorisia toimenpiteitä.

[311] Jay, ym., 2017, s. 173.
[312] TSA johdanto-osan 81 perustelukappale.
[313] WP 173, s. 9.
[314] Jay, ym., 2017, s. 172.

4.4.2. Vaikutustenarviointi

Tietosuojaa koskeva vaikutustenarviointi eli (D)PIA on tietosuoja-asetuksen mukainen velvollisuus mutta myös työväline organisaatiolle kehittää omaa toimintaansa vastaamaan sisäänrakennetun ja oletusarvoisen tietosuojan periaatetta. Sisäänrakennetun ja oletusarvoisen tietosuojan kohdalla on tärkeää muistaa, että TSA suhteuttaa vaatimuksen saatavilla olevan tekniikan tasoon, toteuttamiskustannuksiin ja käsiteltävien tietojen laatuun. Merkitystä on myös käsittelyn luonteella, laajuudella, asiayhteydellä ja tarkoituksella sekä käsittelyn aiheuttamien riskien todennäköisyydellä ja vakavuudella. Asiaa täytyy punnita luonnollisten henkilöiden oikeuksille ja vapauksille aiheutetut riskit huomioon ottaen.[315]

On hyvä huomata, että PIA- ja DPIA-lyhenteitä käytetään vaihtoehtoisesti monissa eri tilanteissa, mutta näillä menettelyillä on eri roolit. Tästä syystä on keskeistä erottaa nämä käsitteet toisistaan. Tietosuoja-arviointi tai yksityisyyden vaikutusten arviointi (PIA), jota käsiteltiin jo aiemmin tarkoittaa siis *analysointia siitä, miten organisaatio kerää, käyttää, jakaa ja ylläpitää olemassa oleviin riskeihin liittyviä henkilökohtaisia tietoja.* Kyse on prosessista, jota käytetään henkilötietojen käsittelyn suojaamiseen suunnittelussa, kun organisaatio aloittaa tai ostaa uuden liiketoiminnan, toteuttaa uuden prosessin tai lanseeraa uuden tuotteen.

Tietosuojaa koskeva vaikutustenarviointi (DPIA) puolestaan tarkoittaa *henkilötietojen käsittelyyn liittyvien riskien tunnistamista ja minimointia.* Siinä kyse on jatkuvasta prosessista, jota sovelletaan säännöllisesti henkilötietojen käsittelyyn. Prosessissa tunnistetaan ja lievennetään riskejä. Vaikutustenarvioinnissa on kyse TSA:n 35 artiklan rekisterinpitäjän velvollisuudesta toteuttaa tietosuojaa koskeva henkilötietoihin kohdistuvien riskien arviointi. Vaikutustenarvioinnissa on kyse prosessista, jossa organisaatiot voivat järjestelmällisesti arvioida ja tunnistaa tarjoamiensa tuotteiden ja palveluiden yksityisyyden ja tietosuojan vaikutukset. Sen avulla he voivat ryhtyä asianmukaisiin toimiin estääkseen tai ainakin minimoidakseen nämä riskit. Mainittuja ongelmia voi syntyä kehitettäessä uusia tuotteita ja palveluita tai kun tehdään uusia toimia, joihin liittyy henkilötietojen käsittelyä.[316] Vaikutustenarviointia tehdessään rekisterinpitäjän tulee pyytää neuvoja tietosuojavastaavalta, jos sellainen organisaatioon on nimetty. Tämä velvollisuus ei kuitenkaan kuulu tietosuojavastaavalle. Jos rekisterinpitäjältä puuttuu kyky arvioida vaikutuksia, tulee tämän siitä huolimatta järjestää arviointi vaaditulla tavalla, esimerkiksi käyttäen alan ammattilaista. Jos ilmenee, että henkilötietojen käsittelystä aiheutuu riski, on

[315] Korpisaari, ym., 2018, s. 279.
[316] Pothos, 2018, s. 207.

vaikutustenarviointi tehtävä. On olemassa myös muita tilanteita, joissa TSA edellyttää arviointia. Tilanteet, joissa vaikutustenarviointia edellytetään, voidaan tiivistää seuraavasti:

1) Jos tietyntyyppinen henkilötietojen käsittely todennäköisesti aiheuttaa rekisteröidyn oikeuksien ja vapauksien kannalta korkean riskin.
2) Jos rekisteröidyn henkilökohtaisiin ominaisuuksiin koskevia henkilötietoja käsitellään automaattisesti, ja se johtaa päätöksiin, joilla on oikeusvaikutuksia tai ne vaikuttavat rekisteröidyn henkilöön merkittävästi.
3) Jos henkilötietojen käsittely kohdistuu TSA 9 artiklan 1 kohdassa tarkoitettuihin erityisiin henkilötietoryhmiin tai TSA 10 artiklassa tarkoitettuihin rikostuomioihin tai rikkomuksiin.
4) Jos suoritetaan yleisölle avoimena olevan alueen järjestelmällistä ja laajamittaista valvontaa.
5) Jos vaikutustenarviointia edellytetään kansallisissa erityisvaatimuksissa.

On syytä huomata, että luettelo ei ole tyhjentävä. Tapauksissa, joissa ei ole selvää, vaaditaanko tietosuojaa koskeva vaikutustenarviointi, sen tekemistä suositellaan joka tapauksessa, koska se auttaa rekisterinpitäjiä noudattamaan tietosuojalainsäädäntöä. Lisäksi tulee huomioida TSA:n 35 artiklan 4 kohdassa kansalliselta valvontaviranomaiselta edellytetty luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan vaikutustenarviointia. Tämän ohella tietosuojatyöryhmä on lausunnossaan (WP 248) pyrkinyt avaamaan tilanteita, joissa henkilötietojen käsittelyyn kohdistuu korkea riski. Korkean riskin muodostavat ainakin nämä henkilötietojen käsittelytilanteet, joissa käsittelyn kohteena on:

1) rekisteröidyn työsuoritus, taloudellinen tilanne, terveys, henkilökohtaiset mieltymykset tai kiinnostuksen kohteet, luotettavuus tai käyttäytyminen tai liikkumisen profilointi, ennakointi, arviointi tai pisteytys
2) muut arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot, jotka eivät kuulu erityisiin henkilötietoryhmiin tai rikostuomioihin, kuten kotitaloutta koskevat ja yksityiseen toimintaan (esim. sähköinen viestintä), perusoikeuden käyttämiseen (esim. sijaintitiedot) tai selvästi rekisteröidyn arkeen kohdistuvat vakavia vaikutuksia sisältävät tiedot (esim. taloudelliset tiedot tai henkilökohtaiset asiakirjat)
3) henkilötietojen käsittely laajamittaisesti
4) tietokokonaisuuksien sovittaminen yhteen tai yhdistäminen
5) heikossa asemassa olevat rekisteröidyt
6) uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen

7) tapaukset, joissa itse käsittelytoimet estävät rekisteröityjä käyttämästä oikeuksiaan tai palvelua tai noudattamasta sopimusta
8) bíometriset tai geneettiset tiedot
9) ilmiantojärjestelmää koskeva konteksti
10) rekisteröidyn informointia koskevan TSA 14 artiklan 5 kohdan poikkeussääntö[317]

Vaikutuksenarvioinnin kysymyksenasettelu ja metodologia on mahdollista ajatella siten, että se tukee tuote- ja palvelukehitystä sekä antaa mahdollisuuden organisaatiolle tunnistaa tietosuoja-riskejä ja -ratkaisuja. Vaikutustenarvioinnissa on tarkoitus *kuvata henkilötietojen käsittely, arvioida käsittelyn tarpeellisuutta, oikeasuhteisuutta sekä arvioida henkilötietojen käsittelystä aiheutuvia riskejä ja tarvittavia toimenpiteitä, joilla riskeihin puututaan.* Rekisterinpitäjän tulee varmistua käsittelyn oikeellisuudesta siinä kohtaa, kun käsittelytoimista päätetään ja sen lisäksi koko tietojen käsittelyn elinkaaren ajan. Vaatimus on päällekkäinen TSA:n 25 ja 35 artiklan velvoitteiden kanssa ja käytännössä rekisterinpitäjän tulee käsitellä näitä velvoitteita osana yhtä saumatonta prosessia. Tämä lienee mahdotonta toteuttaa ilman tuplatyötä, sillä velvollisuudet nivoutuvat toisiinsa. Mielenkiintoista on kuitenkin tässä mielessä se, että vaikutustenarviointia ei tarvitse tehdä järjestelmien kehitysvaiheessa. Vaikutustenarviointi on kuitenkin tehtävä ennen kuin henkilötietojen käsittelyyn ryhdytään. Vaikka tämä ei olekaan välttämätöntä, vaikutustenarvioinnin tekemistä on ehdotettu tehtäväksi mahdollisimman aikaisessa vaiheessa, joka voisi olla suunnittelun loppupuolella tai valmiin järjestelmän hankinnan kohdalla.[318] Euroopan komissio on suosituksessaan todennut, että (vapaaehtoisella) vaikutustenarvioinnilla on useita tehtäviä. Sitä voidaan pitää hyödyllisenä työkaluna, jolla rekisterinpitäjä pystyy noudattamaan sisäänrakennettua tietosuojaa varautuen potentiaalisiin riskeihin, jotka voivat paljastaa rekisteröidyn henkilötietoja. Työkaluna se on myös kansallisille tietosuojaviranomaisille hyödyllinen väline sääntöjen noudattamisen valvontaan.[319]

Vaikutustenarvioinnissa törmää helposti kahteen käsitteeseen. Ensinnäkin puhutaan *riskeistä* mutta toisaalta *uhkista*. Mikä näiden ero käytännössä on, ja miten niitä tulee ajatella osana vaikutustenarviointia? Uhka on käsitteenä monimuotoinen. Uhka voidaan määritellä sellaiseksi (periaatteessa) *pakottavaksi toiminnaksi, jossa toteutettavaksi uhatun toimen oletetaan saavan aikaan negatiivisen vaikutuksen kohteessa ja/tai kohteen intressissä*. Pakottavuus ilmenee siinä,

[317] WP 248, s. 9–12, ks. myös tietosuojavaltuutetun luettelo vaikutustenarviointia edellyttävistä käsittelytoimista https://tietosuoja.fi/luettelo-vaikutustenarviointia-edellyttavista-kasittelytoimista, luettu 29.12.2020.
[318] Jay, ym., 2017, s. 185.
[319] Ks. Euroopan komission suositus älykkäiden verkkojen ja mittausympäristöjen vaikutustenarvioinnista, kohta 1.3.

että kohteen toimintavaihtoehdot minimoidaan uhkaajan haluamallaan tavalla.[320] Bittimaailmassa kyse on usein siitä, että uhka on abstrakti: se voi olla *jokin mahdollisesti toteutuva epämiellyttävä tai vahingollinen asia tai vaara, joka uhkaa tai jonka voi ajatella uhkaavan tiettyä toimijaa*. Vahingollisen luonteensa vuoksi uhkaa pyritään estämään ja/tai torjumaan.[321] Uhka voi kohdistua organisaatioon sekä ulkopuolelta että sisäpuolelta.

Toisin kuin uhkaa, riskiä ei voida torjua, vaan se sisältyy kaikkeen toimintaan. Riskiä voi kuitenkin mitigoida. Riski ei myöskään ole ongelma, sillä ongelmat ovat seurauksia jostain jo tapahtuneesta. Riski on normaali olemassaolon ehto, joka tarkoittaa jonkin negatiivisen tapahtuman (tai ongelman) mahdollisuutta tulevaisuudessa. Riskien torjumisen sijaan niihin tulee varautua esimerkiksi riskiperusteisella lähestymistavalla, jolla pyritään välttämään, omaksumaan, rajaamaan tai lieventämään riskejä. Kyse voi olla myös siitä, että opitaan elämään riskien kanssa. Kyse on tavanomaisesti riskienhallinnasta, jolla pyritään järjestämään systemaattista ja jatkuvaa muutosta, koska toimijoilla ei ole muuta vaihtoehtoa. Riskienhallintaa voidaan kuvata metodiksi, jolla pyritään tunnistamaan, arvioimaan, valitsemaan, kehittämään sekä toteuttamaan vaihtoehtoja riskien käsittelemiseksi organisaatiossa.[322]

Käytännössä nämä kaksi velvollisuutta voidaan täyttää yhdessä prosessissa. Mahdolliset toteutustavat vaihtelevat laajasti, mutta vaikutustenarvioinnin on sisällettävä TSA:n 35 artiklan 7 kohdan mukaisesti vähintään seuraavat asiat: 1) järjestelmällinen kuvaus suunnitelluista käsittelytoimista ja käsittelyn tarkoituksista, 2) arvio käsittelytoimien tarpeellisuudesta ja oikeasuhteisuudesta tarkoituksiin nähden, 3) arvio rekisteröityjen oikeuksia ja vapauksia koskevista riskeistä ja 4) suunnitellut toimenpiteet riskeihin puuttumiseksi, mukaan lukien suoja- ja turvallisuustoimet ja mekanismit, joilla varmistetaan henkilötietojen suoja ja osoitetaan, että TSA:ta on noudatettu ottaen huomioon rekisteröityjen ja muiden asianomaisten oikeudet sekä oikeutetut edut. Käytännön toimien pohjalle voidaan asettaa seuraavanlainen ohjenuora:

1) Uuden käsittelyn yhteydessä rekisterinpitäjän tulee arvioida joko suunnitteluvaiheessa tai ennen uuden tietojärjestelmän hankintaa niiden riskien luonne, jotka todennäköisesti vaikuttavat tulevaisuuden käsittelyyn ja luokitella ne pieniksi, keskisuuriksi tai suuriksi ottaen erityisesti huomioon TSA:n 35 artiklassa suureksi riskiksi luetellut käsittelytyypit. Jos organisaatiolla on tietosuojavastaava, tulee hänen olla mukana.
2) Tämän arvioinnin jälkeen rekisterinpitäjän tulee arvioida, tarvitaanko täydellinen vaikutustenarviointi ennen uuden käsittelyn täytäntöönpanoa.

[320] Limnéll, ym., 2014, s. 105.
[321] Ibid., s. 106.
[322] Ibid., s. 108–109.

3) Kaikissa tapauksissa rekisterinpitäjän on tarkasteltava suojatoimien tasoa ja vaikutusta havaittujen riskien vähentämiseksi ja mahdollisuutta sisällyttää suunnitteluun muita suojaominaisuuksia. Rekisterinpitäjän on kirjattava tällaisten suojatoimien sisällyttämistä koskevat päätökset.
4) Kun järjestelmä tai tekniikka on kehitetty tai hankittu ja ennen sen käyttöönottoa, tulee suorittaa ns. toisen vaiheen tarkistus.
    a) Jos käsittely sisältää edelleen riskejä, mukaan lukien tapaukset, jotka ovat TSA:n 35 artiklan 3 kohdan a alakohdassa olevassa korkean riskin luokkien luettelossa, uudelleentarkastelun olisi täytettävä 35 artiklassa edellytetyt vaatimukset virallisesta vaikutustenarvioinnista.
    b) Jos käsittelystä aiheutuu keskitasoista tai vähäistä riskiä rekisteröidyn oikeuksille, uudelleentarkastelun olisi täytettävä TSA:n 25 artiklan 1 kohdan vaatimukset ja se olisi kirjattava sellaiseksi tietosuojakirjanpitoon.[323]

Vaikka edellä olevat toimet saattavat näyttää vaikeilta ja hankalilta, ei tästä syystä ole mahdollista jättää vaikutustenarviointia suorittamatta. Esimerkiksi Suomessa tätä tutkimusta kirjoitettaessa tietosuojavaltuutetun toimisto on julkaissut luonnoksen tietosuojan vaikutustenarvioinnin ohjeesta rekisterinpitäjien tueksi. Ohjeen rinnalle on laadittu myös yksinkertainen Excel-kirjaamistyökalu.[324] Tämän ohella internetistä on saatavilla lukuisia ohjeita ja valmiita työkaluja. Lisäksi yritysten tueksi on syntymässä enemmän kaupallisia palveluita, jotka helpottavat vaikutustenarvioinnin tekemistä.

4.4.3. Käytännesäännöt

Kuten aihetta käsiteltäessä on huomattu, ei ole mahdollista esittää kulloinkin täsmällistä ohjetta siitä, miten TSA 25 artiklaa tulee käytännössä soveltaa. Eri sidosryhmien panos onkin tässä mielessä erittäin merkityksellistä, sillä jokaisen toimialan oma konteksti edellyttää harkintaa asetuksen noudattamisessa. Yhtenä hyvänä vaihtoehtona voidaan pitää siten käytännesääntöjen *(Codes of Conduct)* luomista asiantuntijoiden johdolla, milloin TSA 25 artiklan sisältöä voidaan avata entistä enemmän. TSA 40 artiklan 2 kohdan h alakohdassa kehotetaan viranomaisia sekä yksityisiä toimijoita laatimaan käytännesääntöjä esimerkiksi asianmukaisten teknisten ja organisatoristen toimenpiteiden selventämiseksi. Mielestäni käytännesääntöjä koskevan TSA 40

[323] Jay, ym., 2017, s. 190–191.
[324] Ks. Tietosuojavaltuutetun toimiston luonnos tietosuojan vaikutustenarvioinnin ohjeesta rekisteripitäjien tueksi, https://tietosuoja.fi/-/tietosuojavaltuutetun-toimisto-pyytaa-kommentteja-uudesta-tietosuojan-vaikutustenarviointia-koskevasta-ohjeesta, käytetty 16.4.2021.

artiklan sisältöön liittyy kehotus sisäänrakennetusti ja oletusarvoisesti kehittää yhteisesti tietosuojakäytänteitä:

> *1. Jäsenvaltioiden, valvontaviranomaisten, tietosuojaneuvoston ja komission on edistettävä sellaisten käytännesääntöjen laatimista --.*
>
> *2. Yhdistykset ja muut elimet, jotka edustavat rekisterinpitäjien tai henkilötietojen käsittelijöiden eri ryhmiä, voivat tämän asetuksen säännösten soveltamisen täsmentämiseksi laatia käytännesääntöjä --.*

Artikla kannustaa kaikkia, kuten teollisuusyhdistyksiä, luomaan käytännesääntöjä kaikilla tietosuojavaatimusten noudattamisen osa-alueilla, ja niiden keskeinen piirre on, että rekisterinpitäjiä, jotka sitoutuvat soveltamaan käytännesääntöjä, olisi valvottava sääntöjen noudattamisen suhteen. Ylikansallisten sääntöjen hyväksyminen edellyttää TSA:n 63 artiklassa tarkoitetun yhdenmukaisuusmekanismin käyttöä, milloin luonnos säännöstöksi vaikuttaa ainakin kahteen EU:n jäsenvaltioon. Viitteitä siitä, miten käytännössä tämä voisi ilmetä, voidaan etsiä NAI:n (Network Advertising Initiative) käytännesäännöistä Yhdysvalloissa, joissa NAI panee ensin täytäntöön ohjeistuksensa jäsenyhdistyksen sisällä ja siirtää asian sitten Yhdysvaltain liittovaltion kauppakomissiolle (FTC), jos jäsenyhdistys on edelleen jättänyt noudattamatta ohjeistuksia.[325]

TSA:n 40 artiklan 4 kohdassa todetaan, että käytännesääntöihin on sisällyttävä mekanismi, jonka avulla akkreditoitu riippumaton elin voi valvoa, että rekisterinpitäjät ja henkilötietojen käsittelijät, jotka sitoutuvat soveltamaan sitä, noudattavat käytännesääntöjä.[326] Elimen akkreditointi on valvontaviranomaisen[327] tehtävä.[328] Asetuksessa on useita lakisääteisiä akkreditointiperusteita, ja valvontaviranomaisen on valmisteltava ja julkaistava muita kriteerejä ja vaatimuksia. Edellä 41 artiklan 1 kohdassa säädetty yleinen vaatimus on, että elimellä on oltava asianmukainen asiantuntemus säännöstön aiheesta. Asetuksen 41 artiklan 2 kohdassa todetaan, että jotta elimet voidaan akkreditoida, niiden on osoitettava riippumattomuutensa ja asiantuntemuksensa säännöstön aiheessa toimivaltaista valvontaviranomaista tyydyttävällä tavalla. Riippumattomuus edellyttää, että elin ei kuulu mihinkään osapuoleen tai että se voisi vaikuttaa

[325] Pothos, 2018, s. 236, ks. yhdenmukaisuusmekanismista Pothos, 2018, s. 248–249.
[326] TSA 4 artiklan 4 kohta ja TSA 41 artiklan 1 kohta.
[327] Toimivaltaisen valvontaviranomaisen, joka on toimivaltainen ja jonka olisi toimitettava kriteerit Euroopan tietosuojaneuvostolle ja myönnettävä akkreditointi, herättää joitakin vaikeita kysymyksiä. Oletuksena on, että tietosuojaneuvosto sopii keskeisistä kriteereistä, joita tullaan *prima facie* soveltamaan kaikkiin valvontaelimiin. Jay olettaa, että yksi valvontaviranomainen tulee ottamaan johtoaseman näiden ydinkriteerien kehittämisessä ja niiden toimittamisessa tietosuojaneuvostolle. Kun ydinstandardit on selvitetty, niitä sovelletaan kaikkialla EU:ssa, ja niitä soveltavat kaikki akkreditointia tekevät valvontaviranomaiset. ks. Jay, ym., 2017, s. 395–396.
[328] TSA 41 artiklan 1 kohta ja TSA 57 artiklan 1 kohdan p ja q alakohdat.

siihen. Vielä ei ole selvää, onko valvontaelinten toimittava erillisinä oikeushenkilöinä vai voisivatko ne olla yhteydessä muihin oikeushenkilöihin. Asiantuntemusvaatimus ei välttämättä edellytä asiantuntemusta tietosuoja-asetuksesta kokonaisuudessaan, vaan asiantuntemus voi mahdollisesti liittyä tiettyihin aloihin, kuten tietoturvallisuuteen. Näiden kykyjen osoittaminen edellyttää, että elin osoittaa tarvittavat ominaisuudet asianmukaisella tasolla ja että viranomainen hyväksyy nämä. Lisäksi TSA:n 41 artiklan 2 kohdan b ja c alakohdissa edellytetään, että elimillä on kyky järjestää seuraavat asianmukaiset sisäiset rakenteet ja menettelyt asioiden käsittelyä varten eli kyky 1) arvioida, ovatko rekisterinpitäjät ja henkilötietojen käsittelijät kelpoisia soveltamaan säännöstöä, 2) valvoa käytänteiden noudattamista, 3) arvioida säännöllisesti käytänteiden käyttämistä ja toimintaa, 4) käsitellä käytänteiden rikkomista koskevia valituksia ja 5) käsitellä rekisterinpitäjän tai henkilötietojen käsittelijän käytänteiden täytäntöönpanoa koskevat valitukset. TSA:n 41 artiklan 2 kohdan d alakohdassa edellytetään, että elimen on osoitettava valvontaviranomaista tyydyttävällä tavalla, että niiden "tehtävät ja velvollisuudet" eivät johda eturistiriitoihin.

TSA:n 57 artiklan 1 kohdan p alakohdassa valvontaviranomaiset velvoitetaan laatimaan ja julkaisemaan perusteet, joiden mukaisesti 41 artiklan mukainen valvontasäännöstön valvontaelin voidaan akkreditoida. Toimivaltaisen viranomaisen on toimitettava perusteet Euroopan tietosuojaneuvostolle johdonmukaisuusmekanismin mukaisesti.[329] Tietosuojaneuvosto antaa tämän jälkeen lausunnon elimen akkreditointiperusteista.[330]

Oikeudellisessa mielessä ajateltuna ollaan siirtymässä aikaan, jossa teknologian käytön sääntelyyn osallistuu uusia toimijoita. Perinteisessä mallissa lainsäätäjä on ainut autoritäärinen toimija. Nyt ollaan hyväksymässä entistä laajemmin alalla toimivien mahdollisuus alan sisäiseen sääntelyyn erityisesti metasääntelyn tasolla. Tämä on sinällään hyvin ymmärrettävää, sillä kuten jo aiemmin on todettu, perinteinen oikeusnormien tuottaminen on teknologista kehitystä hitaampaa. Tästä syystä alalla toimijoiden on itsesääntelyn avulla entistä helpompi luoda toimialalla paremmin sopivia ohjeistuksia. Kyse voi olla esimerkiksi koordinoinnista, johon osallistuvat sekä alan toimijat verkostoineen itse että myös ylikansalliset toimielimet. Tässä yhteydessä saattaa ilmetä kuitenkin ongelmia. Kyse on siitä, että henkilötietojen käsittelystä kilpailijalle annettavat tiedot voivat olla laittomia kilpailunrajoituksia ja päätyä siten kilpailuoikeudellisessa mielessä arvioitavaksi. Toimialan sisällä käytävät neuvottelut henkilötietojen käsittelyn osalta tulee järjestää geneerisesti niin, että keskusteluja käydään ainoastaan esimerkiksi yksilön suojaamisen intressissä. Lisäksi markkinoilla itsellään on merkitystä, kuten myös kunkin

[329] TSA 41 artiklan 3 kohta.
[330] Jay, ym., 2017, s. 394–395. Ks. akkreditointiperusteista TSA 64 artiklan 1 kohdan c alakohta.

valtion kansallisilla hallituksilla. Kuitenkaan tällainen ei ole täysin ongelmatonta, ja kritiikkiä on helppo ymmärtää. Ongelmalliseksi tämän tekee se, että useiden toimijoiden piirissä käsiteltävät käytännesäännöt saattavat aiheuttaa epätietoisuutta siitä, mikä on milloinkin vallitseva, niin sanottu oikea käytäntö. Toisaalta se aiheuttaa myös viranomaisille ongelmia siitä, mikä heidän roolinsa on tai mihin sääntöihin tilanteessa nojaudutaan. Tässä tietosuojavaltuutetun toimisto joutuu käyttämään paljon aikaa. On kuitenkin todettava, että tietoisuus tästä mahdollisuudesta on lisääntynyt, ja jossain määrin se hyväksytään entistä laajemmin. Valtioiden ulkopuolisten toimijoiden vaikutusvalta on nykyisen verkkoympäristön tunnusmerkki.[331] Tätä voidaan verrata jo edellä mainittuihin reiluihin tiedotuskäytäntöihin (FIPs), jotka ovat olleet pitkään Yhdysvalloissa teknologia-alan itsensä muovaamia. Tällöin aloille syntyy helpommin sen ominaispiirteet huomioon ottavaa, koherenttia toimintaa. Lienee siten mahdollista todeta, että sääntelyn suhteen jako tulee toteuttaa sopivassa tasapainossa niin, että suuret linjaukset sääntelyn suunnasta (esimerkiksi ihmisarvon kunnioittamisen ja yksityisyyden suojan lisäämisestä teknologisessa kehityksestä) tehdään unionin ja jäsenvaltioiden tasolla, mutta tarkkarajaiset ohjeistukset kunkin alan käytännön toimista (alojen yksityiskohtaiset ominaispiirteet huomioon ottaen) esimerkiksi sisäänrakennetun ja oletusarvoisen tietosuojan osalta voitaisiin laatia luomalla alalle omat käytänteet alan toimijoiden kesken.

Sisäänrakennetun ja oletusarvoisen tietosuojan osalta käytännesäännöillä on tärkeä rooli ensinnäkin siinä mielessä, että niiden avulla rekisterinpitäjät pystyvät yhteistyöllä kehittämään tietosuojaratkaisuja, jotka palvelevat TSA:n tarkoitusta. Toisekseen rekisterinpitäjille on keskeistä pystyä osoittamaan tietosuojatoimenpiteidensä täytäntöönpano. Yhtenä osoitusvelvollisuuden noudattamisen välineenä voisi olla juuri nojautuminen yhteisesti hyväksyttyihin käytännesääntöihin. Tämä puolestaan vähentää rekisterinpitäjän itsensä suurta vaivaa pohtia kulloinkin asianmukaisuusvaatimuksen täyttymistä sekä tarpeellisia teknisiä ja organisatorisia toimenpiteitä. Näen siten käytännesääntöjen palvelevan niin rekisteröityjen oikeuksia kuin myös rekisterinpitäjän kykyä noudattaa tietosuojavelvoitteita.

Käytännesääntöjen valvontaelimiä ei ole toistaiseksi juuri nähty. Tämän taustalla lienee se, että ei ole olemassa vielä yhtenäistä linjaa tietosuojan kokonaisvaltaiseen toteutukseen. Suomessa ollaan kuitenkin hyvässä tilanteessa siinä mielessä, että tietosuojavaltuutetun toimisto julkaisi käytännesääntöjen valvontaelinten akkreditointikriteeristön alkuvuodesta 2021.[332] Näitä ohjeita tulee hyödyntää yhdessä Euroopan tietosuojaneuvoston ohjeistusten kanssa.[333]

[331] Ks. Leiser – Murray, 2017, s. 692–693.
[332] Suomen kansallisen valvontaviranomaisen akkreditointikriteeristö yleisen tietosuoja-asetuksen mukaisten käytännesääntöjen valvontaelimille, Tietosuojavaltuutetun toimisto Dnro. 572/117/20, annettu 29.1.2021.
[333] Ks. Tietosuojaneuvoston ohjeistus käytännesääntöjä ja valvontaelimiä koskevista suuntaviivoista 1/2019.

Tietosuojavaltuutetun toimiston akkreditointikriteeristön perusteet ovat hyvin vaativia, sillä valvontaelimen tulee olla esimerkiksi taloudellisesti riippumaton ja vakaa, sekä valvontaelimen tulee järjestää itselleen muista toimijoista riippumaton rahoitus. Perusteissa edellytetään lisäksi, että valvontaelimen henkilöstöllä on oltava perusteellinen tietosuojaosaaminen.[334] Perusteellisen osaamistason määrittämineen on hyvin vaikeaa. Voi olla, että Suomeen ei lähitulevaisuudessa saada käytännesääntöjä käyttöön siinä määrin kuin TSA:n sisältö antaa toivoa.

4.4.4. Sertifiointimekanismit

Sertifiointimekanismien käyttö vaatimusten noudattamisen osoittamiseksi on ollut tietosuojasääntelyn yksi kehityskohteita. TSA:n myötä sertifiointien jakaminen on mahdollistettu virallisella tasolla. Tietosuojan kohdalla sertifiointia voidaan ajatella eräänlaisena ”sinettinä”, ”merkkinä” tai ”tavaramerkkinä”. TSA:ssa ei ole juuri ohjeistusta siitä, miten näiden kanssa tulisi toimia.[335] TSA:n johdannossa todetaan, että *läpinäkyvyyden ja tämän asetuksen noudattamisen tehostamiseksi olisi edistettävä sertifiointimekanismien sekä tietosuojasinettien ja -merkkien käyttöönottoa, jotta rekisteröidyt voisivat nopeasti arvioida asianomaisten tuotteiden ja palvelujen tietosuojan tason*.[336] Yleensä sinetti tai merkki on osoitus siitä, että prosessi tai tuote on käynyt läpi asianmukaisen tarkastusmekanismin. Sinetit ja merkit ovat siis onnistuneen ja läpäistyn tarkastuksen tulos. Näin ollen sertifiointimekanismi antaa laajimmassa merkityksessä varmuuden siitä, että tuote, prosessi tai palvelu täyttää tietyt asianmukaiset standardit.[337] On syytä huomata, että sinetin tai merkin saaminen ei poista rekisterinpitäjän tai käsittelijän vastuuta noudattaa TSA:ta. Myöskään se ei ole virallinen tapa osoittaa asetuksen noudattamista, vaikkakin se on yksi keino rekisterinpitäjälle osoittaa menettelevänsä sisäänrakennetun ja oletusarvoisen tietosuojan mukaisesti. Tässä tutkimuksessa pidän sertifiointimekanismeja kuitenkin osana osoitusvelvollisuutta hahmottamisen helpottamiseksi.

TSA 42 ja 43 artiklan mukaiset sinettejä ja merkkejä koskevat sertifiointisäännökset ovat jokseenkin monimutkaisia mutta toimivat samalla tavalla kuin edellä käsitellyt hyväksytyt käytännesäännöt. Sertifioinnin myöntävät sertifiointielimet, joita ovat joko kansallinen tietosuojaviranomainen tai tietosuojaviranomaisen hyväksymä akkreditoitu elin.[338] Hyväksynnän saamiseksi sertifiointielinten on täytettävä tietosuojaviranomaisten asettamat vaatimukset riippumattomuudesta ja asiantuntemuksesta sekä vältettävä eturistiriitoja. Lisäksi elimellä on oltava

[334] Ks. Tietosuojavaltuutetun toimiston käytännesääntöjen valvontaelinten akkreditointikriteeristö, s. 2–6.
[335] Jay, ym., 2017, s. 399.
[336] TSA johdanto-osan 100 perustelukappale.
[337] Jay, ym., 2017, s. 400.
[338] Ks. TSA 43 artiklan 1 kohta.

menettelyt valitusten käsittelemiseksi.[339] Jotta sertifioinnilla olisi vaikutusta, on lisäksi huomioitava se, että TSA mahdollistaa rekisterinpitäjien ja henkilötietojen käsittelijän rankaisemisen hallinnollisella seuraamusmaksulla sertifikaatin sääntöjen vastaisesta toiminnasta ja rikkomisesta.[340]

Yhtenä esimerkkinä olemassa olevista järjestelmistä voidaan pitää Ranskan tietosuojaviranomaisen, *Commission nationale de l'informatique et des libertés (CNIL)*, julkaisemaa järjestelmää, jota kutsutaan *standardiksi*. Siinä asetetaan yksityiskohtaisia vaatimuksia yksityisyyden hallinnassa käytettävistä menettelyistä. Standardi on jaettu 25 erilliseen vaatimukseen. Niissä kuvataan useita vaiheita, joita CNIL pitää tarpeellisena osana tehokasta tietosuojahallintaohjelmaa. Tällaisia vaiheita ovat esimerkiksi sisäisen ja ulkoisen tietosuojakäytännön kehittäminen sekä tietosuojatarkastukset. Rekisterinpitäjä, joka voivat osoittaa noudattavansa uutta standardia, voivat saada CNIL:ltä *yksityisyyssinetin*.[341]

5. JOHTOPÄÄTÖKSET

5.1. Ajattelumallin muutos

Yhtenä tämän tutkimuksen kantavana ajatuksena olen pyrkinyt valaisemaan niin tieteellistä näkökulmaa sisäänrakennetun ja oletusarvoisen tietosuojan takana kuin myös esittämään lainopillisesti ajateltuna, mitä asianmukaiset tekniset ja organisatoriset toimenpiteet käytännössä tarkoittavat. Loppujen lopuksi kaiken lähtökohta on vaatimus siitä, että yksilöt sisäistävät yksityisyyden ja henkilötietojen suojan merkityksen yhteiskunnallisena perus- ja ihmisoikeutena, ja täydentävät omia arvojaan liittämällä nämä oikeudet osaksi omaa arvomaailmaansa. Siten keskeisenä tutkimuksen tuloksena on, että uusi tietosuolainsäädäntö edellyttää uudenlaisen tietosuojakulttuurin hyväksymistä osaksi arkea.

Ajattelumallia tulee muokata siten, että teknologiasta tulee tehdä luottamuksemme arvoinen. Esimerkiksi *Hartzogin* Privacy's Blueprint pyrkii lainsäädännön teknologianeutraalisuuteen kehittämällä uudenlaisen tietosuojalainsäädännön teoreettiset perustelut, jotka reagoivat siihen, miten ihmiset todella havaitsevat ja käyttävät digitaalista teknologiaa. *Hartzog* kysyy oivallisesti, miksi yritykset ovat vastuussa käyttäjille sanallisista lupauksista, mutta yritykset ovat vähemmän vastuussa suunnittelun kautta käyttäjille toimitetuista lupauksista.[342] Jos haluamme

[339] Ks. TSA 43 artiklan 2 kohta.
[340] Ks. TSA 83 artiklan 4 kohdan b alakohta.
[341] Deliberation No. 2014-500 of 11 December 2014 on the Adoption of a Standard for the Deliverance of Privacy Seals on Privacy Governance Procedures, saatavilla https://www.cnil.fr/sites/default/files/typo/document/CNIL_Privacy_Seal-Governance-EN.pdf, käytetty 3.2.2021.
[342] Hartzog, 2018, s.169.

olla vapaita muiden puuttumisesta asioihimme, teknologia ei saa rasittaa käyttäjiä niin monilla käytännön toimenpiteillä, että se musertaa kyvykkyyden vaikuttaa, toisin sanoen käyttämään niitä. Paljon parempi vaihtoehto on, että keskitytään siihen, miten suunnittelemalla teknologiaa voidaan lisätä luottamusta muihin ihmisiin, sekä varmistamaan, että lupaukset täytetään. Paras suunnittelu priorisoi kontrollin siellä, missä se on tärkeintä ja hyödyllisintä ilman, että siitä tulee taakka.[343]

Globaalisti ollaan siirtymässä neljänteen teolliseen vallankumoukseen. Tätä vallankumousta on kutsuttu nimellä Industry 4.0 (IND 4.0). Samalla siinä on kyse Saksasta kotoisin olevasta *sui generis* -sääntelykonseptista, jossa *Möller* pitää sisäänrakennettua ja oletusarvoista tietosuojaa tärkeänä. Sisäänrakennettu ja oletusarvoinen tietosuoja ottaa huomioon IND 4.0:n erityispiirteet, koska sille ovat ominaisia älylaitteet. Sen tarkoituksena on lieventää yksityisyyden riskejä, joita voi esiintyä älykkään yrityksen kaikilla osa-alueilla ja näin ollen valmistajia tulee kannustaa sisällyttämään tietosuojavaatimukset osaksi teknologista suunnittelua.[344] Tulevaisuuden teknologiseen kehitykseen liittyen onkin positiivista, että TSA:ssa sisäänrakennetun ja oletusarvoisen tietosuojan puitteissa annetaan toimijoille tietynlainen joustamismahdollisuus ilman tarkkarajaista sääntelyä siinä, miten teknologian tulisi käyttäytyä suojatakseen rekisteröityjen oikeuksia. Samalla tulevaisuuden teknologian kehitystä rajoittavat käyttötarkoitussidonnaisuus ja automatisoidun päätöksenteon lähtökohtainen kielto.

Keskeisin huomioni ajattelumallin muuttamisessa piilee siinä, että luottamusta tulee rakentaa rekisterinpitäjän ja rekisteröidyn välillä. Luottamuksen saavuttaminen edellyttää, että yksilöt pystyvät ymmärtämään teknologisten ratkaisujen toiminnan ja sen, miten heidän henkilötietojaan käsitellään. Luottamuksen rakentamiseksi rekisterinpitäjiltä edellytetään uudenlaista asennetta tarkastella ja havainnoida potentiaalisia riskejä, joita syntyy jatkuvasti uudenlaisia. Teknologian kehittyessä sääntelyä nopeammin, tulee rekisterinpitäjän pystyä tässä tutkimuksessa esitettyjen periaatteiden mukaisesti huolehtimaan yksilön eduista ja oikeuksista. Luottamusta voidaan rakentaa monella eri tavalla. Ainakin itse koen asian niin, että jos rekisterinpitäjä omaksuu sisäisesti ajatusmallin sisäänrakennetusta ja oletusarvoisesta tietosuojasta, ja ymmärtää toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet minun henkilötietojeni suojaamiseksi, kykenen luottamaan henkilötietojen käsittelyyn. Jos henkilötietojen suojaa ei lähestytä oletusarvoisesti käsittelyn yhteydessä, en pysty täysin luottamaan rekisterinpitäjään.

[343] Hartzog, 2018, s. 95.
[344] Ibid., s. 46.

5.2. Lopuksi

On hyvä pitää myös tämän tutkimuksen taustalla se, että olemme Euroopan unionin ansiosta hyvässä asemassa. Henkilötietojen käsittelyyn liittyen tulee pitää lähtökohtana, että yksilöllä on oikeus päättää häntä koskevien henkilötietojen käsittelystä haluamallaan tavalla aina, kun se vain on mahdollista. Toisin voisi olla, sillä esimerkiksi Yhdysvalloissa tiedon kerääjä omistaa sanotun tiedon, ja vain osaa tiedoista, kuten terveystietoja, suojataan lailla.[345] Jo tässä mielessä onkin siten varsin ongelmallista, että tietojamme liikkuu ties missä ja niitä saatetaan käsitellä miten tahansa.

Itsemääräämisoikeuteen kuuluu se, että voimme tehdä ratkaisuja siitä, mihin ja milloin luovutamme tietojamme. Tämän oikeuden sisällä oleva joustovara vaikuttaa tutkimuksen tuloksena olevan riittävä. Yksilön kannalta ei olisi järkevää siirtyä absoluuttiseen henkilötietojen salaamiseen, sillä tällöin sosiaalinen kanssakäyminen ja palveluiden käyttäminen yhteiskunnassa estyisi. Se ei ole myöskään yhteiskunnan etu, sillä liiallinen eristäytyminen ei edesauta yhteiskunnan kehittymistä. Sen sijaan yksilön tietoisuus henkilötietojen käsittelyn toteuttamisesta auttaa parantamaan yksilön suojaa. Kun yksilölle viestitään henkilötietojen käsittelystä, se lisää luottamusta yhteiskuntaa kohtaan enemmän kuin liian tarkkarajaisen kontrollin käyttäminen. Toisaalta pidän tärkeänä sitä, että yksilöille jätetään mahdollisimman paljon vaikutusmahdollisuuksia ohjata henkilötietojen käsittelyä hänen haluamallaan tavalla. Vastapainona yksilöiden tulee ymmärtää, että heidän tietojaan käsitellään esimerkiksi lakisääteisiin velvoitteisiin perustuen.

Kuten olen tässä tutkimuksessa esittänyt, ei sisäänrakennettua ja oletusarvoista tietosuojaa tai tietosuojalainsäädäntöä itsessään tule pitää vaikeana ja hankalana maanvaivana. Sääntely on pyritty tekemään mahdollisimman joustavaksi, jotta se olisi teknologianeutraalia niin pitkälle kuin se ylipäänsä on vain mahdollista. Teknologian kehittyessä on helpompi soveltaa voimassa olevaa sääntelyä, kun se on tarpeeksi joustavaa. Kuten olen tutkimuksessa tuonut esille, jokaisella käytännön soveltamistilanteella on oma kontekstinsa. Tämäkin tulee ottaa huomioon, ja tässä periaatesääntelyllä on iso merkitys. Yksilön oikeutta yksityisyyteen ja henkilötietojen suojaan tulee kunnioittaa sisäänrakennetun ja oletusarvoisen tietosuojan avulla. Ne keinot, joilla tämä tapahtuu, ovat suhteellisen yksinkertaisia.

Kaiken kaikkiaan kaikki on kiinni eräänlaisesta varovaisuudesta, johon tulisi kiinnittää huomiota arjessa – samoin kuin esimerkiksi tätä kirjoittaessa kukin käyttää varovaisuutta

[345] Schneier, 2015, s. 229.

pandemian suhteen ja huolehtii hygieniastaan. Toimenpiteet, joilla oletusarvoista ja sisäänrakennettua tietosuojaa voidaan parantaa, eivät aina siten ole merkittäviä tietoteknisiä ratkaisuja vaan järjenkäyttöä liiallisten tietojen antamisessa tai ylimääräisen seurannan mahdollistamisessa.

TSA 25 artiklassa tarkoitetuilla teknisillä toimenpiteillä viittaavat suurimmilta osin riittävän tietoturvallisuuden aikaansaamiseen vaadittuihin keinoihin. Tekniset toimenpiteet kattavat esimerkiksi TSA 32 artiklassa mainitut, mutta voivat olla myös jotain muuta. Tässä yhteydessä kontekstilla on merkitystä. On eri asia turvata valtionsalaisuuksia kuin pienyrittäjän asiakasrekisteriä. Tekniset toimenpiteet toisaalta eivät pelkästään liity tietoturvallisuuteen. Kyse voi olla muista teknistä toteutusta vaativista keinoista, joilla turvataan yksilön oikeutta henkilötietojen suojaan. Teknologiasta puhuttaessa se rinnastetaan usein vaikeisiin koodaamista edellyttäviin toimiin. Kuten tässä tutkimuksessa on käynyt ilmi, yllättävän pieni osa esitetyistä keinoista vaatii suuria ponnisteluja tai resursseja tavoitteiden täyttämiseksi. Kyse on ainoastaan siitä, että tiedostetaan käytettävissä olevat keinot, ja toteutusta ei tule pitää liian monimutkaisena.

Organisatorisissa toimenpiteissä keskeistä on tietosuojasta viestiminen ja tietoisuuden jakaminen. Rekisterinpitäjä ei yksinään pysty toteuttamaan henkilötietojen käsittelyä. Käsittelyyn osallistuvat esimerkiksi rekisterinpitäjän työntekijät, joilla täytyy olla tietopääomaa henkilötietojen suojasta. Vaikka rekisterinpitäjällä olisi käytössä parhaimmat teknologiset ratkaisut, ei henkilötietojen käsittely voi onnistua tietosuoja-asetuksen mukaisesti ilman huolehtimista käsittelystä ruohonjuuritasolla. Johtoryhmän pöydän ympärillä kaikki saattavat olla hyvin perillä tietosuoja-asetuksen vaatimuksista, mutta niistä tulee myös viestiä käytännön tasolle. Henkilötietojen käsittelyn prosesseja tulee arvioida ja kehittää jatkuvasti huomioiden käsittelyn varsinaiset toteuttajat.

Osoitusvelvollisuuden puolesta rekisterinpitäjän tulee ymmärtää, että esimerkiksi dokumentointi ja riskienarviointi ei ole ylimääräistä työtä. Arvioinniksi ei käy sisäiset keskustelut organisaation sisällä, vaan toimenpiteet tulee täsmällisesti kirjata osoitusvelvollisuuden perusteella osaksi kirjanpitoa. Kun asiat kirjataan ylös, tulee samalla tarkasteltua organisaation tietosuojaprosesseja myös paperilla. Tämä puolestaan edes auttaa toteuttamaan sisäänrakennettua ja oletusarvoista tietosuojaa. Osoitusvelvollisuus edellyttää rekisterinpitäjältä pientä panostusta käytänteiden luomiseen. Esimerkiksi vuosikellojen ja vastaavien suunnitelmien luominen helpottaa huomattavasti esimerkiksi tietojen minimointia.

Tarkoituksenani on ollut selventää asianmukaisia teknisiä ja organisatorisia toimenpiteitä. Kuten tutkimuksesta on käynyt ilmi, tyhjentävän luettelon muodostaminen on mahdotonta.

Toisaalta se ei edes ole tarkoituksenmukaista. Toin tutkimuksessa esille laajalti yksilön oikeutta yksityisyyteen ja henkilötietojen suojaan. Nämä oikeudet ovat tärkeitä asianmukaisten ja organisatoristen toimenpiteiden osalta siinä, että jos jonkin toimenpiteet asianmukaisuutta ja tarvetta joudutaan pohtimaan, tulisi mielestäni rekisterinpitäjän arvioida tilannetta yksityisyyden ja henkilötietojen suojan valossa. Tähän voidaan lisäksi yhdistää kulloinenkin konteksti. Arviointi tulisi tehdä sen perusteella, miten kulloinkin rekisteröity voisi kohtuudella olettaa henkilötietojaan suojattavan. Riittävän turvallisuustason rakentamisessa tulee huomioida siten konteksti ja yksilön luottamuksen suoja siihen, että hänen henkilötietojaan suojataan.

Tätä maisteritutkielmaa kirjoittaessa vallitseva pandemia, COVID-19, on asettanut suuria haasteita yksityisyydelle ja henkilötietojen suojalle. Olemme joutuneet yhtäkkiä tilanteeseen, jossa operoimme entistä enemmän syvällä tietojärjestelmissä käyttäen teknisiä järjestelmiä ja laitteita. Toisaalta pandemia on osoittanut nämä haasteet arkipäiväisiksi ja todellisiksi uhkakuviksi, joihin tulee suhtautua asianmukaisella vakavuudella. Toisaalta tiedostamme yksityisyyden merkityksen entistä enemmän tarkkaillessamme, onko kameramme päällä vai ei. Toisaalta tiedämme, että tietojamme kerätään lukuisiin tarkoituksiin. ”Omaisuudellamme” eli henkilötiedoillamme käydään kauppaa. Tietovuodoista on puhuttu entistä enemmän, ja niiden merkitys yhteiskunnallisesti on ollut suuri. Yksilönä emme voi olla varmoja siitä, että tietomme ovat turvassa.

Kaiken tämän paineen alla lienee syytä todeta, että rekisterinpitäjien on herättävä todellisuuteen aivan uudella tavalla ja rakennettava itselleen uudenlainen tapa kohdata henkilötietojen käsittelyyn liittyvät yksityisyyden suojan kysymykset. Tutkimuksessa olen huomannut, ettei oletusarvoisen ja sisäänrakennetun tietosuojan sisältö TSA:ssa ole täydellinen ja helposti ymmärrettävissä. TSA sisältääkin paljon puutteita, mutta se on selvästi oikeassa linjassa siihen, miten tulevaisuuden tulee muotoutua. Keskeistä olisi pyrkiä olemaan ylpeä siitä, miten meillä jokaisella omassa roolissamme on mahdollisuus vaikuttaa omilla toimillamme toisten yksilöiden perus- ja ihmisoikeuksiin. Siten meidän teoillamme on merkitystä myös laajemmassa mittakaavassa, vaikka emme sitä aina tiedostakaan. Suunta on oikea, mutta jokaisen tulee tehdä *oma parhaansa* varjellakseen yksilöiden oikeuksia. Olemme sen velkaa toisillemme, itsellemme ja lapsillemme.