

LIIKESALAISUUSSUOJAN TULKINTA DATASÄÄDÖKSESSÄ JA DATAN SOVELTUMINEN LIIKESALAISUUDEKSI

Annemari Kauppi

Lapin Yliopisto

Oikeustieteiden tiedekunta

Maisteritutkielma

Immateriaalioikeus

Kevät 2025

Lapin yliopisto

Tiedekunta: Oikeustieteiden tiedekunta

Työn nimi: Liikesalaisuussuojan tulkinta datasäädöksessä ja datan soveltuminen liikesalaisuudeksi

Tekijä/-t: Annemari Kauppi

Koulutusohjelma/oppiaine: OTM, Immateriaalioikeus

Työn laji: Pro gradu -tutkielma/Maisteritutkielma_x_ Lisensiaatintutkimus__

Sivumäärä, liitteiden lukumäärä: XIV + 74

Vuosi:2025

Tiivistelmä:

Tutkimus tarkastelee esineiden internetin (IoT) datan jakamisen ja liikesalaisuussuojan tasapainoa Euroopan unionin datasäädöksessä ((EU) 2023/2854) sekä sitä, miten IoT-data soveltuu liikesalaisuuden määritelmään. Datasäädöksen mukaan datan haltija voi vaatia ennen datan luovutusta käyttäjältä ja kolmannelta osapuolelta sopimusta liikesalaisuuksien suojaamiseksi tarvittavista toimenpiteistä. Lisäksi datan haltija voi pidättäytyä, keskeyttää tai kieltäytyä datan jakamisesta tietyissä tilanteissa. Tätä kutsutaan komission mukaan ”liikesalaisuuksien käsijarru” -mekanismiksi.

Tutkimuksessa tarkastellaan lainopillisten metodien avulla, milloin data voi saada liikesalaisuussuojaa. Data voi täyttää liikesalaisuuden kriteerit, jos sillä on taloudellista arvoa salaisuutensa vuoksi ja sen haltija on ryhtynyt kohtuullisiin suojaustoimenpiteisiin. Lisäksi tutkimuksessa tulkitaan ja systematisoidaan datasäädöksen liikesalaisuuksia koskevia artikloja sekä annetaan de lege ferenda -suosituksia siitä, miten datan saatavuuden ja liikesalaisuuksien suojan välistä tasapainoa tulisi kehittää.

Tutkimuksen perusteella tiedon salaisuus ja taloudellinen arvo liittyvät yleensä datakokonaisuuksiin, yhdistelmiin ja tiedon rakenteeseen, kun taas yksittäinen raakadata harvoin täyttää liikesalaisuuden määritelmää. IoT-ympäristössä salaisuuden säilyttäminen on haastavaa verkottuneisuuden ja laajan tiedon jakamisen vuoksi, mikä vaikeuttaa kohtuullisten suojaustoimenpiteiden arviointia.

Datasäädöksen soveltamisessa on varmistettava, ettei liikesalaisuuksia käytetä perusteettomasti datan jakamisen tai uudelleenkäytön estämiseen. Datan haltijan mahdollisuutta pidättäytyä tai keskeyttää datan jakaminen on tulkittava rajoittavasti. Datan jakamisesta kieltäytymisen tulisi olla mahdollista vain, jos se koskee erittäin arvokkaita liikesalaisuuksia, joiden paljastaminen vaarantaisi tiedon haltijan liiketoimintaedellytykset. Liikesalaisuussuojan käytännön soveltamisessa painopisteen tulisi siirtyä entistä enemmän datan saatavuuden parantamiseen yhteiskunnan eduksi. Datasäädös on askel kohti oikeudenmukaisempaa tasapainoa liikesalaisuuden haltijan ja yhteiskunnan etujen välillä.

Avainsanat: datasäädös, liikesalaisuussuoja, liikesalaisuuden määritelmä, liikesalaisuussuojan kriittinen tarkastelu, esineiden internet, B2B ja B2C datan jakaminen

x Tutkielma ei sisällä muita kuin tekijän/tekijöiden omia henkilötietoja.

SISÄLLYS	
LÄHTEET	V
LYHENTEET	XV
1. JOHDANTO	1
1.1 Taustaa	1
1.2 Tutkimuskysymykset ja tutkielman rakenne	4
1.3 Aiheen rajaus ja datasäädöksen suhde immateriaalioikeuksiin	6
2. DATASÄÄDÖS	10
2.1 Taustalla EU:n datastrategia	10
2.2 Tavoitteet	12
2.3 Soveltamisalaan kuuluva data	12
2.4 Keskeiset uudistukset	15
2.5 Datasäädöksen haasteet liikesalaisuussuojan kannalta	18
2.5.1 Riski liikesalaisuussuojan heikentymisestä	18
2.5.2 Liikesalaisuussuoja esteenä asetuksen tehokkaalle soveltamiselle	21
3. LIIKESALAISSUUSÄÄNTELYN PERUSTEET JA SOVELTUMINEN IOT- DATAAN	23
3.1 Liikesalaisuussuojan perusteet	23
3.1.1 Suojan kohde, luonne ja soveltamisala	23
3.1.2 Tavoitteet (liikesalaisuuksien ”dilemma”)	25
3.2 Liikesalaisuuden määritelmä ja soveltuminen (IoT-) dataan	27
3.2.1 Datan soveltuminen liikesalaisuudeksi yleistä	27
3.2.2 Tiedon salaisuus	30
3.2.3 Tiedon taloudellinen arvo	33
3.2.4 Kohtuulliset toimenpiteet tiedon salassa pitämiseksi	37
3.2.5 Liikesalaisuuksien yksilöinti	39
3.3 Liikesalaisuuden haltijan määrittäminen datataloudessa	42
3.4 Eräitä kriittisiä näkökulmia liikesalaisuuksien suojaan	44
3.4.1 Tasapaino datan haltijan edun ja dataan pääsyyn välillä	44
3.4.2 Liikesalaisuussuojan oikeutus	46
4. LIIKESALAISSUUSUOJAN TULKINTA DATASÄÄDÖKSESSÄ	49
4.1 Sallitut datan käyttötarkoitukset suhteessa eri tahoihin	49
4.1.1 Käyttäjä	49
4.1.2 Kolmas osapuoli	50
4.1.3 Toinen kolmas osapuoli	51

4.1.4 Datan haltija	52
4.2 Kielletyt datan käyttötarkoitukset	52
4.2.1 Kilpaileva tuote	52
4.2.2 Datan analysoinnin rajoitukset ja käänteismallinnuksesta sopiminen	54
4.3 Toimenpiteet liikesalaisuuksien suojaamiseksi	58
4.3.1 Oikeasuhteisista toimenpiteistä sopiminen	58
4.3.2 Tekniset ja organisatoriset toimenpiteet datan suojaamisessa	60
4.4 “Liikesalaisuuksien käsijarru”-mekanismi	63
4.4.1 Oikeus pidättäytyä tai keskeyttää datan jakaminen.....	63
4.6.2 Oikeus kieltäytyä datan jakamisesta	64
4.5 Datan luvaton käyttö ja luovuttaminen	66
5. JOHTOPÄÄTÖKSET	70

LÄHTEET

Kirjallisuus

Alemanno, Alberto: Towards a European Strategy on Business-To-Government Data Sharing for the Public Interest. Final report prepared by the High-Level Expert Group on Business-to-Government Data Sharing European Commission, HEC Paris Research Paper No. LAW-2020-1394, 2020.

Aplin, Tanya: The Data Act and Trade Secrets: An Experiment in Compulsory Licensing, teoksessa Sattler, Andreas & Zech, Herbert (toim.), The EU Data Act: First Assessments, s. 85–103, Weizenbaum Institute for the Networked Society, Humboldt University of Berlin, 2024.

Aplin, Tanya F.: A Critical Evaluation of the Proposed EU Trade Secrets Directive. King's College London Law School Research Paper No. 2014-25, 2014.

Aplin, Tanya – Radauer, Alfred – Bader, Markus A. et al.: The Role of EU Trade Secrets Law in the Data Economy: An Empirical Analysis. IIC, Vol. 54, 2023, s. 826–858.

Aplin, Tanya F.: The Limits of EU Trade Secret Protection. Teoksessa S. Sandeen, C. Rademacher ja A. Ohly (toim.), Research Handbook on Information Law and Governance. Edward Elgar, tulossa. King's College London Law School Research Paper No. 2021/3, 2020.

Atkinson, Robert D.: IP Protection in the Data Economy: Getting the Balance Right on 13 Critical Issues," SSRN, 2019.

Atik, Can: Data Act: Legal Implications for the Digital Agriculture Sector. Tilburg Law School Research Paper 2022.

Aracı, Gözde, A Quest for Fair Balance: Testing the Right of Access against IP Rights and Trade Secrets. MIPLC Master Thesis Series (2018/19). 2019.

Ballardini, Rosa Maria – Kaisto, Janne – Similä, Jukka: Developing Novel Property Concepts in Private Law to Foster the Circular Economy. Journal of Cleaner Production, Vol. 279, 2021.

Banterle, Francesco: Data Ownership in the Data Economy: A European Dilemma, in EU Internet Law in the Digital Era Springer, 2018.

Botero Arcila, Beatriz – Groza, Teodora: The New Law of the European Data Market: Demystifying the European Data Strategy. 2023.

Bone, Robert G.: The (Still) Shaky Foundations of Trade Secret Law Texas Law Review, 2014, U of Texas Law, Public Law Research Paper No. 563, 2014.

Burri, Mira – Meitingner, Ingo: The Protection of Undisclosed Information: Commentary of Article 39 TRIPS. Teoksessa Thomas Cottier ja Pierre Véron (toim.), Concise International and European IP Law: TRIPS, Paris Convention, European Enforcement and Transfer of Technology. Kluwer Law International, 2014.

Bräutigam, Tobias – Cunningham, Francine – Aholainen, Maria – Geus, Marjolein – Kukorelli, Floora: EU Regulation Builds a Fairer Data Economy: Working Paper, Bird & Bird, 2022.

De Noyette, Ella – Stähler, Leander - Margoni, Thomas: Data Secrets: The Data Act's new trade secrets framework. SSRN. Draft 0.2 – preprint. 2024.

- Determann, Lothar: No One Owns Data. UC Hastings Research Paper No. 265, 2018.
- De Werra, Jacques: Patents and Trade Secrets in the Internet Age. 1.9.2015.
- De Noyette, Ella - Margon, Thomas: Luku 15. The Data Act and the 2016 Trade Secrets Directive. Teoksessa: CiTiP Working Paper Series White Paper on the Data Act Proposal. Ducuing, Charlotte – Margoni, Thomas – Schirru, Luka (toim.). 2022.
- Drexl, Josef: Data Access and Control in the Era of Connected Devices - Study on Behalf of the European Consumer Organisation BEUC, BEUC, Bryssel 2018.
- Drexl, Josef – Banda, Carolina – Gonzalez Otero, Begoña – Hoffmann, Jörg – Kim, Daria – Kulhari, Shraddha – Moscon, Valentina – Richter, Heiko – Wiedemann, Klaus: Position Statement of the Max Planck Institute for Innovation and Competition, 2022.
- Drexl, Josef: Between Propertisation and Access. Max Planck Institute for Innovation & Competition Research Paper No. 16–13, 2016.
- Drexl, Josef: Designing Competitive Markets for Industrial Data – Between Propertisation and Access. JIPITEC, Vol. 8, 2017. s. 257–292.
- Drexl, Josef and Banda, Carolina and Gonzalez Otero, Begoña and Hoffmann, Jörg and Kim, Daria and Kulhari, Shraddha and Moscon, Valentina and Richter, Heiko and Wiedemann, Klaus, Position Statement of the Max Planck Institute for Innovation and Competition of 25 May 2022 on the Commission's Proposal of 23 February 2022 for a Regulation on Harmonised Rules on Fair Access to and Use of Data (Data Act).Max Planck Institute for Innovation & Competition Research Paper No. 22-05, 2022.
- Dreyfuss, Rochelle Cooper: Trade Secrets and Deep Secrets. NYU Law and Economics Research Paper No. 24-37, NYU School of Law, Public Law Research Paper No. 24–40.2024. Teoksessa Research Handbook on Unfair Competition and Passing Off (Graeme B. Dinwoodie ja Ansgar Ohly, toim.). Edward Elgar Publishing.
- Ducuing, Charlotte: An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses, 2022.
- Eckardt, Martina – Kerber, Wolfgang: Property Rights Theory, Bundles of Rights on IoT Data, and the EU Data Act. European Journal of Law and Economics, Vol. 57, Nr. 1-2, s. 113–143, Special Issue: The Law and Economics of the Data Economy, toim. Thomas Eger ja Marc Scheufen, 2023.
- Ettredge, Michael, Guo, Feng, and Li, Yijun: Trade secrets and cyber security breaches. Journal of Accounting and Public Policy, Volume 37, Issue 6, 2018, s. 564–585.
- Farkas, Thomas: Data Created by the Internet of Things: The New Gold Without Ownership? revista la propiedad inmaterial, No. 23, Enero–Junio 2017.
- Fia, Tommaso: An Alternative to Data Ownership: Managing Access to Non-Personal Data through the Commons. Global Jurist, 2020.
- Fia, Tommaso: Resisting IP Overexpansion: The Case of Trade Secret Protection of Non-Personal Data. IIC, Vol. 53, 2022, s. 917–949.
- Geiregat, Simon: The Data Act: Start of a New Era for Data Ownership? 2022.
- Grafenstein, Maximilian: Reconciling Conflicting Interests in Data through Data Governance. An Analytical Framework (and a Brief Discussion of the Data Governance Act

Draft, the Data Act Draft, the AI Regulation Draft, as well as the GDPR), HIIG Discussion Paper Series No. 2022-02.

Graef, Inge – Husovec, Martin: Seven Things to Improve in the Data Act, SSRN, 2022.

Graf Ballestrem, Johannes, Harris, Tim - de le Court, Valentin - Trigg, Robyn: The EU Data Act: Data versus Trade Secrets, 295 managing intell. PROP. 22, 2022.

Graves, Tait – Macgillivray, Alexander: Combination Trade Secrets and the Logic of Intellectual Property. Santa Clara High Tech. L.J., Vol. 20, nro 2, 2004, s. 261–292.

Hauck, Ronny: Blockchain, Smart Contracts and Intellectual Property. Using Distributed Ledger Technology to Protect, License and Enforce Intellectual Property Rights. Legal Issues in the Digital Age, vol. 1, no. 1.03/2021, s. 17–41.

Hernandez Gonzalez, Lennin: Trade Secret Protection... in the Cloud. The Entertainment Law Review, 2013, s. 7–24.

Hennemann, Moritz, Ebner, Gordian, and Karsten, Benedikt: The Data Act Proposal – Literature Review and Critical Analysis - Part I (Art. 1-13, 35). University of Passau Institute for Law of the Digital Society Research Paper S, 2023.

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

Hull, John: Trade Secret Licensing: The Art of the Possible. Journal of Intellectual Property Law & Practice, Vol. 4, nro 3, 2009, s. 203–212.

Hynönen, Kalle – Leino, Saara – Bützow, Alexander: Euroopan datatalouden uudet säännöt: Tarkastelussa datasäädös ja tekoälyasetus, Defensor Legis 3/2023, s. 466–488.

Keltto, Tuomas: Vierashuoneessa Specialist Counsel Tuomas Keltto: EU:n datasäädös (EU Data Act) – uudet säännöt koskien datan käsittelyä, Edilex uutiset, 2024.

Kerber, Wolfgang: Governance of IoT Data: Why the EU Data Act will not Fulfill Its Objectives, GRUR International, 72(2), 2023, s. 120–135.

Kerber, Wolfgang: EU Data Act: Will New User Access and Sharing Rights on IoT Data Help Competition and Innovation?" Journal of Antitrust Enforcement, 2024.

Kim, Daria and Kwok, Man Wai: Data Usability as a Parameter of Rights and Obligations under the EU Data Act. Max Planck Institute for Innovation & Competition Research Paper No. 24-04, 2024.

Kim, Hye Jin; Rhee, Jung Soo: Utilizing an Enhanced Internet of Things to Prevent the Disclosure of Industrial Trade Secrets. Asia-Pacific Journal of Convergent Research Interchange, Vol. 10, No. 5, 2024, s. 87–94.

Krämer, Jan, Colangelo, Giuseppe, Richter, Heiko, and Schnurr, Daniel: Data Act: Towards a Balanced EU Data Regulation. Centre on Regulation in Europe (CERRE), March 2023.

Leistner, Matthias: The Existing European IP Rights System and the Data Economy – An Overview with Particular Focus on Data Access and Portability. Forthcoming, Josef Drexl (toim.), Data Access, Consumer Protection and Public Welfare (Verbraucherrechtstage 2019), Nomos 2020.

Leistner, Matthias and Antoine, Lucie, IPR and the Use of Open Data and Data Sharing Initiatives by Public and Private Actors. Study commissioned by the European Parliament's

Policy Department for Citizens' Rights and Constitutional Affairs at the request of the Committee on Legal Affairs 2022.

Leistner, Matthias: Towards an Access Paradigm in Innovation Law?, GRUR International, Volume 70, Issue 10, 2021, s. 925–931.

Lemley, M.: The Surprising Virtues of Treating Trade Secret as IP Rights. Stanford Law Review, 2008.

Leskinen, Minni: De lege ferenda -tutkimuksesta metodina ja tieteenä. Lakimies 7–8/2022, s. 1158–1185.

Martens, Bertin: Pro- and Anti-Competitive Provisions in the Proposed European Union Data Act, TILEC Discussion Paper No. 2023-03, 2023.

Mata, Melissa: Industrial Data and Trade Secrets: A Balanced Approach or an Excessive Mismatch? MIPLC Master Thesis Series 2017/18, 2018.

Margoni, Thomas and Strowel, Alain M.: Contractual Freedom and Fairness in EU Data Sharing Agreements. Forthcoming in de Werra & Calboli (toim.), Research Handbook on Intellectual Property Licensing 2.0, 2024.

Manzo, Valentina: The Internet of Things and Intellectual Property Rights: The Protection of Data. WIPO Academy, University of Turin and ITC-ILO - Master of Laws in IP - Research Papers Collection - 2017-2018, 2019.

Menell, Peter S. – Almeling, David – Cundiff, Victoria A. – Pooley, James – Rowe, Elizabeth A. – Toren, Peter J. – Wexler, Rebecca: Trade Secret Case Management Judicial Guide, 2023. Luvut: 4: Identification of Trade Secrets ja 2: Trade Secret Law Primer.

Moore, Taylor R.: Trade Secrets and Algorithms as Barriers to Social Justice. 2017.

Moscon, Valentina, Data Access Rules, Copyright and Protection of Technological Protection Measures in the EU. A Wave of Propertisation of Information. Max Planck Institute for Innovation & Competition Research Paper No. 23-14, 2023.

Mylly, Ulla-Maija: Trade Secrets and the Data Act. SpringerLink, 06 March 2024, Volume 55, s. 368–393.

Mylly, Ulla-Maija: Proportionality of Trade Secret Remedies in European Union – In Comparison with Patent Law Enforcement, IIC 53, 2022, s. 1444–1476.

Määttä, Tapio – Tolvanen, Matti – Väättä, Ulla – Kolehmainen, Antti – Myrsky, Matti – Keinänen, Anssi: Oikeudellisen ajattelun perusteita. Oikeustieteiden pääsykoekirja 2012. University of Eastern Finland Oikeustieteiden laitos. Joensuu 2012.

Nordberg, Ana: Trade Secrets, Big Data and Artificial Intelligence Innovation: A Legal Oxymoron? Teoksessa Jens Schovsbo, Timo Minssen, Thomas Riis (toim.): The Harmonization and Protection of Trade Secrets in the EU: An Appraisal of the EU Directive (Edward Elgar, 2020), s. 192–218.

Noto La Diega, Guido: Ending Smart Data Enclosures: The European Approach to the Regulation of the Internet of Things between Access and Intellectual Property. Teoksessa Stacy-Ann Elvy ja Nancy Kim (toim.), The Cambridge Handbook on Emerging Issues at the Intersection of Commercial Law and Technology, 2022.

Noto La Diega, Guido – Sappa, Cristiana: The Internet of Things at the Intersection of Data Protection and Trade Secrets. Non-Conventional Paths to Counter Data Appropriation and Empower Consumers, (2020) 3 *Revue européenne de droit de la consommation* / *European Journal of Consumer Law*, s. 419–458.

Oesch, Rainer: *Lisenssisopimusoikeuden perusteet*, Otavan Kirjapaino Oy, Keuruu 2024.

Picht, Peter Georg: Caught in the Acts: Framing Mandatory Data Access Transactions under the Data Act, Further EU Digital Regulation Acts, and Competition Law. Max Planck Institute for Innovation and Competition Research Paper No. 22-12, 2022.

Pihlajarinne, Taina – Ballardini, Rosa Maria. Chapter 9. Owning Data via Intellectual Property Rights: Reality or Chimera? *Lapin yliopiston tutkimusportaali* 2019.

Risch, Michael: Trade Secret Law and Information Development Incentives. Teoksessa Rochelle C. Dreyfuss, Katherine J. Strandburg (toim.), *The Law and Theory of Trade Secrecy: A Handbook of Contemporary Research*. Edward Elgar Publishing 2010.

Radauer, Alfred – Bader, Martin – Aplin, Tanya – Konopka, Ute, Searle, Nicola – Altenburger: Study on the legal protection of trade secrets in the context of the data economy: final report. Publications Office of the European Union, 2022.

Rowe, Elizabeth A.: Contributory Negligence, Technology, and Trade Secrets. University of Florida Levin College of Law Research Paper No. 2008-06, 2009.

Sappa, Cristiana: How Data Protection Fits with the Algorithmic Society via Two Intellectual Property Rights – A Comparative Analysis. *Journal of Intellectual Property Law & Practice*, Vol. 14, Issue 5, 2019, s. 407–418.

Sappa, Cristiana: What Does Trade Secrecy Have to Do with the Interconnection-Based Paradigm of the Internet of Things? *European Intellectual Property Review*, Vol. 40, nro 8, 2018, s. 518–523.

Sandeen, Sharon K. – Aplin, Tanya F.: Trade Secrecy, Factual Secrecy and the Hype Surrounding AI. Teoksessa Ryan Abbott (toim.), *Research Handbook on Intellectual Property and Artificial Intelligence*. Edward Elgar, 2021.

Schiller, Eryk, Aidoo, Andy, Fuhrer, Jara, Stahl, Jonathan, Ziörjen, Michael, and Stiller, Burkhard: Landscape of IoT security. *Computer Science Review*, Volume 44, 2022.

Schovsbo, Jens: The directive on trade secrets and its background. Teoksessa *The Harmonization and Protection of Trade Secrets in the EU*, toim. Jens Schovsbo, Timo Minssen ja Thomas Riis, s. 7–21. Edward Elgar Publishing 2020.

Searle, Nicola: The Economic and Innovation Impacts of Trade Secrets. UK Intellectual Property Office Research Paper No. 2021/01, 2021.

Siltala, Raimo: *Oikeustieteen tieteenteoria*. Suomalainen lakimiesyhdistys. Vammala 2013.

Sousa e Silva, Nuno: What Exactly is a Trade Secret Under the Proposed Directive? *Journal of Intellectual Property Law & Practice*, Vol. 9, nro 11, 2014, s. 923–932.

Thomas, Lord John – Wendehorst, Christiane – Schwamberger, Sebastian: Response to the Public Consultation on 'A European Strategy for Data' COM(2020) 66 Final, 2020.

Vapaavuori, Tom: *Liikesalaisuudet ja salassapitosopimukset*. 3., uudistettu painos. Alma Talent. Helsinki 2019.

Wiebe, Andreas: Protection of Industrial Data – A New Property Right for the Digital Economy? *Journal of Intellectual Property Law & Practice*, Vol. 12, nro 1, 2017, s. 62–71.

Wiebe, Andreas – Schur, Nico: Protection of trade secrets in a data-driven, networked environment – Is the update already out-dated? *Journal of Intellectual Property Law & Practice*, Volume 14, Issue 10, 2019, s. 814–821.

Wiedemann, Nils and Leicht, Maximilian: *Supply Chain Data Sharing: Evaluating Challenges and Opportunities of EU Data Law*, 2023.

World Intellectual Property Organization (WIPO): *WIPO Guide to Trade Secrets and Innovation*, Geneva, 2024, DOI: 10.34667/tind.49735.

Zech, Herbert: Data Access Rights as Property Rights, teoksessa Sattler, Andreas & Zech, Herbert (toim.), *The EU Data Act: First Assessments*, s. 51–67, Weizenbaum Institute for the Networked Society, Humboldt University of Berlin, 2024.

Zech, Herbert: A Legal Framework for a Data Economy in the European Digital Single Market: Rights to Use Data. *Journal of Intellectual Property Law & Practice*, Vol. 11, 2016, s. 460–470.

Zech, Herbert: Data as a Tradeable Commodity – Implications for Contract Law. Teoksessa Josef Drexl (toim.), *Proceedings of the 18th EIPIN Congress: The New Data Economy between Data Ownership, Privacy and Safeguarding Competition*. Edward Elgar Publishing, 2017.

Virallislähteet

Hallituksen esitykset

HE 114/1978 vp. Hallituksen esitys eduskunnalle 1)laeiksi sopimattomasta menettelystä elinkeinotoiminnassa ja 2)markkinatuomioistuimesta annetun lain muuttamisesta.

HE 49/2018 vp. Hallituksen esitys eduskunnalle liikesalaisuuslaiksi ja eräiksi siihen liittyviksi laeiksi.

Muut kansalliset virallislähteet

Elinkeinoelämän tutkimuslaitos: Datasäädös – tietopohja markkinoista Suomessa. ETLA Julkaisut, Raportit 148, 2024. Viitattu 4.1.2025. Koski, Heli – Pajarinen, Mika (tekijät) <https://www.etla.fi/julkaisut/raportit/datasaadoks-tietopohja-markkinoista-suomessa/>. (ETLA 2024)

Liikenne- ja viestintäministeriö (LVM): Hallituksen esitys EU:n datasäädöksen täytäntöönpanoa koskevaksi lainsäädännöksi lausunnoille. 20.12.2024. Viitattu: <https://valtioneuvosto.fi/-/1410829/hallituksen-esitys-eu-n-datasaadoksen-taytantoonpanoa-koskevaksi-lainsaadannoksi-lausunnoille> (LVM 2024)

U 29/2022 vp Valtioneuvoston kirjelmä eduskunnalle komission ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös)

Euroopan unioni

Euroopan parlamentti, European Parliamentary Research Service (EPRS): BRIEFING EU Legislation in Progress. The data act. 03/2023. Saatavilla: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI\(2022\)733681_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733681/EPRS_BRI(2022)733681_EN.pdf) (EPRS 2023)

European Union Intellectual Property Office: Trade Secrets Litigation Trends in the EU. 2023. Saatavilla: <https://www.euipo.europa.eu/fi/publications/trade-secrets-litigation-trends-in-the-eu> (EUIPO 2023)

Euroopan unionin neuvosto: Ehdotus Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös). 2022/0047(COD). Saatavilla: <https://data.consilium.europa.eu/doc/document/ST-7413-2023-INIT/en/pdf> (Neuvosto 2023)

Euroopan unionin neuvosto: Council of the European Union, Regulatory Scrutiny Board Opinion - Data Act, SEC(2022) 81 final, 2022. Viitattu 3.1.2025. Saatavilla: <https://op.europa.eu/fi/publication-detail/-/publication/8f3ef878-9663-11ec-b4e4-01aa75ed71a1> (EU:n Neuvosto 2022)

European Data Protection Board: Data protection guide for small business. Secure personal data. Viitattu 10.1.2025. Saatavilla: https://www.edpb.europa.eu/sme-data-protection-guide/secure-personal-data_en#toc-2 (EDPB)

Komissio: Frequently Asked Questions: Data Act. Versio 1.1, 13.9.2024. Saatavilla: <https://digital-strategy.ec.europa.eu/en/library/commission-publishes-frequently-asked-questions-about-data-act>. (Komissio 2024)

Komissio: Commission staff working document - Impact assessment report. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). SWD/2022/34 final. (Komissio 2022a).

Komissio: Final report - sector inquiry into consumer Internet of Things. COM(2022) 19 final, 20.1.2022. Saatavilla: https://competition-policy.ec.europa.eu/document/download/c74fd54d-7cbb-41c5-aad5-0175be7b8a99_en. (Komissio 2022b)

Komissio: Ajoneuvon datan, toimintojen ja resurssien saatavuus. Viitattu 3.1.2025. Saatavilla: https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/13180-Ajoneuvon-datan-toimintojen-ja-resurssien-saatavuus_fi. (Komissio 2022c)

Komissio: Ehdotus Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös). 23.2.2022. COM(2022) 68 final 2022/0047(COD). {SEC(2022) 81 final} - {SWD(2022) 34 final} - {SWD(2022) 35 final}. (Komissio 2022d)

Komissio: Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Euroopan datastrategia COM/2020/66 final. (Komissio 2020a)

Komissio: Komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Kaikki irti EU:n innovointipotentiaalista – Teollis- ja tekijänoikeuksia koskeva toimintasuunnitelma EU:n elpymisen ja palautumiskyvyn tueksi. COM/2020/760 final. (Komissio 2020b)

Komissio: Directorate-General for Communications Networks, Content and Technology, Scaria, E., Berghmans, A., Pont, M., Arnaut, C. et al., Study on data sharing between companies in Europe – Final report, Publications Office, 2018, <https://data.europa.eu/doi/10.2759/354943> (Komissio 2018)

Komissio: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Building a European Data Economy (COM(2017) 9 final). 10.1.2017. {SWD(2017) 2 final}. (Komissio 2017a)

Komissio: Commission Staff Working Document: On the free flow of data and emerging issues of the European data economy, accompanying the document Communication: Building a European Data Economy (COM(2017) 9 final). 10.1.2017. {SWD(2017) 2 final}. (Komissio 2017b)

Komissio: Directorate-General for Communications Networks, Content and Technology, Legal study on ownership and access to data – Final report, Publications Office, 2016, <https://data.europa.eu/doi/10.2759/299944V> (Komissio 2016)

Komissio: Public Consultation on the Data Act and amended rules on the legal protection of databases: Summary Report. Consultation results. 2021. (Komissio 2021)

YK

YK: Our Common Agenda: Policy Brief 5 – A Global Digital Compact: An Open, Free and Secure Digital Future for All. 2023. Saatavilla <https://indonesia.un.org/sites/default/files/2023-07/our-common-agenda-policy-brief-gobal-digi-compact-en.pdf> (YK 2024a)

YK: Global Digital Compact. A/79/L.2. 2024. Saatavilla: https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf (YK 2024b)

Oikeustapakset

Markkinaoikeus (MaO)

MAO 398/20

MAO 232/2023

MAO H71/2022

Korkein oikeus (KKO)

KKO 2013:17

EU-tuomioistuin

Asia C-490/14 Freistaat Bayern v. Verlag Esterbauer GmbH. 29.11.2015. ECLI:EU:C:2015:735.

Asia C-355/12, Nintendo v. PC-Box. 23.1.2014. ECLI:EU:C:2014:25.

Euroopan unionin yleinen tuomioistuin

Asia T-235/15 Pari Pharma GmbH v. Euroopan lääkevirasto (EMA). 5.2.2018.
ECLI:EU:T:2018:65.

Asia T-201/04 Microsoft Corp v Commission of the European Communities. 17.9.2007.
ECLI:EU:T:2007:289.

Muut lähteet

Association of the Electrical and Digital Industry (ZVEI): ZVEI key recommendations on the Data Act's Trilogue negotiations. 16.6.2023. Saatavilla:

https://www.zvei.org/fileadmin/user_upload/Presse_und_Medien/Publikationen/2023/Juni/Data_Act/2023-06-16_ZVEI_recommendations_on_Trilogue_negotiations.pdf

Barrowman, Nick (2018). Why data is never raw: On the seductive myth of information free of human judgment. The New Atlantis, Summer/Fall 2018.

Bird & Bird: Why IP lawyers need to pay attention to the EU's draft Data Act. 2022. Bond, Toby – Stephens, Katharine (tekijät). Saatavilla:

<https://www.twobirds.com/en/insights/2022/uk/why-ip-lawyers-need-to-pay-attention-to-the-eus-draft-data-act> (Bird & Bird 2022)

Business Europe & Orgalim: Underestimating the Data Act's impact on trade secrets' protection will undermine European industrial competitiveness. 17.1.2023. Joint statement. Saatavilla:

https://www.businesseurope.eu/sites/buseur/files/media/position_papers/internal_market/2023-01-07_joint-policy_statement_be_orgalim_on_data_act_and_trade_secrets.pdf (Business Europe & Orgalim 2023)

Datanami: Global DataSphere to Hit 175 Zettabytes by 2025, IDC Says. Woodie, Alex (kirjoittaja). 27.11.2018. Verkkosivu. Saatavilla:

<https://www.datanami.com/2018/11/27/global-datasphere-to-hit-175-zettabytes-by-2025-idc-says/>.

Euroopan unionin neuvosto: Eurooppalainen terveysdata-avaruus: neuvostolta uusi asetus sähköisten terveystietojen rajatylittävän saatavuuden parantamiseksi EU:ssa. 21.1.2025.

Saatavilla: <https://www.consilium.europa.eu/fi/press/press-releases/2025/01/21/european-health-data-space-council-adopts-new-regulation-improving-cross-border-access-to-eu-health-data/> (EU:n neuvosto 2025)

Forbes: 175 Zettabytes By 2025. Coughlin, Thomas (kirjoittaja). 27.11.2018. Viitattu

4.1.2025. <https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/>

Freshfields: The Data Act and the EU's Digital Agenda – striking a balance in trade secret protection? 14.11.2023. Viitattu 10.1.2025. Saatavilla:

<https://technologyquotient.freshfields.com/post/102isit/the-data-act-and-the-eus-digital-agenda-striking-a-balance-in-trade-secret-pro>

Gartner: What Edge Computing Means for Infrastructure and Operations Leaders. Van der Meulen, Rob (kirjoittaja). 3.10.2018. Verkkosivu. Viitattu 4.1.2025.

<https://www.gartner.com/smarterwithgartner/what-edge-computing-means-for-infrastructure-and-operations-leaders>

Hannes & Snellman: The Data Act and Trade Secrets – Part II: Refusing Access to Data Under the Data Act Based on Trade Secret Protection. Vaaraniemi, Liisa – Schröder, Vilhelm (tekijät). Blogi, 11.1.2024. Saatavilla: <https://www.hannessnellman.com/news-views/blog/the-data-act-and-trade-secrets-part-ii-refusing-access-to-data-under-the-data-act-based-on-trade-secret-protection/> (Hannes & Snellman 2024)

Hannes & Snellman: The Data Act and Trade Secrets. Schröder, Vilhelm (tekijä). Blogi, 7.9.2023. Saatavilla: <https://www.hannessnellman.com/news-views/blog/the-data-act-and-trade-secrets/> (Hannes & Snellman 2023)

Home Appliance Europe (APPLIA): Data Act's trade secrets protection woes risk crippling EU industry. Lavoro, Federica (tekijä). 8.3.2023. Saatavilla: <https://www.applia-europe.eu/press-releases-applia/data-acts-trade-secrets-protection-woes-risk-crippling-eu-industry>

IPR University Center: Tuotetiedot, immateriaalioikeudet ja EU:n datasäädös (EU Data Act). Keltto, Tuomas (kirjoittaja). 06/2023. 8.11.2023 (Keltto 2023)

The International Road Transport Union (IRU): Position on the Data Act proposal. 3.6.2022. Saatavilla: <https://www.iru.org/resources/iru-library/european-commissions-proposal-regulation-harmonised-rules-fair-access-and-use-data> (IRU 2022)

Networkworld: Just one autonomous car will use 4,000 GB of data/day. Nelson, Patrick (kirjoittaja). 7.12.2016. Verkkosivu. Viitattu 4.1.2025. <https://www.networkworld.com/article/958319/one-autonomous-car-will-use-4000-gb-of-dataday.html>

Reinsel, David., Gantz, J. & Rydning, John: The Digitization of the World: From Edge to Core. IDC White Paper 2018. Viitattu 4.1.2025. <https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf>

Toffaletti, Sebastiano: SMEs call on the EU to unleash innovation: protecting trade secrets is no excuse to water down the Data Act. European DIGITAL SME Alliance 2023. Saatavilla: <https://www.digitalsme.eu/smes-call-on-the-eu-to-unleash-innovation-protecting-trade-secrets-is-no-excuse-to-water-down-the-data-act/>

Luennot

IPR University Center & Hannes Snellman Attorneys Ltd: Data Act and Trade Secrets. Webinaari, Aholainen, Maria – Schröder, Vilhelm (luennoitsijat), 3.10.2024, klo 10.30–11.45. (IPR University 2024)

IPR University Center's Data -series Lost in Data Laws? – EU's Big Five and Beyond. The Data Act Proposal and its interaction with the Database Sui Generis Right. Data act, DA. Derclaye, Estelle (University of Nottingham). Helsinki 23.3.2023. (IPR University 2023a)

IPR University Center's Data -series Lost in Data Laws? – EU's Big Five and Beyond. Data Act: Selected topics. Contracts, trade secrets, interplay with GDPR Hynönen, Kalle (Krogerus). Helsinki 23.3.2023. (IPR University 2023b)

Krogeruksen Datakoulu: Data Act: Sopimukset ja liikesalaisuuksien suojaaminen. Hynönen, Kalle – Bützow, Alexander - Yli-Houhala, Aleksi. 3.4.2024. Webinaari. (Krogerus 2024)

LYHENTEET

BKT

Datasäädös

Bruttokansantuote

Euroopan parlamentin ja neuvoston asetus (EU) 2023/2854 datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta. 13.12.2023. EUVL L, 2023/2854, 22.12.2023.

Datanhallinta-asetus

Euroopan parlamentin ja neuvoston asetus (EU) 2022/868, eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta (ETA:n kannalta merkityksellinen teksti). 30.6.2022. EUVL L 152, 3.6.2022, p. 1–44.

Digimarkkinasäädös

Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925, kilpailullisista ja oikeudenmukaisista markkinoista digitaali-alalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta. 14.9.2022. EUVL L 265, 12.10.2022, p. 1–66.

Digipalvelusäädös

Euroopan parlamentin ja neuvoston asetus (EU) 2022/2065, digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta. 19.10.2022. EUVL L 277, 27.10.2022, p. 1–102.

EU

EU-tuomioistuin

IoT

Liikesalaisuusdirektiivi

Euroopan unioni

Euroopan unionin tuomioistuin

Internet of Things (esineiden internet)

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943 julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta. 08.06.2016. EUVL L 157, 15.6.2016, p. 1–18.

Liikesalaisuuslaki (10.8.2018/595).

Markkinaoikeus

Patenttilaki (15.12.1967/550).

Sopimus Euroopan unionin toiminnasta

Tekijänoikeuslaki (8.7.1961/404).

Euroopan parlamentin ja neuvoston asetus (EU) 2024/1689, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä

LSL

MAO

Patenttilaki

SEUT

Tekijänoikeuslaki

Tekoälysäädös

	direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta. 13.6.2024. EUVL L, 2024/1689, 12.7.2024.
Tietokantadirektiivi	Euroopan parlamentin ja neuvoston direktiivi 96/9/EY tietokantojen oikeudellisesta suojasta. 11.3.1996. EYVL L 77, 27.3.1996, p. 20–28.
Tietoyhteiskuntadirektiivi	Euroopan parlamentin ja neuvoston direktiivi 2001/29/EY, tekijänoikeuden ja lähioikeuksien tiettyjen piirteiden yhdenmukaistamisesta tietoyhteiskunnassa 22.5.2001. EYVL L 167, 22.6.2001, s. 10—19.
TRIPS	Agreement on Trade-Related Aspects of Intellectual Property Rights
WTO	Maailman kauppajärjestö
YK	Yhdistyneet Kansakunnat
Yleinen tietosuojasetus / GDPR	Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus). 27.4.2016. EUVL L 119, 4.5.2016, p. 1–88.

1. JOHDANTO

1.1 Taustaa

Arvioiden mukaan esineiden internetin (IoT, eng. *Internet of Things*) laitteet tulevat tuottamaan noin 90 zettatavua (ZB) dataa vuoteen 2025 mennessä. Tämä määrä on osa suurempaa datakokonaisuutta, jonka ennustetaan kasvavan maailmanlaajuisesti 175 ZB samana aikana.¹ Gartnerin ennusteen mukaan vuoteen 2025 mennessä jopa 75 % yritysten tuottamasta datasta syntyy ja käsitellään lähellä sen alkuperää, mihin vaikuttaa erityisesti esineiden internetin laitteiden yleistymisen. Reunalaskennalla (eng. *edge computing*) on yhä suurempi rooli, kun tietojen käsittely tapahtuu lähellä lähdettä tai käyttäjää.² Esimerkiksi älykkäät ajoneuvot voivat tuottaa jopa 4 000 gigatavua dataa päivittäin.³ Euroopan komissio on ennustanut, että esineiden internetin arvo ylittää 5–11 biljoonaa euroa vuoteen 2030 mennessä. Lisäksi komission mukaan datasääntelyn avulla on mahdollista saavuttaa jopa 270 miljardin euron BKT:n lisäkasvu EU:n laajuisesti vuoteen 2028 mennessä.⁴ IDC on ennustanut, että vuosina 2023–2026 investoidaan maailmanlaajuisesti eniten esineiden internetin sovelluksiin valmistus- ja prosessiteollisuudessa (noin 25 %)⁵. Teollisuus 4.0 viittaa neljänteen teolliseen vallankumoukseen, jossa tieto- ja viestintäteknologiat integroidaan osaksi valmistusprosesseja. Tässä kehityksessä merkittävä rooli on esineiden internetin innovaatioilla.⁶

Euroopan komission vuonna 2022 teettämässä kyselytutkimuksessa havaittiin, että suuri osa teollisesta datasta keskittyy alan isoille toimijoille, jotka estävät kolmansien osapuolien pääsyn dataan⁷. Teollisen IoT- datan heikko saatavuus johtuu valmistajien kyvystä pitää data salassa teknisillä ja oikeudellisilla keinoilla, kuten liikesalaisuuksien suojan avulla. Käytännössä valmistajat ovat pystyneet teknisen suunnittelun avulla saamaan *de facto* yksinoikeuden laitteiden tuottamaan dataan.⁸ Ne ovat luoneet valmistajille lähes omistusoikeuteen verrattavan

¹ Datanami 2018. Forbes 2018.

² Gartner 2018. Reunalaskennassa tietojenkäsittely tapahtuu lähellä datan lähdettä tai käyttäjää.

³ Networkworld 2016. Autonominen ajoneuvojen tuottama data liittyy erityisesti ajoneuvon sensoreihin, kuten tutkiin ja kameroihin, sekä sen ulkopuolelta keräämään tietoon, kuten karttoihin.

⁴ U 29/2022 vp, s. 12.

⁵ Reinsel – Gantz 2018, s. 3. Seuraavaksi eniten IoT-sovelluksiin investoidaan paikallishallinnossa (12 %) ja telekommunikaatioalalla (11,7 %).

⁶ Wiebe - Schur 2019, s. 814–815. Zech 2016, s. 7.

⁷ Komissio 2022b, kohdat 1,2 ja 43/s.2–44. Tutkimus koski pääasiassa virtuaaliassistentteja, kuten Google Assistant.

⁸ Eckardt - Kerber 2023, s. 1. Ks. myös Fia 2020, s. 6–7. Fia erottelee teknologiset, oikeudelliset ja valmistajien käyttäytymiseen liittyvät esteet.

vallan päättää datan jakamisesta, käytöstä ja kaupallistamisesta⁹. Tämä on herättänyt pohdintoja uudensääntelyn tarpeesta datan läpinäkyvyyden lisäämiseksi¹⁰.

Euroopassa tämä keskustelu on johtanut Euroopan parlamentin ja neuvoston asetuksen (EU) 2023/2854 datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta (datasäädös) säätämiseen ja voimaantuloon 11.1.2024. Datasäädöstä sovelletaan 12.9.2025 alkaen.¹¹ Datasäädös määrittelee, kuka saa käyttää, jakaa ja hyödyntää IoT-tuotteiden ja niihin liittyvien palveluiden tuottamaa ja keräämää dataa. Datasäädös antaa käyttäjälle oikeuden päästä verkkoon liitettyjen tuotteiden ja liitännäispalveluiden käytön seurauksena syntyvään dataan ja hallita sitä datan haltijoiden kanssa tehtävillä sopimuksilla. Käyttäjällä voi päättää datan jakamisesta valitsemilleen kolmansille osapuolille tai estää datan haltijan ja kolmannen osapuolen pääsyn dataan.¹² Asetuksessa ei luoda omistusoikeutta dataan, vaan säädetään sen hallinta- ja käyttöoikeudesta. Tämä on perusteltua, sillä omistusoikeuden määrittely datalle voisi aiheuttaa ongelmia, kuten monopoleiden syntymistä ja innovoinnin rajoittumista.¹³ Euroopan unioni (EU) on myös hylännyt mahdollisuuden myöntää datan haltijalle omistusoikeuden suuriin datakokonaisuuksiin (*ex novo* omistusoikeus)¹⁴.

Datasäädös kattaa datan jakamisen sekä yrityksiltä kuluttajille (B2C) että yrityksiltä yrityksille (B2B). -tapauksissa on kuitenkin perusteltua puhua B2C2B-mekanismista, sillä datan jakaminen kolmannelle osapuolelle tulee aina käyttäjän aloitteesta.¹⁵ Lisäksi datasäädös sisältää säännöksiä datan tarjoamisesta julkisen sektorin elimille, komissiolle, Euroopan keskuspankille ja muille EU:n elimille (B2G), mikäli se on tarpeen poikkeuksellisesti tai yleistä etua koskevan tehtävän suorittamiseksi¹⁶. Datasäädös on horisontaalisäädös eli sitä sovelletaan lähtökohtaisesti kaikkiin IoT-tuotteisiin ja liitännäispalveluihin alasta riippumatta.

⁹ Kerber 2024, s. 3.

¹⁰ Sappa 2019, s. 1–2.

¹¹ Datasäädös 50 artikla.

¹² Ducuing 2022, s. 6 ja 27–28. Kirjoittaja tarkastelee datasäädöstä omistusoikeuden näkökulmasta. Datasäädös ei luo perinteistä omistusoikeutta IoT -dataan, johon kuuluu se, että oikeudet ovat universaaleja (*in rem*) ja sovellettavissa kaikkia vastaan (*erga omnes*). Sen sijaan kyseessä on rajatumpi, henkilökohtaisempi oikeus (*ad personam*), jossa oikeudet ja velvollisuudet koskevat vain tiettyjä toimijoita ja tilanteita. Datasäädöksen sääntely muodostaa uudenlaisen omaisuusinstituution (property institution) antamalla käyttäjille oikeuden hallita dataansa, vaikka oikeudet ovatkin rajalliset.

¹³ Drexler 2018, s. 42–43. Farkas 2017, s. 14.

¹⁴ Tämä käy ilmi datasäädöksen johdannosta (25), jonka mukaa asetuksessa ei anneta datan haltijoille *uutta oikeutta* käyttää tuotteen tai siihen liittyvän palvelun dataa. Ks. myös Determann 2018, s. 1 ja 5. Oikeuskirjallisuudessa on keskusteltu omistusoikeuden myöntämisestä IoT-laitteista peräisin olevalle datalle. Omistusoikeuden myöntämistä ei ole kannatettu, koska yksinoikeuden luominen dataan voi olla julkisen edun vastaista ja aiheuttaa monimutkaisia oikeuksien jakamiseen liittyviä kysymyksiä

¹⁵ Arcila - Groza 2023 s. 25–27. Kerber 2024, s. 3–4.

¹⁶ Datasäädös johdanto (5). Datasäädös sääntelee myös vaihtoa datankäsittelypalveluiden välillä sekä asettaa vaatimuksia datan ja datan jakamismekanismien ja -palveluiden yhteentoimivuudelle.

Datasäädös on herättänyt huolta liikesalaisuuksien suojusta, koska jakovelvoitteisiin kuuluva data voi paljastaa luottamuksellisia tietoja, kuten liikesalaisuuksia. Datan haltijan ei voi lähtökohtaisesti kieltäytyä jakamasta dataa, joka sisältää liikesalaisuuksia.¹⁷ Asetuksen valmisteluvaiheessa liikesalaisuuksien suoja muodostui keskeiseksi kiistakysymykseksi. Lopullisessa asetuksessa kiinnitettiin huomattavasti enemmän huomiota liikesalaisuuksien suojaan kuin asetusehdotuksessa¹⁸. Muutoksilla pyrittiin sovittamaan paremmin yhteen datasäädöksen tavoitteet ja liikesalaisuuksien sekä immateriaalioikeuksien suoja¹⁹. Datan haltija voi ennen datan luovutusta vaatia käyttäjältä ja kolmannelta osapuolelta sopimusta, jossa he sitoutuvat säilyttämään tietojen luottamuksellisuuden ja ryhtyvät toimenpiteisiin niiden suojaamiseksi. Lisäksi asetuksessa sallitaan datan haltijalle mahdollisuus pidättäytyä, keskeyttää tai poikkeuksellisesti kieltäytyä datan jakamisesta tietyissä tilanteissa. Tätä kutsutaan "liikesalaisuuksien käsijarru" -mekanismiksi²⁰.

EU:ssa liikesalaisuussuoja perustuu Euroopan parlamentin ja neuvoston direktiiviin julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta ((EU) 2016/943, liikesalaisuusdirektiivi). Direktiivillä harmonisoitiin kansallinen sääntely EU:n jäsenvaltioissa. Direktiivi on täytäntöönpantu Suomessa liikesalaisuuslailla (595/2018, LSL). Vaikka datasäädös pyrkii tasapainottamaan datan jakamisen ja liikesalaisuuksien suojan välisiä ristiriitoja²¹, datasäädöksen ja liikesalaisuusdirektiivin välinen suhde ei ole täysin aukoton, vaan siihen liittyy tulkinnanvaraisuutta. Käytännössä datan haltijan voi olla haastavaa osoittaa, että datasäädöksen soveltamisalaan kuuluva data täyttää liikesalaisuuden kriteerit, sillä liikesalaisuuden määritelmä ja sen soveltaminen dataan ovat osin epäselviä²². Tulkintaongelmia aiheuttavat myös asetuksessa käytetyt käsitteet, kuten soveltamisalaan kuuluvan datan ja eri roolien, kuten datan haltijan, määrittely²³. Lisäksi keskeinen haaste on

¹⁷ Datasäädös johdanto (31).

¹⁸ EU Neuvosto 2022, s. 10. Komissio 2022d. Sääntelyntarkastuslautakunta arvioi asetusehdotusta ja antoi negatiivisen mielipiteen.

¹⁹ Komissio 2022d ja Neuvosto 2023. Datasäädösehdotuksessa 4 artiklan 3, 5 artiklan 8 ja 19 artiklan 3 kohdat edellyttivät, että liikesalaisuuksia sai ilmaista vain, jos ne oli suojattu erityistoimenpiteillä ja kun se oli "ehdottoman välttämätöntä" kolmansille osapuolille tai julkiselle sektorille. Datan haltijalla ei ollut oikeutta kieltäytyä datan jakamisesta liikesalaisuuksiin vedoten. Lopullisessa asetuksessa täsmennettiin liikesalaisuuksien suoja ja muutettiin riidanratkaisua koskevia artikloja, erityisesti immateriaalioikeuksien ja liikesalaisuuksien suojan osalta.

²⁰ Euroopan komissio 2024, s. 16. Datasäädös 4 artikla 6–8 kohdat. Datasäädös 5 artikla 9–11 kohdat.

²¹ Margoni – Strowel 2024, s. 7.

²² Aplin, Radauer ym. 2023, s. 835–836. Liikesalaisuuden määritelmän epäselvyys johtuu oikeuskäytännön puutteesta ja liikesalaisuusdirektiivin uutuudesta. Epäselvyydestä huolimatta liikesalaisuuden suojaan vedotaan usein. Myös Hynönen - Leino -Bützow 2023, s. 475–476. Keltto 2023. Graf Ballestrem – Harris – De le Court ym. 2022, s. 23.

²³ Hynönen - Leino -Bützow 2023, s. 487.

se, miten liikesalaisuudet voidaan yksilöidä datasta²⁴. Datasäädöksen valmistelussa päädyttiin siihen, ettei näistä epäselvyyksistä huolimatta ole toistaiseksi tarpeen tehdä muutoksia liikesalaisuusdirektiiviin²⁵. Näiden epäselvyyksien selkeyttäminen on tärkeää, jotta sääntelyn tavoitteet ja liikesalaisuuksien suoja voidaan sovittaa yhteen oikeudenmukaisella tavalla.

Suomessa on annettu datasäädöksen perustella hallituksen esitys kansalliseksi täytäntöönpanolaiksi, joka tulee selventämään kansallista sääntelyä muun muassa säätämällä toimivaltaisista viranomaisista²⁶. Suomessa datasäädöksen soveltamisalaan kuuluvien yritysten liikevaihto on arvioitu olevan 5,8–6,9 % BKT:stä, mikä korostaa säädöksen taloudellista merkitystä²⁷.

1.2 Tutkimuskysymykset ja tutkielman rakenne

Tässä tutkielmassa tarkastellaan EU:n datasäädöstä ja sen suhdetta liikesalaisuussuojaan. Lisäksi tarkastellaan liikesalaisuussuojan suhdetta dataan, erityisesti esineiden internetin sovellusten tuottamaan dataan. Datasäädöksen soveltamisalaan ja liikesalaisuuksien suojan kohteen välinen ristiriita herättää kysymyksiä käyttäjien tietojen saantia koskevien oikeuksien ja datan haltijoiden intressien yhteensovittamisesta. Tutkielman tavoitteena on siis selkeyttää datasäädöksen sääntelyä liikesalaisuuksien osalta ja arvioida, miten se vaikuttaa liikesalaisuuden määritelmään ja soveltamiseen IoT-tuotteiden ja niihin liittyvien palveluiden tuottamaan datan osalta. Erityisesti pyritään analysoimaan, miten datasäädöksessä on tasapainotettu datan jakaminen ja liikesalaisuuksien suoja. Lisäksi tutkielmassa arvioidaan kriittisesti, onko sääntelyssä annettu liiallista painoarvoa liikesalaisuussuojalle käyttäjien oikeuksien kustannuksella. Koska datasäädös ei ole vielä tuottanut oikeuskäytäntöä, tutkielma pyrkii antamaan mahdollisimman tarkan tulkinnan säädöksen liikesalaisuuksia koskevista artikloista ja selvittämään, mikä olisi oikea tulkinta tämänhetkisen tiedon valossa.

Tutkielman keskeiset tutkimuskysymykset ovat seuraavat:

1. Mitkä ovat liikesalaisuussuojan perusteet EU:ssa, ja miten ne liittyvät datasäädökseen?

1.1 Milloin esineiden internetin tuotteiden ja niihin liittyvien palveluiden data (IoT-data) muodostaa liikesalaisuuden?

2. Miten liikesalaisuussuojaa tulisi tulkita datasäädöksessä?

²⁴ Hynönen - Leino -Bützow 2023, s. 475. Vaaraniemi – Schröder 2024.

²⁵ Komissio 2020b.

²⁶ LVM 2024. Hallituksen esitysluonnos on lausunnoilla 31.1.2025 saakka.

²⁷ ETLA 2024.

Ensimmäinen tutkimuskysymys muodostaa tutkielman perustan ja selventää liikesalaisuussuojan keskeiset peruseriaatteen ja käsitteet EU:ssa. Tavoitteena on arvioida sitä, miten datasäädös kytkeytyy olemassa olevaan liikesalaisuuslainsäädäntöön. Ensimmäisen kysymyksen alakysymys on olennainen osa liikesalaisuuksien suojan tulkintaa, koska datan luokittelu liikesalaisuudeksi on edellytys datasäädöksen liikesalaisuuksien suojaa koskevien toimenpiteiden soveltamiselle. Näihin tutkimuskysymyksiin vastaaminen selventää ja lisää ymmärrystä siitä, millaiset periaatteet ja tavoitteet ovat liikesalaisuussuojan taustalla. Lisäksi se tuo esiin, millaisia vaatimuksia liikesalaisuussuojalle asetetaan EU:ssa sekä sen, miten liikesalaisuuksien suoja soveltuu nykyaikaisiin teknologioihin, erityisesti IoT-teknologian osalta. Toiseen tutkimuskysymykseen vastaamiseksi käsitellään datasäädöksen artikloja, jotka liittyvät liikesalaisuuksien suojaan. Tämä auttaa tunnistamaan mahdollisia tulkinnallisia aukkoja ja kehityskohteita sekä mahdollisesti tarjoaa suosituksia lainsäädännön soveltamiseen ja kehittämiseen.

Tutkielman rakenne koostuu viidestä pääluvusta. Luvussa 1 esitellään tutkielman tausta, tavoitteet, tutkimuskysymykset sekä rajaukset, rakenne ja metodit. Luvussa 2 käsitellään datasäädöksen tausta, tavoitteet, soveltamisalaan kuuluva data ja sen yhteys liikesalaisuuksiin sekä keskeiset syyt sille, miksi liikesalaisuuksien suoja nousi kiistakysymykseksi datasäädöksen valmisteluvaiheessa. Luvussa 3 tarkastellaan liikesalaisuussäätelyn perusteita, erityisesti sitä, milloin data muodostaa liikesalaisuuden. Lisäksi tarkastelen eräitä kriittisiä näkökulmia liikesalaisuussuojaan, kuten sen, että suoja on perinteisesti korostanut datan haltijan asemaa yhteiskunnan etuun nähden, ja miten tämä liittyy datasäädökseen. Luvussa 4 perehdytään datasäädöksen liikesalaisuuksia koskeviin artikloihin ja niiden tulkintaan. Yleisesti datasäädöksessä on säädetty keinoista, joilla datan haltija voi rajoittaa datan käyttöä ja jakamista. Ne voidaan jakaa viiteen ryhmään: 1) tuoteturvallisuusperuste²⁸, 2) henkilötietojen suoja²⁹, 3) yleiset käyttörajoitukset, kuten kilpailevan tuotteen kehittämisen kieltäminen ja datan analysoinnin rajoitukset³⁰, 4) Liikesalaisuuksien suojaaminen³¹ ja 5) luvaton datankäyttöä vastaan suojaavat toimet.³² Tutkielmassani perehdyn erityisesti liikesalaisuuksien

²⁸ Datasäädös 4 artikla 2 kohta: ”Käyttäjät ja datan haltijat voivat tehdä sopimuksen dataan pääsyn, sen käytön tai edelleen jakamisen rajoittamisesta tai kieltämisestä, jos tällainen käsittely voisi heikentää unionin oikeudessa tai kansallisessa lainsäädännössä säädettyjä verkkoon liitetyn tuotteen turvallisuusvaatimuksia ja aiheuttaa vakavia haittavaikutuksia luonnollisten henkilöiden terveydelle tai turvallisuudelle—”. Krogerus 2024. Tuoteturvallisuusperuste koskee pääasiassa raskaita liikennevälineitä, kuten lentokoneita ja raideliikennettä, sekä infrastruktuuriin liitettviä tuotteita.

²⁹ Datasäädös 4 artikla 12 kohta ja 5 artikla 7 kohta.

³⁰ Datasäädös 4 artikla 10 kohta ja 6 artikla 2 kohta e alakohta.

³¹ Datasäädös 4 artikla 6–9 kohdat ja 5 artikla 9–12 kohdat.

³² Datasäädös 11 artikla.

suojaamiseen, mutta käsittelen myös käyttörajoituksia ja luvattomalta datankäytöltä suojaavia toimia siltä osin, kun ne liittyvät liikesalaisuuksien suojaan. Luvussa 5 käydään läpi johtopäätökset ja pohdinta.

1.3 Aiheen rajausta ja datasäädöksen suhde immateriaalioikeuksiin

Jo datastrategiaa valmisteltaessa kiinnitettiin huomiota holistisen eli kokonaisvaltaisen näkökulman tärkeyteen. Sen mukaan datan saatavuuden lisäämistä ja datastrategian puitteissa tehtäviä toimenpiteitä tulisi tarkastella suhteessa eri oikeudellisiin intresseihin, kuten immateriaalioikeudet, henkilötietojen suoja, kilpailuoikeus, sui generis -tietokantasuoja ja liikesalaisuudet.³³ Liikesalaisuuksien suoja toimii yhtenä näkökulmana, jonka kautta datasäädöksen velvoitteita voidaan tarkastella.

Tässä tutkielmassa en käsittele tietosuojaan liittyviä kysymyksiä. EU:ssa henkilötietojen suoja perustuu EU:n yleiseen tietosuojasetukseen ((EU) 2016/679)³⁴. Datasäädös koskee dataa, joka sisältää henkilötietoja ja muuta kuin henkilötietoja sisältävää dataa. IoT-tuotteet ovat laajasti käytössä ja niillä on monia eri käyttötarkoituksia. Ne keräävät myös runsaasti dataa, jota voidaan hyödyntää luonnollisten henkilöiden tunnistamiseen. Asiaa monimutkaistaa se, että henkilötieto voi olla myös liikesalaisuus.³⁵ Liikesalaisuuksien suojaamiseen liittyy myös haaste, koska henkilötietojen ja ei-henkilötietojen erottaminen voi olla vaikeaa. Datasäädös koskee raakadataa, joka harvoin liittyy tunnistettavaan henkilöön. Kuitenkin suuret datamassat sisältävät todennäköisemmin myös henkilötietoja, jolloin rajanveto henkilötietojen ja muun datan välillä käy entistä vaikeammaksi.³⁶ Jos datasäädöksen velvoitteiden ja henkilötietojen sekä yksityisyyden suojan välillä ilmenee ristiriitaa, henkilötietojen ja yksityisyyden suoja asetetaan etusijalle³⁷.

Lisäksi kilpailu- ja sopimusoikeudellinen tarkastelu jää tämän tutkimuksen ulkopuolelle. Kilpailuoikeus voi rajoittaa datan jakamista kilpailijoiden välillä Euroopan unionin toiminnasta

³³ Thomas -Wendehorst – Schwamberger 2020, s. 9.

³⁴ Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuojasetus).

³⁵ Drexler 2021, s. 101. Noto La Diega – Sappa 2020, s. 452. IoT-laitte, kuten Amazon Echo tai Google Home keräämään dataa voi liittyä sekä henkilötietoja että liikesalaisuuksia, kuten algoritmeja tai muita liiketoimintatietoja. Liikesalaisuus voi olla esimerkiksi asiakaslista, joka sisältää tietoja käyttäjän käyttäytymisestä.

³⁶ Drexler 2018, s. 15–16.

³⁷ Datasäädös 1 artikla 5 kohta.

tehdyn sopimuksen (SEUT) 101 ja 102 mukaan³⁸. Lisäksi kilpailevan tuotteen olemassaolo ratkaistaan EU:n kilpailusääntöjen vakiintuneiden periaatteiden pohjalta³⁹. Sopimusoikeus on keskeinen tapa suojata liikesalaisuuksia. Datasäädös korostaa sopimusten merkitystä liikesalaisuuksien suojaamisessa, joten sopimusoikeudellisten näkökulmien avaaminen voi olla välttämätöntä.

Immateriaalioikeuksien osalta on syytä huomioda, että käyttäjien, kolmansien osapuolten, datan haltijan sekä, kun kyseessä on eri taho, liikesalaisuuden tai teollis- ja tekijänoikeuden haltijan oikeudet voivat olla keskenään ristiriidassa⁴⁰. Asetus ei muuta tai poista teollis- ja tekijänoikeuksia⁴¹. Poikkeuksena on tietokantojen suoja. Datasäädöksen 43 artiklan mukaan *sui generis* -oikeutta ei sovelleta tietokantoihin, joiden data saadaan verkkoon liitetystä tuotteesta tai siihen liittyvästä palvelusta tai tuotetaan sen avulla. Täten datan haltijat eivät voi vedota direktiivin 96/9/EY 7 artiklan mukaiseen *sui generis* -oikeuteen eivätkä näin ollen voi tehdä tyhjiksi datasäädöksen oikeuksia. Siten on mahdollista, että asetuksen soveltamisalaan kuuluvaa IoT-dataa suojataan *sui generis* -oikeudella, mutta tämä oikeus ei saa estää julkista sektoria saamasta tai jakamasta kyseistä dataa yleisessä hätätilanteessa.⁴² Siten datasäädös muuttaa tietokantadirektiivin soveltamisalaa.⁴³

Lisäksi datasäädös suojaa muita teollis- ja tekijänoikeuksia soveltamisalan rajauksella. Asetus ei sovellu dataan, joka johdetaan tai päätellään monimutkaisilla algoritmeilla, mukaan lukien ne, jotka ovat osa omisteista ohjelmistoa. Algoritmi voi esimerkiksi yhdistää useista verkkoon liitettyihin tuotteisiin kiinnitetyistä antureista saatua dataa.⁴⁴ Lisäksi teksti-, ääni- tai audiovisuaalisialtö, jota toistetaan IoT-laitteella, kuuluu usein teollis- ja tekijänoikeuksien piiriin. Asetuksen soveltamisalan ulkopuolelle on rajattu sellaiset verkkoon liitetyt tuotteet, joiden pääasiallinen toiminto on datan tallennus, käsittely tai siirto muun osapuolen kuin käyttäjän puolesta⁴⁵.

Tekijänoikeussuojan merkitys IoT-datan suojaamisessa on usein pieni, koska tekijänoikeus suojaa vain teoksia, jotka ovat syntyneet luovan prosessin tuloksena. Vaikka periaatteessa IoT-

³⁸ Datasäädös johdanto (116).

³⁹ Datasäädös johdanto (32).

⁴⁰ Geiregat 2022, s. 26.

⁴¹ Datasäädös johdanto (13). Datasäädös 1 artikla 2 kohta 8 alakohta. Asetuksella ei rajoiteta sellaisten unionin tai kansallisten säädösten soveltamista, joissa säädetään teollis- ja tekijänoikeuksien suojaamisesta.

⁴² Datasäädös johdanto (112) ja (71).

⁴³ IPR University 2023a, dia 15. Tietokantasuojan saaminen edellyttää huomattavaa panostusta eli investointeja tietokannan keräämisessä, varmistamisessa tai esittämisessä (TekL 49 §). Ennen datasäädöksestä esimerkiksi verkkoon liitetyn tuotteen antureiden avulla kerätty ja tuotettu data saattoi saada *sui generis* suojaa.

⁴⁴ Datasäädös johdanto (15). IPR University 2023a, dia 8. Ohjelmisto voi saada patentti- ja tekijänoikeussuojaa.

⁴⁵ Datasäädös 2 artikla 1 kohta 5 alakohta.

laitteiden tuottama datakokonaisuus voisi olla teos ja saada tekijänoikeudellista suojaa, datasäädöksen mukainen dataan pääsy on todennäköisemmin ristiriidassa tekijänoikeuden lähioikeuksien, kuten äänitetuottajien tai elokuvien ensimmäisten tallenteiden tuottajien oikeuksien kanssa⁴⁶. Lisäksi suuri määrä dataa voi muodostaa myös tekijänoikeuslain (404/1961, TekL) 5§:n mukaisen kokoomateoksen⁴⁷.

Tutkielman analyysi kohdistuu datasäädöksen II ja III lukuihin, joissa säädetään datan jakamisesta yrityksiltä käyttäjille ja yritysten välillä sekä datan haltijan velvoitteista. Näiden lukujen sääntely muodostaa asetuksen keskeisen sisällön⁴⁸. Lisäksi ne sisältävät liikesalaisuuksien kannalta keskeiset artikkelit. Tässä tutkielmassa ei käsitellä datan jakamista yrityksiltä julkiselle sektorille tai tietyille EU:n elimille⁴⁹. On myös huomioitava, että liikesalaisuussuoja ulottuu myös asetuksen muihin lukuihin, kuten VI lukuun, joka käsittelee datankäsittelypalveluiden vaihtamista sekä VII luvussa, jossa säädetään kolmannen maan viranomaisen pääsystä dataa sekä datan kansainvälisestä siirrosta.⁵⁰ Tutkielmassa ei kuitenkaan käsitellä näitä lukuja, vaan tarkastelu keskittyy ensisijaisesti datasäädöksen liikesalaisuusartiklojen tulkintaan, jotka koskevat IoT-datan jakamista yrityksiltä kuluttajille ja yritysten välisissä suhteissa.

1.4 Tutkimusmetodi

Tutkielmassa käytän metodina lainoppia eli oikeusdogmatiikkaa. Lainopin tutkimuskohde on voimassa oleva oikeus. Lainopin kaksi päätehtävää ovat tulkinta ja systematisointi. Lainopin avulla voidaan selvittää voimassa olevan oikeuden sisältö. Lainoppi tutkii oikeusnormeja käyttämällä oikeusnormilauseita ja sen tehtävänä on tulkinnan avulla selvittää oikeusnormit.⁵¹ Tulkintaa voidaan tehdä ensinnäkin säännöksen kielellisen ilmaisun perusteella. Muita tulkintaperusteita ovat systemaattinen tulkinta, historiallinen tulkinta eli lainsäädännön taustalla oleva tavoite ja tarkoitus, oikeuskäytännössä vakiintunut tulkinta, periaatepohjainen tulkinta sekä yhteiskunnallisten vaikutusten arviointi.⁵² tutkielmassa tulkitsen asetusta ensisijaisesti sen sanamuodon pohjalta. Lisäksi otan lainopillisessa tulkinnassa huomioon

⁴⁶ Geiregat 2022, s. 26. Ks. direktiivin 2001/29/EY 2 ja 3 artikkelit.

⁴⁷ Oesch 2024, s. 71.

⁴⁸ Drexl – Banda, Conzalez Otero ym. 2022, s. 8–9.

⁴⁹ Datasäädöksen V luku (B2G-sääntely) jää tarkastelun ulkopuolelle.

⁵⁰ Drexl – Banda - Gonzalez Otero ym. 2022, s.104–105. Esimerkiksi datasäädöksen 32 artikla velvoittaa pilvipalveluntarjoajat suojaamaan ei-henkilökohtaista dataa ja estämään luvattoman pääsyn tai tiedonsiirron, mikä voi tapahtua EU tai jäsenvaltioiden lakien, kuten liikesalaisuuksien suojan, rikkomisen seurauksena.

⁵¹ Hirvonen 2011, s. 22–24 ja s. 36–37. Oikeusnormi ilmenee tulkinnan tasolla eli se vaatii, että tulkitaan sitä, mikä on normin merkityssisältö. Oikeusnormilause on olemassa kielen tasolla, kuten laki teksti, ja se kertoo, mitä laki tai muu oikeuslähde kertoo.

⁵² Siltala 2003, s. 333–334.

asetuksen ja liikesalaisuusdirektiivin tarkoituksen, joka ilmenee muun muassa asetuksen johdannosta, asiantuntijoiden kannanotoista sekä mahdollisesti valmisteluaineistosta. Huomioin myös eri tulkintaratkaisujen yhteiskunnalliset vaikutukset, joissa vastakkain ovat datan haltijoiden liiketoimintaintressit sekä käyttäjien, kolmansien osapuolten ja julkisen sektorin oikeudet. Lainopin tehtävänä on myös tarkastella oikeudellisia ongelmia ja esittää niitä selkeämmin tai uudella tavalla sekä osoittaa, miten eri oikeudelliset käsitteet ja normit liittyvät toisiinsa⁵³. Tämä on olennaista tutkielmassani, jossa tarkastellaan liikesalaisuussuojan tekijöitä, jotka vaikuttavat datasäädöksen tulkintaan, sekä sitä, miten nämä säädökset täydentävät toisiaan.

Systematisointi tarkoittaa lakien, käsitteiden ja periaatteiden jäsentämistä johdonmukaisiksi kokonaisuuksiksi. Sen tehtävänä on järjestää voimassa oleva oikeus selkeäksi ja johdonmukaiseksi kokonaisuudeksi.⁵⁴ Tässä yhteydessä tarkastelen datasäädöksen ja liikesalaisuusdirektiivin välisiä yhteyksiä sekä suhteita. Lisäksi huomioin, miten datasäädöksen artikkelit liittyvät toisiinsa ja kuinka ne vaikuttavat liikesalaisuuden määritelmään ja sen suojaamiseen. Systematisointi auttaa ymmärtämään laajoja säädöskokonaisuuksia ja jäsentämään niitä.

Tutkielman pääpaino on voimassa olevan oikeuden tulkinta (de lege lata). Tutkielmaan sisältyy myös oikeuspoliittisia pohdintoja siitä, mitä oikeuden tulisi olla (de lege ferenda).⁵⁵ Tällöin on tarpeen arvioida, millaisen kokonaisuuden liikesalaisuuksia koskevat artikkelit muodostavat, jotta voisin ottaa kantaa esimerkiksi siihen, miten sääntelyn tasapainoa datan saatavuuden ja liikesalaisuuksien suojan välillä voitaisiin parantaa. Lisäksi tulee tulkita liikesalaisuussuoja perusteita, kuten tavoitteita ja suojan oikeutusta sekä niiden suhdetta datasäädökseen.

⁵³ Määttä 2012, s. 74.

⁵⁴ Hirvonen 2011, s. 25.

⁵⁵ Määttä 2012, s. 18. Leskinen 2022, s. 1162–1168. De lege ferenda -tutkimuksen tarkoitus on tuottaa suosituksia siitä, miten oikeustilaa tulisi kehittää ja muuttaa saatujen havaintojen nojalla. Muutosehdotusten esittäminen edellyttää sääntelyn lainopillista analysointia, joka liittyy sen oikeusdogmaattiseen tutkimusmetodiin.

2. DATASÄÄDÖS

2.1 Taustalla EU:n datastrategia

Datasäädös on osa Euroopan komission vuonna 2020 antaman datastrategian toimenpiteitä, joiden tavoitteena on tehdä EU:sta dynaamisin, turvallisin, houkuttelevin ja nopeasti reagoivin datatalous. Datastrategian tavoitteena on luoda yhteiseneurooppalainen data-avaruus eli todelliset datan sisämarkkinat. Data-avaruudessa on neljä pilaria, jotka ovat 1) hallintomalli datan saatavuuden ja käytön varmistamiseksi, 2) investoinnit infrastruktuureihin, standardeihin ja välineisiin, 3) osaamisen lisääminen ja 4) strategisten sektoreiden ja alojen tunnistaminen ja data-avaruuksien luominen.⁵⁶ Datasäädös kuuluu ensimmäiseen pilariin. Datasäädöksen tavoitteena on kannustaa datan jakamista eri alojen välillä.⁵⁷

Datan tehokas hyödyntäminen edistää tuottavuutta, parantaa kilpailukykyä sekä tukee terveyden, hyvinvoinnin ja ympäristön tilan parantamista sekä julkisten palveluiden laadun kehittämistä. Datastrategiassa pyritään monipuolisesti edistämään datataloutta ja lisäämään datapohjaisten tuotteiden ja palveluiden kysyntää sekä käyttöä EU:n sisämarkkinoilla. Parantunut datan saatavuus tuo hyötyjä koko yhteiskunnalle, mukaan lukien yrityksille, julkishallinnolle, kansalaisille ja tutkimusyhteisölle.⁵⁸ Dataa säätelemällä pyritään myös varmistamaan EU-yritysten kilpailukyky ja edistämään eurooppalaisia arvoja, kuten henkilötietojen suojaa, kuluttajansuojaa ja sananvapautta. Samalla edistetään EU:n digitaalista ja vihreää siirtymää.⁵⁹ Siten datastrategiassa pyritään sekä lisäämään dataan saatavuutta ja sen hyödyntämisestä saatavaa arvoa, että suojaamaan EU:n kansalaisten ja oikeushenkilöiden oikeuksia ja etuja.⁶⁰

Datastrategialla pyritään vastaamaan useisiin haasteisiin, jotka liittyvät muun muassa datan rajoitettuun saatavuuteen, eri lähteistä peräisin olevan datan yhdistettävyyden puutteisiin, heikkoon datan laatuun, yhtenäisen lainsäädännön puutteeseen sekä markkinavoimien keskittymiseen suurille pilvipalveluiden ja datainfrastruktuurien tarjoajille, jotka hallitsevat datan saatavuutta ja käyttöä.⁶¹ Käytännössä on tunnistettu useita tekijöitä, jotka heikentävät

⁵⁶ EU:n neuvosto 2025. EU:n neuvosto on hiljattain hyväksynyt asetuksen, joka luo terveysdata-avaruuden helpottamaan terveysdatan käyttöä ja vaihtoa.

⁵⁷ Komissio 2020a, s. 11–15. Datastrategiassa on suunniteltu data-avaruudet useille aloille, kuten terveydenhuoltoon, maatalouteen, valmistusteollisuuteen ja liikkuvuuteen, ja myöhemmin on tarkoitus luoda data-avaruudet myös kulttuuriperinnölle ja tiedotusvälineille. Datastrategia 2020, s. 25–32.

⁵⁸ Komissio 2020a.

⁵⁹ Komissio 2020a, s. 1–3. Aholainen – Bräutigam ym. 2022, s.15–16.

⁶⁰ Botero – Groza 2023, s. 16.

⁶¹ Komissio 2020a, s. 6–8. Myös Aholainen – Bräutigam ym. 2022, s.11–12. ks. tarkemmin ongelmista, joihin datasäädöksellä pyritään puuttumaan. Komissio 2022a, s. 7–15.

yritysten välistä datan jakamista, kuten kannustimien puute, pelko kilpailuedun menettämisestä sekä epäluottamus datan salassapitoon. IoT-datan jakamista estävät käytännössä neuvotteluvoiman epätasapaino, pelko kolmansien osapuolien väärinkäytöksistä sekä oikeudelliset epäselvyydet.⁶²

Datastrategian tavoitteena on luoda oikeudellinen kehys datalle, joka toteutetaan niin sanotun "big five" lakipaketin avulla. Tämä paketti sisältää viisi asetusta: digipalvelusäädös⁶³ (DSA, Digital Services Act), digimarkkinasäädös (DMA, Digital Markets Act)⁶⁴, datahallintasäädös⁶⁵ (DGA, Data Governance Act), datasäädös⁶⁶ (DA, Data Act) ja tekoälysäädös⁶⁷ (AIA, AI Act). Kaikki asetukset ovat jo voimassa, joista viimeisimpänä tekoälysäädös tuli voimaan 1.8.2024. Kunnianhimoista tavoitetta luoda yhteiset datan sisämarkkinat osoittaa se, että kaikki säädökset ovat asetuksia eli suoraan sovellettavissa EU:n jäsenvaltioissa⁶⁸. Datastrategian tavoitteet eivät toteudu pelkästään yksittäisillä säädöksillä, vaan "big five" -asetusten tarkoitus on luoda kokonaisuus, joka edistää kilpailukykyistä mallia datan käytölle ja saatavuudelle⁶⁹. Siten ei ole olemassa yhtä yleislakia datan saatavuutta edistäväksi sääntelyksi, vaan useita sääntelyinstrumentteja, jotka ohjaavat datan jakamista eri tavoitteiden saavuttamiseksi ja asettavat vaihtelevia velvoitteita⁷⁰. Datasäädös tulee hahmottaa osana laajempaa sääntelyjärjestelmää, joka yhdistää lainsäädännön, teknologiset ratkaisut ja infrastruktuurit⁷¹.

⁶² Komissio 2020a, s. 7. Komission kyselytutkimuksessa (Komissio 2018, s. 73–77) havaittiin, että suurimmat esteet datan jakamiselle yritysten välillä liittyvät teknisiin ja oikeudellisiin esteisiin. Oikeudelliset esteet, kuten epäselvyys datan käyttöoikeuksista. Muina esteinä mainittiin haasteet valvoa ja seurata jaetun datan käyttöä. Tekniset esteet voivat liittyä muun muassa datan yhteensopivuuden puutteeseen sekä turvallisuus- ja suojausvaatimuksiin.

⁶³ Euroopan parlamentin ja neuvoston asetukset (EU) 2022/2065, annettu 19 päivänä lokakuuta 2022, digitaalisten palvelujen sisämarkkinoista ja direktiivin 2000/31/EY muuttamisesta (digipalvelusäädös). Se tuli voimaan 16.11.2022 ja sitä sovelletaan 17.2.2024 alkaen.

⁶⁴ Euroopan parlamentin ja neuvoston asetukset (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaalisella ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (digimarkkinasäädös). Se tuli voimaan 1.11.2022 ja sitä sovelletaan 2.5.2023.

⁶⁵ Euroopan parlamentin ja neuvoston asetukset (EU) 2022/868, annettu 30 päivänä toukokuuta 2022, eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta (datanhallinta-asetus) (ETA:n kannalta merkityksellinen teksti). Se tuli voimaan 23.6.2022 ja sitä sovelletaan 24.9.2023 alkaen.

⁶⁶ Euroopan parlamentin ja neuvoston asetukset (EU) 2023/2854, annettu 13 päivänä joulukuuta 2023, datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä ja asetuksen (EU) 2017/2394 ja direktiivin (EU) 2020/1828 muuttamisesta (datasäädös). Se tuli voimaan 11.1.2024 ja sitä sovelletaan 12.9.2025 alkaen.

⁶⁷ Euroopan parlamentin ja neuvoston asetukset (EU) 2024/1689, annettu 13 päivänä kesäkuuta 2024, tekoälyä koskevista yhdenmukaistetuista säännöistä ja asetusten (EY) N:o 300/2008, (EU) N:o 167/2013, (EU) N:o 168/2013, (EU) 2018/858, (EU) 2018/1139 ja (EU) 2019/2144 sekä direktiivien 2014/90/EU, (EU) 2016/797 ja (EU) 2020/1828 muuttamisesta (tekoälysäädös). Tuli voimaan 1.8.2024, sitä sovelletaan 2.8.2026.

⁶⁸ Aholainen – Bräutigam ym. 2022, s. 15.

⁶⁹ Aholainen – Bräutigam ym. 2022, s. 28. Merkittävyydeltään big five lakipakettia ja datastrategiaa on verrattu GDPR:ään, jolla luotiin globaaleja standardeja ja sääntöjä henkilötietojen käsittelylle (ns. Bryssel vaikutus).

⁷⁰ Moscon 2023, s. 5.

⁷¹ Margoni – Strowel 2024, s. 21.

2.2 Tavoitteet

Datasäädös pyrkii vastaamaan datastrategiassa tunnistettuihin ongelmiin, jotka liittyvät etenkin siihen, että suurin osa datasta on keskittynyt alan suurille toimijoille ja jää hyödyntämättä. Datasäädöksen tavoitteena on edistää datan uudelleenkäyttöä siten, että kaikki voivat hyötyä dataan liittyvästä potentiaalista tasapuolisesti.⁷² Datasäädöksen tavoitteena on purkaa yksinoikeus datan hallintaan, joka antaa käytännössä portinvartija-aseman tuotteiden valmistajille. Sen tavoitteena on lisätä datan saatavuutta käyttäjille ja kolmansille osapuolille niin, että edistetään kilpailua ja innovointia IoT-tuotteiden toissijaisilla markkinoilla, kuten huolto- ja korjauspalveluissa, mutta myös kokonaan uudenlaisten tuotteiden ja palveluiden innovointia.⁷³ Käyttäjät hyötyvät lisääntyneen kilpailun tuomista eduista, kuten alhaisemmista hinnoista, laajemmasta palveluvalikoimasta ja laadukkaammista palveluista. Lisäksi datasäädös pyrkii parantamaan käyttäjien asemaa lisäämällä mekanismeja, joiden avulla käyttäjät voivat paremmin hallinta heidän käyttämiensä tuotteiden käytön tuloksena syntynyttä dataa. Datasäädöksellä pyritään myös edistämään datan oikeudenmukaista jakautumista koko yhteiskunnassa⁷⁴. Tiivistetysti tavoitteena on parantaa IoT-tuotteen käyttäjän oikeuksia hallita omaa dataansa ja hyötyä siitä sekä edistää oikeudenmukaisuutta IoT-datan markkinoilla.

2.3 Soveltamisalaan kuuluva data

Datasäädös koskee verkkoon liitettyjen tuotteiden⁷⁵ ja niihin liittyvien palveluiden⁷⁶ keräämää dataa. Asetuksessa data määritellään laajasti. Data tarkoittaa kaikkea toimenpiteiden, tosiseikkojen tai tietojen digitaalista esittämistä sekä tällaisten koosteita⁷⁷. Soveltamisalaan kuuluvat fyysisten, verkkoon liitettyjen tuotteiden data, jota ne saavat, tuottavat ja keräävät suorituskyvystään, käytöstään tai ympäristöstään. Verkkoon liitetyillä tuotteilla tarkoitetaan esineiden internetin tuotteiden dataa, johon kuuluvat muun muassa kodinkoneet, ajoneuvot, kulutuselektroniikka (kuten älykellot ja -sormukset), terveydenhuollon laitteet sekä maatalous- ja teollisuuslaitteet, kuten tuotantolaitteet ja sensorit. Asetusta ei sovelleta prototyyppien

⁷² Datasäädös johdanto (1).

⁷³ Datasäädös johdanto (32).

⁷⁴ Datasäädös johdanto (119). Komissio 2022d, s. 3. Taustalla vaikuttavat laajemmat poliittiset pyrkimykset lisätä yksilöiden vaikutusmahdollisuuksia omaan dataansa, luoda paremmat edellytykset yrityksille kilpailla ja innovoida, parantaa julkiselle sektorin valmiuksia vastata erilaisiin yhteiskunnallisiin ja poliittisiin haasteisiin sekä datan käytön ja yhteiskäytön lisäämiseen eri sektoreilla.

⁷⁵ Datasäädös 2 artikla 1 kohta 5 alakohta. Verkkoon liitetty tuote on esine, joka ”saa, tuottaa tai kerää dataa käytöstään ja ympäristöstään ja kykenee välittämään tämän datan sähköisen viestintäpalvelun, fyysisen yhteyden tai laiteyhteyden kautta. Asetus kattaa vain ne tuotteet, joiden ensisijainen toiminto ei ole datan tallennus, käsittely tai siirto kolmannen osapuolen toimesta.

⁷⁶ Datasäädös 2 artikla 1 kohta 6 alakohta. Verkkoon liitettyyn tuotteeseen liittyvät palvelut ovat digitaalisia palveluita (pois lukien sähköinen viestintäpalvelu) ja mukaan lukien ohjelmistot, jotka ovat välttämättömiä tuotteen toimintojen kannalta tai ne lisätään tuotteeseen sen toiminnallisuuden päivittämiseksi tai parantamiseksi. Ne voivat olla liitetty tuotteeseen ostohetkellä tai myöhemmin valmistajan tai kolmannen osapuolen toimesta.

⁷⁷ Aplin 2024, s. 89. Datasäädös 2 artikla 2 kohta.

tuottamaan dataan tai muihin tuotteisiin, joita ei ole saatettu markkinoille.⁷⁸ Lisäksi asetuksen soveltamisalaan ei kuulu puhtaasti kuvaileva data, kuten käyttöohjeet ja pakkauksen tiedot, tai data, joka syntyy käyttäjän käyttäessä infrastruktuuria, kuten maanteiden sensorien keräämä data tieverkosta⁷⁹. Verkkoon liitettyyn tuotteeseen liittyvän palvelun datalla tarkoitetaan puolestaan dataa, joka edustaa verkkoon liitettyyn tuotteeseen liittyvien käyttäjän toimien tai tapahtumien taikka toimettomuuden digitointia ja, joka syntyy palveluntarjoajan tarjotessa tuotteeseen liittyvää palvelua⁸⁰. Kyse voi olla esimerkiksi hallintaohjelmistosta, joka seuraa ja ohjaa verkkoon liitetyn tuotteen toimintaa⁸¹.

Datasäädöksen 4 artiklan 1 kohdan mukaa datan haltijan on asetettava käyttäjän saataville data, joka on *helposti saatavilla* sekä *asiaankuuluva metadata*. Helposti saatavilla olevalla datalla tarkoitetaan dataa, jonka datan haltija voi laillisesti hankkia ilman kohtuutonta vaivaa ja niin, että se ei perustuu vain yksinkertaisiin toimenpiteisiin⁸². Metadatalla tarkoitetaan datan jäsenneltyä sisällön tai käytön kuvausta, joka helpottaa kyseisen datan hakemista tai käyttämistä.⁸³ Metadata on kattotermi datalle, joka mahdollistaa sen, että dataa voidaan käyttää paremmin yhdistettynä muuhun dataan. Esimerkkejä metadatasta ovat peruskonteksti tai aikaleima.⁸⁴ Datasäädöksessä säädetty velvollisuus jakaa metadataa riippuu siitä, onko metadata tarpeellista datan tulkitsemiseksi ja hyödyntämiseksi.⁸⁵ Siten metadataa ei ole velvollisuutta jakaa laajemmin kuin sen arvioidaan olevan tarpeellista muun datan tulkitsemiseksi.

Lisäksi asetuksen soveltamisalaan kuuluu vain raakadata ja esikäsitelty data⁸⁶. Raakadata tarkoittaa tietoa, joka on kerätty suoraan sensorista (esimerkiksi lämpötila-, paine- tai

⁷⁸ Datasäädös johdanto (14). Hynönen - Leino -Bützow 2023, s. 471.

⁷⁹ Komissio 2024, s. 6–8. Kuvailevalla datalla ei ole yhteyttä tuotteen toimintaan tai käyttöön.

Infrastruktuuridataa ovat esimerkiksi rautateiden, lentokenttien tai maanteiden sensoreiden keräämää dataa, jota syntyy verkkoon liitetyn tuotteen toiminnan yhteydessä.

⁸⁰ Datasäädös 2 artikla 15 kohta. Datasäädös johdanto (15).

⁸¹ Hynönen - Leino -Bützow 2023, s. 472.

⁸² Datasäädös 2 artikla 17 kohta. Helposti saatavilla olevalla datalla' tuotteen dataa ja siihen liittyvän palvelun dataa, jonka datan haltija laillisesti saa tai voi saada verkkoon liitetyistä tuotteista tai siihen liittyvästä palvelusta ilman kohtuutonta vaivaa ja jota ei voida toteuttaa yksinkertaisin toimenpitein. Daria – Man Wai 2024, s. 20. Laillisia keinoja datan hankkimiselle voivat olla esimerkiksi tekniset keinot, tuotteen suunnittelu sekä datan haltijan ja käyttäjän välinen sopimus.

⁸³ Datasäädös 2 artikla 2 kohta. WIPO 2024, s. 134. Metadatan avulla voidaan määrittää datan luontiaika, tuottaja, tiedostomuoto, koko, sijainti ja suhteet muihin dataelementteihin. Se voi liittyä sekä raakadataan että käsiteltyyn dataan.

⁸⁴ Datasäädös johdanto (15)

⁸⁵ Daria – Man Wai 2024, s. 23 Datasäädös johdanto (20). Metadata eroaa verkkoon liitetyn tuotteen ja siihen liittyvän palvelun datasta myös siinä, että se ei ole helposti saatavilla olevaa dataa.

⁸⁶ Datasäädös johdanto (15): --"data, jota ei olennaisesti muuteta, eli raakamuodossa oleva data, jota kutsutaan myös lähteeksi tai primaaridataksi, joka viittaa automaattisesti ilman lisäkäsittelyä tuotettuihin tietopisteisiin, sekä data, joka on esikäsitelty sen ymmärrettävyyden ja käytön mahdollistamiseksi ennen jatkokäsittelyä ja analysointia, kuuluu tämän asetuksen soveltamisalaan."

tärinäsensorista) ja esitetty digitaalisesti numeerisina arvoina. Tämä data on suoraan seurausta analogisen signaalin, kuten lämpötilan, paineen tai tärinän, muuntamisesta digitaalseksi signaaliksi laitteessa tai ohjelmistossa.⁸⁷ Raakadata voi olla esimerkiksi antureiden keräämää dataa, mittauslaitteiden lukemia, kuvia, tekstiä, videoita tai numeerisia arvoja. Raakadata voi koostua yksittäisistä tietopisteistä tai tietueista, eikä sillä usein ole selkeää rakennetta tai järjestystä⁸⁸. Raakadata on alkuperäisessä muodossaan eli se sisältää kaikki tiedot sellaisina kuin ne on kerätty ilman tulkintoja tai muokkauksia.⁸⁹ Toisaalta voi väittää, että data ei ole koskaan täysin raakaa, koska siihen liittyy aina kognitiivisia prosesseja eli ihmisten tekemiä päätöksiä ja tulkintoja⁹⁰.

Esikäsittely data tarkoittaa dataa, jota on prosessoitu ennen sen varsinaista käsittelyä. Esikäsittelyn tarkoitus on parantaa datan laatua ja käyttökelpoisuutta. Datan esikäsittelyyn voi kuulua myös metadatan luominen.⁹¹ Teknisiä operaatioita, joita voidaan pitää datan esikäsittelynä, ovat esimerkiksi kalibrointi ja kohinan poistaminen (eng. de-noising). Esikäsittelyä dataa saadaan määrittämällä fyysinen määrä tai laatu tai muutos fyysisessä määrässä, jolloin data muuttuu ymmärrettäväksi ja käyttökelpoiseksi.⁹² Olennainen rajoitus on se, että esikäsittely data ei velvoita datan haltijaa tekemään merkittäviä investointeja esimerkiksi datan puhdistamiseen ja muuntamiseen.⁹³ On epäselvää, velvoittaako datasäädös datan haltijaa jakamaan lainkaan esikäsittelyä dataa, jos raakadata täyttää jo helposti saatavilla olevan datan vaatimuksen. Kysymys soveltamisalaan kuuluvan datan teknisestä tilasta on keskeinen, sillä se määrittelee, kuinka laaja velvollisuus datan haltijalla on asettaa dataa saataville.⁹⁴ Se, miten laajasti tai suppeasti datan esikäsittelyä tulkitaan voi vaikuttaa välillisesti myös liikesalaisuuksien suojaan.

⁸⁷ Daria – Man Wai 2024, s. 11.

⁸⁸ WIPO 2024, s. 133. Zech 2016, s. 17. Raakadata koostuu merkeistä (biteistä). Raakadataa ei ole käsitelty manuaalisesti ihmisen tai automaation toimesta (esim. analysointu) niin, että siitä olisi muodostunut merkityksellistä tietoa.

⁸⁹ Alemanno 2020, s. 23.

⁹⁰ Barrowman 2018. Raakadataan liittyy aina valintoja siitä, miksi se on kerätty, miten keruu on suoritettu ja millä tavalla dataa on käsitelty tai muokattu myöhemmin.

⁹¹ Alemanno 2020, s. 22–23.

⁹² Daria – Man Wai 2024, s. 8–10. Toisin sanoen esikäsittelyn avulla antureiden keräämät sähköiset signaalit, jotka on muutettu digitaaliseen muotoon (raakadata) muutetaan esimerkiksi celsiusasteiksi eli lämpötila-arvoksi. Datasäädös johdanto (15): esikäsittelyn avulla voidaan saada näkyväksi muutos esimerkiksi lämpötilassa, paineessa, virtausnopeudessa, äänessä, pH-arvossa, nestetasossa, asennossa, kiihtyvyydessä tai nopeudessa.

⁹³ Datasäädös johdanto (15). Esikäsittely ei saa sisältää ”merkittäviä investointeja”, mikä voi heikentää datan käytettävyyttä.

⁹⁴ Daria - Man Wai 2024, s. 14–15. Jos muuntaminen analogisesta digitaalseksi signaaliksi katsotaan yksinkertaiseksi toimenpiteeksi, raakadatan tarjoaminen riittää ”helposti saatavilla olevan datan” määritelmän täyttämiseksi. Tämä voisi tarkoittaa, että datan haltija voisi kieltäytyä esittämästä tietoja esikäsittelyssä muodossa.

Datasäädöksen soveltamisalan ulkopuolelle jää alkuperäisestä datasta johdettu tai päätelty data. Jos data on tulosta lisäinvestoinneista tai se on johdettu omistetuilla algoritmeilla ja/tai ohjelmistoilla, se ei kuulu asetuksen soveltamisalaan. Käsiteltyä tai johdettua dataa saadaan esimerkiksi keräämällä dataa useista antureista anturifuusiolla tai data-analytiikan avulla. Rajauksella pyritään suojaamaan datan haltijan taloudellisia etuja ja ylläpitämään kannustimia investoida.⁹⁵ Datan käsittely tarkoittaa datan analysointia ja manipulointia, jonka avulla siitä saadaan informaatiota. Käytännössä datan käsittelyvaiheita ovat esimerkiksi datan yhdistäminen tai erottaminen jonkun nimittäjän, kuten maantieteellisen alueen, mukaan, henkilötietojen käsittely, luokittelu, ryhmittely, ennusteiden ja erilaisten mallien rakentaminen.⁹⁶ Johdettu ja päätelty data sisältää todennäköisemmin liikesalaisuuksia kuin raakadata tai esikäsitelty data. Datasäädöksen soveltaminen vain raakadataan, metadataan ja esikäsiteltyyn dataan rajoittaa sen vaikutuksia liikesalaisuussuojan kannalta. Siitä huolimatta se ei tee vaikutusta tyhjäksi, koska myös tällaiseen dataan voi sisältyä liikesalaisuuksia sekä teollis- ja tekijänoikeuksia⁹⁷.

Soveltamisalaan kuuluvan datan tekninen määrittely on keskeinen kysymys, sillä se vaikuttaa siihen, kuinka laaja velvollisuus datan haltijalla on jakaa dataa. Tarkalla määrittelyllä voidaan estää tilanteet, joissa datan haltija yrittää välttää jakamista väittämällä, että kyseessä on esimerkiksi johdettu data esikäsitellyn datan sijaan. Toisaalta datan haltijoille on tärkeää tunnistaa tarkasti, mikä data kuuluu soveltamisalaan, jotta voidaan vähentää riskiä liikesalaisuuksien paljastumisesta, joita esimerkiksi johdetun datan jakaminen voi aiheuttaa. Datasäädös soveltuu vain dataan, joka on tuotettu asetuksen voimaantulon jälkeen 12.9.2025.⁹⁸ Asetuksen soveltamisalaan kuuluvat sekä henkilötiedot että ei-henkilötietoja sisältävä data.

2.4 Keskeiset uudistukset

Datasäädöksen II luvussa säädetään datan jakamisesta yrityksiltä kuluttajille sekä yritysten välillä. Datasäädöksen 3 artiklan 1 kohdan mukaan datan haltijan⁹⁹ on suunniteltava ja valmistettava verkkoon liitetyt tuotteet ja suunniteltava ja tarjottava niihin liittyvät palvelut siten, että tuotteen data ja siihen liittyvän palvelun data on suoraan käyttäjän¹⁰⁰ saatavilla. Data

⁹⁵ Datasäädös johdanto (15). Daria - Man Wai 2024, s. 17–19. Anturifuusion avulla syntyy usein dataa, kuten malleja, joita voidaan hyödyntää koneoppimisessa. Koneoppimismallit voivat olla patentoitavissa, ja omistettuja algoritmeja ja ohjelmistoja voidaan suojata teollis- ja tekijänoikeuksilla.

⁹⁶ Alemanno 2020, s. 22–23 ja 93–94.

⁹⁷ Datasäädös johdanto (31). Datasäädös 4 artikla 6 kohta ja 5 artikla 9 kohta. Mylly 2024, s. 372. Bird&Bird 2022.

⁹⁸ Datasäädös 50 artikla.

⁹⁹ Datasäädös 2 artikla 13 kohta. Datan haltija tarkoittaa luonnollista henkilöä tai oikeushenkilöä, jolla on oikeus tai velvollisuus käyttää ja tarjota dataa saataville esimerkiksi tuotteeseen tai siihen liittyvään palveluun liittyen, kun tästä on sovittu sopimuksella.

¹⁰⁰ Datasäädös 2 artikla 12 kohta. Käyttäjällä tarkoitetaan oikeushenkilöä tai luonnollista henkilöä, joka omistaa, vuokraa verkkoon liitetyn tuotteen tai, joka vastaanottaa tuotteeseen liittyvää palvelua.

on annettava saataville helposti, turvallisesti ja käyttäjälle maksutta kattavassa, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa. Lisäksi datan haltijan on annettava käyttäjälle selkeät ja ymmärrettävät tiedot ennen sopimuksen tekemistä verkkoon liitetyn tuotteen ostamisesta tai siihen liittyvän palvelun tarjoamisesta. Tietoihin kuuluu muun muassa datan tyyppi ja määrä, pääsy dataan, mahdollisuus jakaa dataa kolmannen osapuolen kanssa, datan käyttötarkoitukset, käyttäjän oikeus tehdä valitus viranomaiselle sekä tiedot liikesalaisuuksista ja niiden haltijasta, jos ne eivät kuulu datan haltijalle.¹⁰¹

Datasäädöksen 4 artiklan 1 kohdassa säädetään datan antamisesta käyttäjän saataville tämän pyynnöstä. Jos verkkoon liitetyn tuotteen käyttäjä ei voi saada dataa suoraan tuotteesta tai siihen liittyvästä palvelusta, datan haltijan on asetettava käyttäjän saataville helposti saatavilla oleva data ilman aiheutonta viivytystä samanlaatuksena kuin datan haltijan käytettävissä oleva data – ja tarvittaessa, kun se on teknisesti mahdollista, jatkuvasti ja reaaliaikaisesti. Datan saataville asettaminen koskee myös asianmukaista metadataa, jota tarvitaan datan tulkitsemiseen ja käyttämiseen. Valmistajan päätöstä siitä, miten data tarjotaan käyttäjälle, voivat ohjata esimerkiksi liikesalaisuuksien suojaan liittyvät syyt. Jos data on suoraan käyttäjän saatavilla, valmistajalla on vähemmän mahdollisuuksia hallita sen käyttöä, mikä voi lisätä liikesalaisuuksien paljastumisen riskiä. Tämän vuoksi datan haltijan voi olla järkevää valita epäsuora pääsy käyttäjän pyynnöstä, jos se auttaa paremmin varmistamaan datan säilymisen luottamuksellisenä.¹⁰²

Asetuksen 5 artiklan 1 kohdassa säädetään samanlainen velvollisuus datan haltijalle asettaa dataa käyttäjän pyynnöstä kolmannen osapuolen¹⁰³ saataville. Kolmansilla osapuolilla on puolestaan mahdollisuus jakaa käyttäjän hyväksymän dataan pääsyä koskevat oikeudet eteenpäin uusille kolmansille osapuolille käyttäjän kanssa tehtävän sopimuksen perusteella¹⁰⁴. Datasäädös pyrkii siten estämään toimittajalukkiutumisen (ns. lukkotilanne), joka edistää valmistajan monopoliaseman syntymistä jälkimarkkinoille¹⁰⁵.

Mikro- ja pienyritykset sekä alle vuoden toimineet keskisuuret yritykset on rajattu osittain asetuksen II luvun velvoitteiden ulkopuolelle. Keskisuurille yrityksille myönnetään poikkeus vuoden ajaksi siitä, kun niiden tuotteet tuodaan markkinoille¹⁰⁶. Portinvartijaksi määritelty

¹⁰¹ Datasäädös 3 artikla 2 ja 3 kohdat.

¹⁰² Euroopan komissio 2024, s. 17. Datasäädös 3 artikla 1 kohta.

¹⁰³ Datasäädös johdanto (33). Kolmas osapuoli voi olla luonnollinen henkilö, oikeushenkilö, kuten kuluttaja, yritys, tutkimusorganisaatio tai järjestö. Komissio 2022d, s. 14–15. Käytännössä kolmas osapuoli voi olla esimerkiksi jälkimarkkinapalvelun, kuten korjaus- ja huoltopalvelun, tarjoaja.

¹⁰⁴ Datasäädös johdanto (33). Datasäädös 6 artikla kohta 2 c.

¹⁰⁵ Hynönen - Leino -Bützow 2023, s. 469.

¹⁰⁶ Datasäädös 7 artikla.

yritys ei saa pyytää tai saada pääsyä dataan II luvun perusteella, eikä kolmansilla osapuolilla ole oikeutta jakaa dataa portinvartijoiden kanssa.¹⁰⁷ Kiellettyä on myös se, että kolmas osapuoli teettä palvelun, jota varten käyttäjä on pyytänyt datan jakamista kolmannelle osapuolelle, alihankintana portinvartijalta¹⁰⁸. Jos yksi yritysryhmän oikeushenkilöistä tarjoaa ydinalustapalveluita, kaikkia yritysryhmän jäseniä tulee käsitellä portinvartijoina¹⁰⁹.

Datasäädöksen III luku koskee datan haltijan velvoitteita datan saataville asettamisessa. Datasäädöksen 8 artiklan 1 kodan mukaan datan haltija sopii datan vastaanottajan¹¹⁰ kanssa datan saataville asettamista koskevista järjestelyistä avoimella tavalla sekä noudattaen oikeudenmukaisia, kohtuullisia ja syrjimättömiä ehtoja (FRAND-ehdot). Datan saataville asettamista koskevien korvausten on oltava syrjimättömiä ja kohtuullisia. Tämä korvaus ei saa ylittää datan saataville asettamisesta aiheutuvia kustannuksia, jos vastaanottaja on pk- yritys tai voittoa tavoittelematon tutkimusorganisaatio. Käyttäjille data on asetettava saataville maksutta.¹¹¹ Jos datan haltija ja vastaanottaja eivät pääse yksimielisyyteen datan jakamisen ehdoista, asia voidaan ratkaista jäsenvaltion sertifioimassa riidanratkaisuelimessä. Riidanratkaisumenettely on vapaaehtoinen menettely eikä se rajoita datan haltijan, datan vastaanottajan tai käyttäjän mahdollisuutta käyttää oikeussuojakeinoja jäsenvaltion tuomioistuimessa.¹¹²

Luvussa IV säädetään yritysten välisten sopimusten kohtuuttomien sopimusehtojen kiellosta. Datasäädöksen 13 artiklan 1 kohdan mukaan sopimusehto, jonka yritys on asettanut yksipuolisesti toiselle yritykselle, ei sido viimeksi mainittua, jos se on kohtuuton. Sopimusehto katsotaan kohtuuttomaksi, jos sen käyttö poikkeaa selvästi hyvästä kauppataavasta datan saannissa ja käytössä kunniallisen ja vilpittömän menettelyn vaatimuksen vastaisesti¹¹³. Aina kohtuuttomaksi katsotaan sopimuslausekkeet, jotka rajoittavat yksipuolisesti ehdon asettaneen vastuuta, rajoittavat datan vastaanottajien käytettävissä olevia oikeussuojakeinoja tai antavat datan haltijalle yksinoikeuden päättää, ovatko annetut tiedot sopimusehtojen mukaisia tai

¹⁰⁷ Datasäädös 6 artikla 2 kohta d alakohta ja 5 artikla 3 kohta. Portinvartija on määritelty digimarkkinasäädöksen (EU) 2022/1925 2 artiklan 1 kohdan 2 alakohdassa. Datasäädös johdanto (40). Tämä ei estä datan haltijoita luovuttamasta dataa vapaaehtoisesti portinvartijoiksi määrittelytellyille yrityksille. Kerber 2024, s. 6.

¹⁰⁸ Datasäädös johdanto (40). Datasäädös 5 artikla 3 kohta.

¹⁰⁹ Komissio 2022d. Datasäädös johdanto (36).

¹¹⁰ Datasäädös 12 artikla 14 kohta. Datan vastaanottajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka saa datan haltijalta dataa käyttöönsä omaan elinkeino-, liike-, käsiteollisuus- tai ammattitoimintaansa tarkoitukseen, mutta ei ole itse tuotteen tai siihen liittyvän palvelun käyttäjä; voi olla myös kolmas osapuoli käyttäjän pyynnöstä.

¹¹¹ Datasäädös 9 artikla 1 kohta ja 9 artikla 2 kohta a alakohta.

¹¹² Datasäädös 10 artikla 1 kohta. Datasäädös johdanto (52) ja (53).

¹¹³ Datasäädös 13 artikla 3 kohta.

yksinoikeuden tulkita sopimusehtoja¹¹⁴. Datasäädöksen 13 artiklan 5 kohdan a-f alakohta sisältää luettelon lausekkeista, jolloin sopimusehdon oletetaan olevan kohtuuton. Sopimusehdon asettavalla yrityksellä on todistustaakka siitä, ettei ehto ole kohtuuton¹¹⁵.

Datasäädöksen 14 artiklan mukaan datan haltijan on asetettava data julkisen sektorin elimen saataville poikkeuksellisen tarpeen perusteella. Artiklan 15 mukaan poikkeuksellinen tarve käyttää dataa voi johtua yleisestä hätätilanteesta tai muusta poikkeuksellisesta tilanteesta. Hätätilanne voi olla esimerkiksi terveysuhka, luonnonkatastrofi, ilmastonmuutoksen kärjistyminen tai muu suuri katastrofi. Lisäksi datan haltijan tulee asettaa data saataville, jos se on tarpeen sellaisen yleistä etua koskevan tehtävän suorittamiseksi, josta nimenomaisesti säädetään laissa, kuten virallisten tilastojen tuottamista varten tai yleisen hätätilan lieventämiseksi taikka siitä elpymiseksi. Lisäedellytyksenä on, että julkisen sektorin elin on käyttänyt kaikki muut käytettävissään olevat keinot tällaisen datan saamiseksi. Julkisen sektorin elimen on myös yksilöitävä pyydetty data, jota ei muutoin olisi voitu saada oikea-aikaisesti ja tehokkaasti ja vastaavin edellytyksin.¹¹⁶ Datasäädöksessä liikesalaisuuksien suoja vaihtelee sen mukaan, jaetaanko dataa B2G-suhteessa, yrityksiltä käyttäjille vai yritysten välillä¹¹⁷. Tässä tutkielmassa ei käsitellä tarkemmin datanjakovelvoitteita B2G-suhteessa. Sen sijaan luvussa 4 keskitytään siihen, miten liikesalaisuuksien suoja liittyy datanjakovelvoitteisiin yritysten ja käyttäjien sekä yritysten välisissä suhteissa.

2.5 Datasäädöksen haasteet liikesalaisuussuojan kannalta

2.5.1 Riski liikesalaisuussuojan heikentymisestä

Datasäädöksen yhteydessä liikesalaisuussuojan roolista on esitetty erilaisia näkemyksiä, jotka voidaan jakaa kahteen päälinjaan. Ensimmäisen näkemyksen mukaan liikesalaisuuksien suoja voi muodostaa esteen asetuksen tehokkaalle soveltamiselle, esimerkiksi rajoittamalla datan jakamista. Toisen näkemyksen mukaan taas datasäädös saattaa heikentää liikesalaisuuksien suojaa, mikä voi lisätä riskejä yritysten kannalta. Näitä näkökulmia tarkastellaan seuraavaksi tarkemmin.

Datasäädöksen liikesalaisuussuojan heikentymiseen liittyvät haasteet liittyvät ensinnäkin datan hallinnan menettämistä. Datan haltija ei voi lähtökohtaisesti kieltäytyä datan jakamisesta

¹¹⁴ Datasäädös 13 artikla 4 kohta.

¹¹⁵ Datasäädös johdanto (62).

¹¹⁶ Datasäädös johdanto (64). Datasäädös 15 artikla. Datasäädös 17 artiklassa luetellaan tiedot, jotka datapyynnössä on annettava.

¹¹⁷ Liikesalaisuuksien suoja vaihtelee sen mukaan, jaetaanko dataa B2G-suhteessa vai B2B- ja B2C-suhteissa. Ks. tarkemmin esimerkiksi Wiedemann - Leicht 2024, s. 10–13.

pelkästään sillä perusteella, että data sisältää liikesalaisuuksia. Käytännössä datasäädös tarkoittaa liikesalaisuuksien pakkolisensointia¹¹⁸. Liikesalaisuussuojan tarjoama kilpailuetu perustuu osittain siihen, että liikesalaisuuden haltijalla on harkintavaltaa päättää, milloin liikesalaisuuden käyttö, hankinta tai ilmaiseminen on sallittua. Datasäädöksen seurauksena yritykset eivät enää saa yksinoikeutta tietojen pääsyyn ja käyttöön, mikä voi heikentää niiden kilpailuetua, erityisesti, jos tiedon hallinta on olennainen osa liiketoimintaa¹¹⁹. Tiivistetysti datasäädös heikentää liikesalaisuuksien suojaa kahdella tavalla: datan haltija ei enää voi päättää, kenelle tietoja luovutetaan, eikä täysin kontrolloida niiden käyttötarkoituksia¹²⁰. Aikaisemmin datan haltijat ovat voineet vapaasti päättää, kenelle ne jakavat dataa ja mihin tarkoitukseen. Datasäädöksen myötä datan haltija sidottu käyttäjän ja kolmannen osapuolen välillä sovittuun datan käyttötarkoitukseen¹²¹. Tämä tarkoittaa rajoitusta datan haltijan sopimusvapauteen¹²². Datan haltijan päätösvallan menettäminen on merkittävää, sillä liikesalaisuuksien haltijan oikeus päättää tietojen jakamisesta on keskeinen tekijä. Empiiriset tutkimukset osoittavat, että osapuolten välinen luottamus on olennaista datan jakamisen onnistumiselle.¹²³ Datasäädös puolestaan rajoittaa liikesalaisuuden haltijan määräämisvaltaa, mikä voi heikentää haltijan kontrollia tietoihinsa.

Toiseksi datan jakaminen lisää riskiä siitä, että liikesalaisuudet paljastuvat, jolloin suoja menetetään. Datasäädöksen on nähty heikentävän liikesalaisuuksien suojaa, koska se velvoittaa yritykset jakamaan dataa, mikä altistaa liikesalaisuudet väärinkäytöksille ja antaa kilpailijoille mahdollisuuden hyödyntää niitä.¹²⁴ Datasäädöksessä ei ole eritä harvoja poikkeuksia lukuun ottamatta rajoitettu sitä, kenelle datan haltijan tulee jakaa dataa. Tämä tarkoittaa, että datan haltija voi joutua jakamaan laitteen keräämää dataa myös kilpailijalleen. Datan sisältämät liikesalaisuudet voivat liittyä esimerkiksi tuotteen valmistukseen tai suunnitteluun¹²⁵.

¹¹⁸ Aplin 2024, s. 87. Datasäädös johdanto (31).

¹¹⁹ Drexl – Banda - Gonzalez Otero ym. 2022, s.103. Datasäädöksen myötä datan haltija menettää kontrollin liikesalaisuuksiinsa, koska se ei voi lähtökohtaisesti estää käyttäjiä tai kolmansia osapuolia käyttämästä tai hyödyntämästä luottamuksellisia tietoja (ks. The European Automobile Manufacturers' Association (ACEA)). Esimerkiksi APPLia ja Siemens kritisoivat asetusehdotusta siitä, että liikesalaisuuden haltijalla ei ole keinoja valvoa, että käyttäjä tai kolmas osapuoli noudattaa sovittuja toimenpiteitä, eikä hän voi tehokkaasti panna niitä täytäntöön. Aplin - Radauer ym. 2023, s. 839.

¹²⁰ Bird&Bird 2022.

¹²¹ Drexl – Banda – Gonzalez ym. 2022, s. 37–38. Sopimusoikeuden yleisten oppien mukaan sopimukset sitovat vain osapuolia eikä niillä voida kuormittaa sopimuksen ulkopuolisia tahoja.

¹²² Kelto 2023. Sopimusvapauden kannalta ongelmallista on myös se, että datasäädös kohtelee käyttäjää ja kolmatta osapuolta samalla tavalla heikompina osapuolina suhteessa datan haltijaan. Todellisuudessa tällaista epätasapainoa ei välttämättä ole kolmannen osapuolen ja datan haltijan välillä. Ks. myös Margoni – Strowel 2024, s. 19–21. Leistner – Antoine 2023, s. 6.

¹²³ Radauer – Bader - Aplin ym. 2022, s. 34.

¹²⁴ Graef – Husovec 2022, s.4.

¹²⁵ Kelto 2023.

Liikesalaisuus voi olla myös tieto tuotteen vikaherkkyydestä tai heikkouksista, joiden paljastuminen asettaa datan haltijan haavoittuvaiseen asemaan¹²⁶.

Datasäädös perustuu oletukseen, että sopimuksia noudatetaan ja että ne tarjoavat riittävän suojan liikesalaisuuksille. Käytännössä tämä luottamus on heikentynyt, koska sopimusten noudattaminen ei ole aina taattua.¹²⁷ Datan jakaminen johtaa väistämättä myös tilanteisiin, joissa kolmas osapuoli rikkoo salassapitovelvoitteita. Liikesalaisuussuojaa heikentää myös se, että datan haltijan on usein vaikea valvoa oikeuksiensa toteutumista ja estää mahdollisia väärinkäytöksiä. Empiirisesti on todettu, että liikesalaisuuksien valvonta on vaikeaa ennalta, ja jälkikäteen saattaa olla haastavaa täytöntöönpanna oikeuksia.¹²⁸ Esimerkiksi kolmas osapuoli voi saada vilpittömän mielen suojaa, jolloin liikesalaisuusdirektiivin oikeussuojakeinot ovat käytettävissä vain, jos kolmas osapuoli tiesi tai sen olisi pitänyt tietää, että liikesalaisuus oli hankittu luvattomasti.¹²⁹ Käytännössä voi olla vaikeaa näyttää toteen, että kolmannen osapuolen olisi pitänyt tietää esimerkiksi, että toisella kolmannella osapuolella ei ollut käyttäjän kanssa 6 artikla 1 kohdan c alankohdan nojalla tehdyn sopimuksen perusteella oikeutta jakaa dataa.

Kolmanneksi datasäädöksen on esitetty heikentävän liikesalaisuussuojaa siten, että se vähentää yritysten investointihalukkuutta. Yritykset voivat olla haluttomia investoimaan datan tuottamiseen, jos ne joutuvat jakamaan arvokasta dataa kilpailijoilleen ja muille osapuolille, mikä puolestaan heikentää liikesalaisuussuojan merkitystä¹³⁰. Toisaalta datan haltijan investointikannustimien korostamista on kritisoitu siitä, että datataloudessa ei ole havaittavissa merkittävää investointivajetta¹³¹. On myös esitetty, että sitovan lainsäädännön säätäminen voi olla liian raskas ja ennenaikainen keino, koska datamarkkinat eivät ole vielä riittävästi kehittyneet¹³². Datasäädöksen valmisteluvaiheessa pidettiin tärkeänä, että asetuksella ei velvoiteta jakamaan liikesalaisuuksia sisältävää dataa, koska se heikentäisi yritysten

¹²⁶ Hynönen - Leino -Bützow 2023, s. 475.

¹²⁷ Komissio (2021), s. 6 ja 74. Noin puolet vastaajista, jotka koostuivat pääasiassa yrityksistä, (58 %), luottaa liikesalaisuuksien suojaan datan jakamisessa. Sopimukset ovat tyypillisin tapa, jolla suojataan liikesalaisuuksia dataa jaettaessa Tietojen käytön hallitsemiseksi vastaajat käyttävät erilaisia toimenpiteitä, kuten sopimusjärjestelyjä (45 %), liikesalaisuuksien suojaa (38 %), immateriaalioikeuksia (31 %) ja teknisiä keinoja (31 %).). Lisäksi 74 % vastaajista koki ulkomaisten viranomaisten mahdollisen pääsyn dataan olevan riski liikesalaisuuksien paljastumiselle.

¹²⁸ Aplin – Radauer – Bader – Searle 2023, s. 839. Banterle 2018, s. 7. Komissio 2016, s. 10–11.

¹²⁹ Radauer – Bader - Aplin ym. 2022, s. 98. Vapaavuori 2019, s. 163–166. Tällöin on kyse siitä, että liikesalaisuus ”saastuu”, joka estää sen jatkohyödyntämisen, jos henkilö ei ollut vilpittömässä mielessä.

¹³⁰ APPLIA 2023. Ks. myös Business Europe&Orgalim 2023. Datasäädös ei ole edullinen EU:n teollisuudelle, koska se heikentää liikesalaisuussuojaa.

¹³¹ Esim. Kerber 2023, s. 128. Myös Drexl 2018, s. 3. Radauer – Bader - Aplin ym. 2022, s. 28, jossa Arrow’s paradox viittaa siihen, että tiedon jakaminen voi samalla edistää innovaatioita ja heikentää investointikannustimia. Vastakkaista näkemystä edustaa Atkinson (2019, s. 15), joka katsoo, että datan pakkolisenssointi heikentää innovointia. Ks. tarkemmin luvusta 3.4.

¹³² Business Europe&Orgalim 2023.

toimintaedellytyksiä ja reilun kilpailun edellytyksiä¹³³. Se, millaisia vaikutuksia asetuksella on yritysten päätöksentekoon ja laajemmin talouteen selviää myöhemmin, kun datamarkkinoita tarkastellaan tarkemmin.

2.5.2 Liikesalaisuussuoja esteenä asetuksen tehokkaalle soveltamiselle

Liikesalaisuuksien suoja voi toimia innovaation edistämisen työkaluna, mutta samalla se voi rajoittaa tiedon jakamista ja innovatiivista uudelleenkäyttöä¹³⁴. Datasäädöksen tehokkaan soveltamisen kannalta on ongelmallista, jos liikesalaisuuksien suojaa väärinkäytetään estämään datasäädöksen mukainen dataan pääsy. Datan haltija voi esimerkiksi väittää datan olevan liikesalaisuus, vaikka se ei täyttäisi liikesalaisuuden määritelmää.¹³⁵ Erityisesti datasäädöksessä annettu mahdollisuus kieltäytyä kokonaan liikesalaisuuksia sisältävän datan jakamisesta poikkeuksellisissa olosuhteissa, voi johtaa opportunistiseen käyttäytymiseen¹³⁶. Jos liikesalaisuuksien käsijarrumekanismia käytetään datan jakovelvoitteiden välttämiseksi, asetuksen tehokas soveltaminen kärsii. Esimerkiksi pienten- ja keskisuurten yritysten kilpailukyvyn ja innovoinnin kannalta on tärkeää, ettei liikesalaisuusmekanismia käytetä perusteettomasti estämään dataan pääsyä¹³⁷. Tällöin liikesalaisuussuojaa käytetään ikään kuin strategisena välineenä välttämään sen soveltaminen.

Liikesalaisuuden laaja määritelmä ja sen epäselvä soveltaminen dataan voivat haitata datasäädöksen tehokkuutta. Datan haltijoiden on määriteltävä etukäteen (*ex ante*), onko data liikesalaisuus. Se, onko kyse liikesalaisuudesta, ratkaistaan viime kädessä tuomioistuimessa (*ex post*).¹³⁸ Liikesalaisuuksien liian laaja määrittely voi johtaa siihen, että raakadataa suojataan ilman riittäviä perusteita¹³⁹. Datan haltijat voivat esimerkiksi vaatia tarpeettoman laajoja teknisiä suojatoimia tai salassapitosopimuksia, vedoten liikesalaisuuksiin, vaikka niiden perusteltavuus ei olisi selvää¹⁴⁰. Kyseenalaista on myös se, miten tehokkaasti käyttäjä tai kolmas osapuoli voi riitauttaa datan haltijan ratkaisun liikesalaisuuksien yksilöinnistä, datan liikesalaisuusluonteesta tai toimenpiteiden oikeasuhteisuudesta.¹⁴¹ Datan haltijan ulkopuolisten on usein vaikea todistaa esimerkiksi, että tietty data ei ole liikesalaisuus.

¹³³ U 29/2022 vp s. 18.

¹³⁴ Sappa 2019, s. 416–418.

¹³⁵ Graef – Husovec 2022, s. 5.

¹³⁶ Krämer – Colangelo – Richter 2023, s. 23. Esimerkissä viitattu datasäädös 5 artiklan 11 kohtaan.

¹³⁷ Toffaletti 2023.

¹³⁸ Drexler – Banda – Gonzalez Otero ym. 2022, s. 102. Ducuing – Margoni 2022, s. 81.

¹³⁹ Krogerus luento 2024.

¹⁴⁰ Leistner – Antoine 2022, s. 86–88. Kerber 2023, s. 126.

¹⁴¹ Hynönen – Leino – Bützow 2023, s. 475–476. Keltto 2023.

Liikesalaisuussuojan tulkinta vaikuttaa merkittävästi asetuksen tehokkuuteen. Datasäädös pyrkii lieventämään datan jakamisen ja liikesalaisuuksien suojan välistä jännitettä tasapainottamalla molemmat intressit.¹⁴² Käytännössä este tehokkaalle soveltamiselle voi muodostua siitä, että käyttäjä tai kolmas osapuoli on haluton vastaanottamaan dataa asetuksen nojalla. Haluttomuus voi johtua esimerkiksi siitä, että datan haltija on asettanut tiukkoja ehtoja datan käytölle, kuten vastuun luvattomasta käytöstä, rajalliset käyttöoikeudet tai vaativat toimenpiteet luottamuksellisuuden säilyttämiseksi.¹⁴³ Kuitenkin, jos liikesalaisuuksia tulkitaan laajasti, voi syntyä ristiriitoja, joissa datan jakaminen jää toiseksi¹⁴⁴. Erityisesti datan haltijalle annettu mahdollisuus kieltäytyä datan jakamisesta poikkeuksellisissa olosuhteissa voi asettaa liikesalaisuudet etusijalle datan jakamisen sijaan¹⁴⁵.

¹⁴² Margoni – Strowel 2024, s. 7.

¹⁴³ Vaaraniemi -Schröder 2024.

¹⁴⁴ Drexl – Banda - Gonzalez Otero ym. 2022, s. 40 ja 102.

¹⁴⁵ Datasäädös 4 artikla 8 kohta. IRU 2022. Esimerkiksi se, mitkä tilanteet voidaan katsoa "poikkeuksellisiksi olosuhteiksi", joissa datan jakaminen voidaan estää, on tulkinnanvaraista.

3. LIIKESALAISUUSSÄÄNTELYN PERUSTEET JA SOVELTUMINEN IOT- DATAAN

3.1 Liikesalaisuussuojan perusteet

3.1.1 Suojan kohde, luonne ja soveltamisala

EU:ssa liikesalaisuuksien suojasta säädetään liikesalaisuusdirektiivissä ((EU) 2016/943). Liikesalaisuusdirektiivin 2 artiklan 1 kohdan mukaan liikesalaisuussuojaa suojaa tietoa, jolla on kaupallista arvoa salaisuutensa vuoksi ja, jonka salaisuuden suojaamiseksi tiedon laillinen haltija on ryhtynyt kohtuullisin toimenpiteisiin. Jos tieto täyttää liikesalaisuussuojan määritelmän, se voi saada suojaa väärinkäytöksiltä¹⁴⁶. Liikesalaisuuden laitton hankinta tapahtuu ilman liikesalaisuuden haltijan suostumusta. Liikesalaisuusdirektiivin 4 artiklan 2 kohdan mukaan liikesalaisuuden hankinta on laitonta, jos se tapahtuu esimerkiksi anastamalla, kopioimalla tai muulla tavalla, joka on vastoin rehellisiä kaupallisia käytäntöjä. Liikesalaisuusdirektiivin 4 artiklan 3 kohdan mukaan liikesalaisuuden käyttö tai ilmaiseminen katsotaan laittomaksi, jos se perustuu laittomasti hankittuun tietoon, salassapitosopimuksen rikkomiseen tai velvoitteen rikkomiseen, joka kieltää liikesalaisuuden käytön tai ilmaisemisen. Lisäksi kiellettyä on sellaisten tavaroiden tuotanto, tarjoaminen, saattaminen markkinoille, tuonti, vienti tai varastointi, joiden valmistamisessa on käytetty liikesalaisuutta laittomasti. Liikesalaisuuden laitton käyttö tai ilmaiseminen on kiellettyä myös silloin, kun liikesalaisuutta käytetään palvelujen tarjoamiseen.¹⁴⁷ Direktiivin mukaan suojaa voi saada, jos tiedon hankinta, käyttö tai ilmaiseminen tapahtuu tietoisesti tai olosuhteissa, joissa olisi pitänyt ymmärtää, että tieto oli hankittu tai ilmaistu suoraan tai välillisesti laittomasti¹⁴⁸.

Liikesalaisuusdirektiivin 3 artiklan 1 kohdan mukaan liikesalaisuuden hankinta katsotaan lailliseksi, jos liikesalaisuus saadaan a) itsenäisesti keksimällä tai luomalla, b) havainnoimalla, tutkimalla, purkamalla tai testaamalla tuotteita tai esineitä, jotka on asetettu yleisön saataville tai jotka ovat laillisesti sellaisen tiedon hankkijan hallussa ja, jota ei koske oikeudellisesti pätevä velvoite rajoittaa liikesalaisuuden hankkimista, c) työntekijöiden ja heidän edustajiensa käyttäessä tiedonsaanti- ja kuulemisoikeuttaan tai d) muulla tavalla, joka noudattaa rehellisiä kaupallisia käytäntöjä. Liikesalaisuussuojassa ei ole etuoikeusperiaatetta, kuten patenteissa. Siten valmistajat voivat esimerkiksi kerätä samaa dataa, kuten liikennetietoja, rikkomatta muiden valmistajien liikesalaisuussuojaa¹⁴⁹. Tieto tai keksintö on itsenäinen silloin, kun se on

¹⁴⁶ Drexl 2018, s. 91.

¹⁴⁷ Liikesalaisuusdirektiivi 4 artikla 5 kohta. Liikesalaisuusdirektiivi johdanto (27).

¹⁴⁸ Liikesalaisuusdirektiivi 4 artikla 4 kohta.

¹⁴⁹ Radauer – Bader – Aplin ym. 2022, s. 97. Käänteismallinnuksen ja itsenäisen kehitystyön salliminen on tärkeää kilpailun ja innovaation edistämiseksi dynaamisilla markkinoilla.

saatu tai luotu ilman, että se perustuu liikesalaisuuden laittomaan hankkimiseen, käyttämiseen tai ilmaisemiseen. On kuitenkin usein vaikeaa määrittää, milloin liikesalaisuus on luotu täysin itsenäisesti. Arvioinnissa voidaan ottaa huomioon muun muassa se, onko vastaajan luoma tieto syntynyt ennen mahdollisia lainvastaisia toimia. Toinen huomioon otettava tekijä on se, onko keksintö syy-yhteydessä liikesalaisuutta loukkaaviin laittomiin toimiin. Lisäksi on tarkasteltava, miten liikesalaisuudet on yksilöity eli onko kyse yhdestä vai useammasta liikesalaisuudesta.¹⁵⁰ Datasäädös lisää saatavilla olevan datan määrää, mikä voi kiihdyttää itsenäisen kehitystyön ja käänteismallinnuksen mahdollisuuksia hankkia liikesalaisuuksia.

Liikesalaisuusdirektiivin 3 artiklan 2 kohdassa säädetään, että liikesalaisuuden hankinta, käyttö tai ilmaiseminen on laillista myös silloin, kun sitä edellytetään tai se sallitaan unionin oikeudessa tai kansallisessa laissa. Laillisesti yhdessä EU:n jäsenvaltiossa hankittuja tietoja ei välttämättä voi ilmaista tai käyttää toisessa jäsenvaltiossa, jos se kielletään kyseisen jäsenvaltion lainsäädännössä¹⁵¹. Tämä artikla kattaa myös datan jakamisen datasäädöksen nojalla¹⁵². Siten liikesalaisuuksien hankkiminen datasäädöksen perusteella ei ole laitonta, ellei käyttäjä tai kolmasosapuoli riko liikesalaisuuksien luottamuksellisuutta. Edelleen liikesalaisuusdirektiivin 5 artiklan 1 kohdassa säädetään poikkeuksista, jolloin liikesalaisuuden väitetty laiton hankinta, käyttö tai ilmaiseminen hylätään. Poikkeukset koskevat väärinkäytösten paljastamista, sananvapauden ja tiedotusvälineiden vapautta, liikesalaisuuden ilmaisemista työntekijän edustajalle sekä unionin oikeudessa tai kansallisessa laissa tunnustetun oikeutetun edun suojaamista.

Liikesalaisuuksia ei voida suojata samalla tavalla kuin perinteisiä immateriaalioikeuksia, jotka koskevat tarkemmin määriteltyjä asioita. Liikesalaisuudet rinnastetaan kuitenkin immateriaalioikeuksiin osana yritysten aineetonta varallisuutta¹⁵³. Toisin kuin immateriaalioikeudet, liikesalaisuussuoja ei luo omistusoikeutta tietoon, vaan pyrkii säilyttämään sen salaisena.¹⁵⁴ Liikesalaisuuden haltija menettää mahdollisuuden vedota suojaan, jos tieto paljastuu. Tämän vuoksi liikesalaisuuksia on luonnehdittu myös katoavaksi omistusoikeudeksi¹⁵⁵. Koska liikesalaisuudet ovat luonteeltaan "haavoittuvia" tai "katoavia",

¹⁵⁰ Aplin 2020, s. 8–12.

¹⁵¹ Nordberg 2020, s. 211.

¹⁵² Datasäädös johdanto (15).

¹⁵³ HE 114/1976, s. 14. HE 49/2018, s. 22. Liikesalaisuussuoja täydentää immateriaalioikeuksia ja tarjoaa vaihtoehtoisen suojamuodon. Lemleyn (2008, s. 315–316) mukaan liikesalaisuudet ovat osa immateriaalioikeuksia. Liikesalaisuudet saivat nykymuodossaan alkunsa vasta 1800-luvun angloamerikkalaisessa common law -oikeuskäytännössä. Liikesalaisuussuojassa yhdistyvät sopimus-, vahingonkorvaus- ja varallisuus oikeudesta. Sappa 2019, s. 409. Searle 2021, s. 8.

¹⁵⁴ Drexl 2018, s. 96.

¹⁵⁵ Sappa 2019, s. 409–410.

niiden salassa pitäminen edellyttää lisenssi- ja salassapitosopimusten tarkkaa muotoilua.¹⁵⁶ Liikesalaisuutta on luonnehdittu myös kvasi-immateriaalioikeudeksi, sillä se ei anna täydellistä yksinoikeutta tietoon. Sen sijaan se tarjoaa oikeuden saada korvausta tietyissä vilpillisen menettelyn tilanteissa sekä kilpailuetua tiedoista ennen kuin muut esimerkiksi keksivät saman tiedon itse.¹⁵⁷

Liikesalaisuusdirektiivi on soveltamisalaltaan laaja. Liikesalaisuussuojaa voi saada mikä tahansa tekninen tai taloudellinen tieto taikka taitotieto eli know-how, joka liittyy elinkeinotoimintaan.¹⁵⁸ Luottamukselliset tiedot voidaan niiden luonteen mukaan jakaa teknisiin ja taloudellisiin liikesalaisuuksiin. Esimerkkejä liikesalaisuuksista ovat testitulokset, liikeideat, hinnoittelutiedot, taitotieto (know-how), markkinaselvitykset, talousennusteet, kilpailija-analyysit, asiakasrekisterit sekä hallinnolliset ja organisatoriset tiedot yrityksistä. Liikesalaisuus voi sisältää myös ohjelman salaisia osia, kuten tietokoneohjelman lähdekoodin, rakenteen, määrittelyn ja algoritmit. Myös negatiivinen tieto, kuten toimimaton valmistusmenetelmä, voi olla liikesalaisuus.¹⁵⁹

Lisäksi liikesalaisuusdirektiivin 1 artiklan 2 kohdassa on rajoitettu liikesalaisuussuojan alaa siten, että se ei saa vaikuttaa perusoikeuksiin, kuten sananvapauteen tai tiedonvälityksen vapauteen, taikka yleiseen etuun, jos tietojen paljastamista on pyydetty tämän perusteella unionin tai kansallisten sääntöjen mukaan. Lisäksi lainmukaisten velvoitteiden täyttämiseksi EU:n tai kansallisten viranomaisten saamat tiedot on paljastettava liikesalaisuussuojasta riippumatta.¹⁶⁰ Siten liikesalaisuussuojan ala on laaja, ja lähes mitä tahansa tietoa voi suojata, kunhan se ei ole ristiriidassa perusoikeuksien tai yleisen edun kanssa¹⁶¹.

3.1.2 Tavoitteet (liikesalaisuuksien ”dilemma”)

Liikesalaisuusdirektiivin tavoitteena oli harmonisoida liikesalaisuuksia koskeva sääntely EU:ssa ja yhtenäistää jäsenvaltioiden lainsäädäntöä. Tavoitteena oli suojata liikesalaisuuksia laittomalta hankinnalta, käytöltä ja ilmaisemiselta EU:n sisämarkkinoilla. Yhdenmukaistettu sääntely vähensi sisämarkkinoiden esteitä, lisäsi oikeusvarmuutta ja paransi yritysten

¹⁵⁶ Hull 2009, s. 212 ja 207. Liikesalaisuudet eroavat muista immateriaalioikeuksista, koska niiden suojaaminen ei perustu omistusoikeuteen, vaan ne ovat henkilökohtaisia oikeuksia (*right in personam*). Tämä tarkoittaa, että suojaan voi vedota vain sellaisia tahoja vastaan, jotka ovat tekemisissä liikesalaisuuden haltijaan kanssa.

¹⁵⁷ Sappa 2019, s. 410. Determann 2018, s.14–16. Liikesalaisuuslain tarkoitus on suojata tietoja vilpilliseltä menettelyltä. Liikesalaisuusdirektiivin johdannon (16) mukaan innovoinnin ja kilpailun edistämiseksi direktiivin säännökset eivät luo yksinoikeutta liikesalaisuutena suojattuun tietoon. Wiebe - Schur 2019, s. 814–815.

¹⁵⁸ Liikesalaisuusdirektiivi johdanto (14): ”– on tärkeää ottaa käyttöön yhtenäinen liikesalaisuuden määritelmä, jossa ei aseteta rajoituksia väärinkäytöltä suojattavalle kohteelle”.

¹⁵⁹ HE 49/2018, s. 22 ja 84.

¹⁶⁰ Liikesalaisuusdirektiivi 1 artikla 2 kohta. Datasäädös johdanto (34).

¹⁶¹ Nordberg 2020, s.199–202.

kilpailukykyä tarjoamalla yhtenäisen siviilioikeudellisen suojan koko unionin alueella. Direktiivi vastasi tarpeeseen korjata jäsenvaltioiden sääntelykäytäntöjen erot sekä yritysten kasvaneen haavoittuvuuden esimerkiksi vakoilun ja työntekijöiden tietovarkauksien suhteen.¹⁶² Se määrittelee liikesalaisuuksien suojalle vähimmäisvaatimukset, mutta kansallisesti voidaan säätää kattavammasta suojasta¹⁶³.

Liikesalaisuuksien suojelun tavoitteena on suojata yritysten ja tutkimuslaitosten investointeja tiedon ja osaamisen hankkimiseen, kehittämiseen ja soveltamiseen, sillä nämä ovat keskeisiä kilpailuetuja tietotaloudessa. Kilpailuedun suojaaminen on tärkeää kaikille yrityksille, mutta erityisesti pienille ja keskikokoisille yrityksille. Lisäksi liikesalaisuussuojalla pyritään ylläpitämään luottamusta siihen, että yrityksille arvokkaat tiedot pysyvät salassa. Tämä saavutetaan ehkäisemällä liikesalaisuuksien oikeudetonta hankintaa, ilmaisemista ja käyttämistä. Toinen direktiivin keskeinen tavoite on edistää innovointia.¹⁶⁴ Suojaamalla yritysten panostuksia tiedon hankintaan ja luomiseen tuetaan avointa innovointia sekä yhteistyöhön perustuvaa tutkimusta, joka edistää uusien ideoiden syntymistä¹⁶⁵.

Liikesalaisuuksien suojelussa on tärkeää tasapainottaa kaksi tavoitetta: tiedon suojaaminen ja tiedon jakaminen. Direktiivi pyrkii suojaamaan yritysten kilpailukykyä ja edistämään innovointia samalla, kun se kannustaa tiedon jakamiseen, joka tukee yhteistyöhön perustuvaa tutkimusta ja innovointia.¹⁶⁶ Lisäksi direktiivi huomioi laajemmat yhteiskunnalliset edut ja perusoikeuksiin liittyvät seikat. Näin ollen liikesalaisuuksia koskeva sääntelyn tulee edistää innovointia, kilpailua, tiedon kiertoa sekä tutkimus- ja kehitystoimintaa ilman, että se vaarantaa tai heikentää perusoikeuksia tai -vapauksia taikka yleistä etua, kuten yleistä turvallisuutta, kansanterveyttä, ympäristösuojelua tai kuluttajansuojaa.¹⁶⁷ Siten liikesalaisuusdirektiivin tavoitteena on tasapainottaa yksityiset edut ja laajemmat yhteiskunnalliset intressit.

Kysymys tavoitteista liittyy myös siihen, mikä tieto voi olla liikesalaisuussuojan kohteena. Tavoitteita voi tulkita laajasti niin, että ne suojaavat myös tietoa, joka syntyy yrityksen toiminnan sivutuotteena. Suppean tulkinnan mukaa suojaa voivat saada vain tiedot, jotka liittyvät liikesalaisuuden haltijan ydin liiketoimintaan. Tämä johtuu siitä, että vain tällaisen tiedon suojaaminen edistää yrityksen kilpailukykyä ja innovatiivisuutta. Toiminnan

¹⁶² Liikesalaisuusdirektiivi johdanto (6–10). Schovsbo 2020, s. 7–10.

¹⁶³ Liikesalaisuusdirektiivi johdanto (10).

¹⁶⁴ HE 49/2018 vp, s.11.

¹⁶⁵ Liikesalaisuusdirektiivi johdanto (1–3).

¹⁶⁶ Liikesalaisuusdirektiivi johdanto (16) ja (21).

¹⁶⁷ Liikesalaisuusdirektiivi johdanto (16) ja (21).

sivutuotteena syntyvät tiedot voivat puolestaan edistää muiden yritysten ja julkisyhteisön innovointia, minkä liian laaja liikesalaisuussuoja voi estää.¹⁶⁸ Perusteltua onkin välttää liian laajaa tavoitteiden soveltamista, jos ei ole selvää, miten se hyödyttää liikesalaisuuden haltijaa. Suppean tulkinnan voi myös hahmottaa siten, että se pyrkii edistämään muiden yritysten mahdollisuuksia käyttää dataa esimerkiksi innovointiin tai muulla tavalla, jota liikesalaisuusdirektiivi pyrkii suojaamaan.

Lopuksi voi pohtia, ovatko datasäädöksen ja liikesalaisuusdirektiivin tavoitteet ristiriidassa toistensa kanssa. Datasäädös velvoittaa jakamaan dataa, vaikka se saattaa sisältää liikesalaisuuksia. Liikesalaisuusdirektiivi suojelee tiettyjä tietoja liikesalaisuuksina, mikä rajoittaa niiden jakamista. Sama tieto voi olla sekä liikesalaisuus että datan jakamisvelvoitteiden kohde, jolloin velvoitteet ja kiellot voivat olla ristiriidassa.¹⁶⁹ Siten sääntelyiden perusidea on päinvastainen: liikesalaisuussääntely pyrkii suojaamaan tietoja, kun taas datasäädös pyrkii edistämään datan jakamista.¹⁷⁰ Toisin sanoen molemmat sääntelyjärjestelmät tähtäävät tiedon käytön ja jakamisen edistämiseen, mutta lähestymistavat ja sääntöjen soveltaminen poikkeavat toisistaan. Liikesalaisuusdirektiivi keskittyy tietojen luottamuksellisuuden suojaamiseen, kun taas datasäädös edistää datan jakamista asettamalla velvoitteita.¹⁷¹ Datasäädöksessä on pyritty sovittamaan yhteen nämä vastakkaiset intressit, jolloin voidaan väittää, että ristiriitaa ei ainakaan lähtökohtaisesti synny¹⁷². Vaikka datasäädöksessä on tunnistettu nämä vastakkaiset intressit, ristiriidan olemassaolo ei ole täysin poissuljettu, vaan riippuu soveltamiskäytännöstä.

3.2 Liikesalaisuuden määritelmä ja soveltuminen (IoT-) dataan

3.2.1 Datan soveltuminen liikesalaisuudeksi yleistä

Liikesalaisuusdirektiivin 2 artiklan 1 kohdan mukaan liikesalaisuudella tarkoitetaan tietoa, joka on a) salaista siinä mielessä, että se ei ole kokonaisuutena tai osiensa täsmällisenä kokoonpanona ja yhdistelmänä tällaisia tietoja yleensä käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa, b) sillä on salaisuutensa vuoksi kaupallista arvoa elinkeinotoiminnassa, ja c) henkilö, jolla on tieto laillisesti hallussaan, on ryhtynyt vallitsevissa olosuhteissa kohtuullisiksi katsottaviin toimenpiteisiin sen pitämiseksi salaisena. Kyseessä on kumulatiivinen vaatimus, koska kaikki kolme kriteeriä on täytettävä samanaikaisesti, jotta tieto

¹⁶⁸ Drexl 2017, s. 269.

¹⁶⁹ Wiedemann - Leicht 2023, s. 4–5. Datasäädös johdanto (2). Liikesalaisuusdirektiivi johdanto (3).

¹⁷⁰ IPR University 2024.

¹⁷¹ Ducuing – Margoni 2022, s. 79–80.

¹⁷² Graf Ballestrem – Harris – De le Court ym. 2022, s. 23. Margoni – Strowel 2024, s. 7. Ducuing – Margoni 2022, s. 82 ja 85.

voidaan katsoa liikesalaisuudeksi.¹⁷³ Direktiivi perustuu pitkälti TRIPS-sopimuksen 39. artiklaan, jossa määritellään julkistamaton tieto¹⁷⁴.

Liikesalaisuusdirektiivi on teknologianeutraali, joten se suojaa kaikenlaista tietoa tallennus- tai säilytystavasta riippumatta. Suojan piiriin voivat kuulua esimerkiksi digitaaliset objektit, kuten digitaalisessa muodossa oleva teksti, kuva tai ääni, algoritmi tai ohjelmointikoodi. Liikesalaisuus voi myös olla tallennettu digitaaliseen muotoon, kuten tieto jonkin tuotteen valmistusmenetelmästä.¹⁷⁵ Tästä syystä liikesalaisuussuoja soveltuu lähtökohtaisesti myös IoT-dataan ilman, että tietoa tarvitsee erikseen merkitä salaiseksi.¹⁷⁶

Datassa voidaan erottaa kolme tasoa: rakenteellinen, syntaktinen ja semanttinen. Liikesalaisuussuojaa voi saada vain semanttisen tason data eli tieto (eng. *information*), jolla on merkityksellistä sisältöä. Syntaktinen data, kuten bitit ja tavut, joihin tieto on koodattu, ei yksinään voi saada liikesalaisuussuojaa. Rakenteellinen taso puolestaan viittaa tiedon tallennusvälineeseen, joka voi olla esimerkiksi fyysinen tai digitaalinen tallenne. Tallenneväline itsessään ei voi saada liikesalaisuussuojaa eikä liikesalaisuuden olemassaolo riipu sen muodosta.¹⁷⁷ Lisäksi voidaan erottaa tiedon pragmaattinen taso, joka liittyy datan käyttöön ja tarkoitukseen. Data voi muuttua arvokkaaksi tiedoksi vasta silloin, kun sitä käytetään tai käsitellään tietyllä tavalla.¹⁷⁸ Siten voidaan tehdä ero datan ja liikesalaisuutena suojattavan tiedon välillä, erottamalla syntaksinen taso semanttisesta tasosta. Datan ja informaation erottaminen ei ole aina yksinkertaista, joten liikesalaisuuden määritelmän täyttymistä tulee tarkastella tapauskohtaisesti.¹⁷⁹ Raakadata, esikäsitelty data tai päätelty data voivat kaikki olla informaatiota ja täyttää liikesalaisuuden kriteerit.¹⁸⁰ Siten se, että kyse on

¹⁷³ Vapaavuori 2019, s. 64.

¹⁷⁴ Menell – Almeling – Cundiff ym. 2023, s. 70–71. Kansainvälisesti liikesalaisuuksien periaatteet määriteltiin ensimmäistä kertaa vuonna 1994 voimaan tulleessa TRIPS-sopimuksessa (WTO), joka velvoittaa jäsenvaltioita tarjoamaan liikesalaisuuksille riittävän suojan.

¹⁷⁵ WIPO 2024, s. 137.

¹⁷⁶ Sappa 2018, s. 522–523 ja Vapaavuori 2019, s. 57–58. Syrjimättömyyden periaatteen mukaan IoT-tuotteiden sensoreiden keräämää dataa on suojattava samalla tavalla kuin muulla tavalla syntynyttä dataa. Drexl (2018, s. 92–93 ja 28) katsoo, että yhdistetyistä laitteista peräisin oleva data voi olla liikesalaisuus. Kuitenkin Drexlin analyysi keskittyy yhdistettyihin laitteisiin, jotka eivät ole sama asia kuin IoT-laitteet. Yhdistetyt laitteet ovat laajempi käsite ja viittaavat laitteisiin, jotka ovat yhteydessä muihin laitteisiin tai henkilöihin joko langattoman tai langallisen viestinnän kautta (esimerkiksi Wi-Fi-yhteyden avulla) ja tuottavat dataa. IoT-laitteet (esineiden internet) puolestaan viittaavat laitteisiin, jotka voivat kommunikoida keskenään automaattisesti modernien viestintäteknologioiden, kuten 5G-matkaviestinteknologian, avulla.

¹⁷⁷ Drexl, 2018, s. 92.

¹⁷⁸ Wiebe – Schur 2019, s. 815–816. EU-tuomioistuimen C-490/14 Freistaat Bayernl, kohdat 25–29. EU-tuomioistuimen mukaan datan arvo riippuu kontekstista. Siten datan taloudellinen arvo ei ole vakio, vaan se vaihtelee sen mukaan, miten ja missä sitä käytetään. Datan taloudellinen arvo määräytyy sen käyttötarkoituksen mukaan. Margoni – Strowel 2024, s. 2–3.

¹⁷⁹ Nordberg 2020, s. 202.

¹⁸⁰ Zech 2024, s. 58–59. Liikesalaisuus voidaan suojata riippumatta tiedon ilmenemismuodosta. Tämä tarkoittaa, että liikesalaisuussuoja kattaa sekä merkityksellisen tiedon (semanttinen taso) että sen eri ilmentymät, kuten

esimerkiksi käsittelemättömästä raakadatasta, ei automaattisesti estä sen mahdollisuutta saada liikesalaisuussuojaa.

Etenkin liikesalaisuussuojan soveltuminen raakadataan on ollut kiistanalainen kysymys. Oikeuskirjallisuudessa on esitetty kannanottoja sen puolesta ja vastaan, voiko raakadata muodostaa liikesalaisuuden.¹⁸¹ IoT-tuotteiden keräämä data on suurelta osin raakadataa eli merkkejä syntaktisella tasolla, jotka eivät itsessään sisällä merkitystä¹⁸². Raakadatan osalta on pidetty kriittisenä erityisesti sitä, onko tällaisella datalla kaupallista arvoa ja onko todennäköistä, että se pidetään salassa¹⁸³. Viimeistään datasäädöksen myötä on selvää, että liikesalaisuussuojaa voidaan soveltaa myös verkkoon liitettyjen tuotteiden ja niihin liittyvien palveluiden tuottamaan raakadataan. Kuitenkin liikesalaisuuden määritelmän soveltaminen IoT- dataan on edelleen tulkinnanvaraista monissa tapauksissa¹⁸⁴. Pelkkä tieto siitä, että tuote tai laite kerää dataa, ei itsessään muodosta liikesalaisuutta. Sen sijaan, se miten ja mitä dataa kerätään, voi olla liikesalaisuus. Esimerkiksi patentoitujen sensoreiden keräämä ainutlaatuinen data voi olla liikesalaisuus. Samoin laitteen keräämä metadata voi saada suojaa, jos se ei ole käyttäjien helposti saatavilla.¹⁸⁵ Esimerkiksi älyauton keräämä ainutlaatuinen data, kuten järjestelmien keräämä tai algoritmien tuottama tieto, voi täyttää liikesalaisuuden kriteerit. Liikesalaisuuksia voivat olla myös tiedot, jotka syntyvät järjestelmäalgoritmien sivutuotteena.¹⁸⁶ Datasäädöksen soveltamisalaan kuuluva data jättää kuitenkin osan dataan sisältyvistä liikesalaisuuksista datanjakovelvoitteiden ulkopuolelle.

Erillisenä kysymyksenä liikesalaisuussuojan soveltuvuudesta dataan on myös sen tarkoituksenmukaisuus datan suojamuotona. On esitetty, että koneellisesti tuotetun raakadatan suojaamiseen sopivat erityisesti liikesalaisuussuoja ja tietokantadirektiivin mukainen *sui generis* -suoja.¹⁸⁷ Liikesalaisuussuojaa on pidetty erityisesti datataloudessa tarkoituksenmukaisimpana suojamuotona, sillä se ei luo yksinoikeutta, toisin kuin immateriaalioikeudet ja omistusoikeudet, vaan keskittyy siihen, miten kolmannet osapuolet

koodin (syntaktinen taso), fyysisen tallenteen tai muun datan esitysmuodon. Liikesalaisuus voi olla esitetty syntaktisella tasolla, kuten koodina.

¹⁸¹ Aplin – Radauer – Bader – Searle (2023, s. 843–844) esittivät, että liikesalaisuusdirektiiviin tulisi lisätä täsmennys, jonka mukaan raakadataa tai käsittelemätöntä dataa ei voida suojata liikesalaisuutena. Myös Farkas (2017, s. 10–11) on katsonut, että IoT-laitteiden keräämä tieto ei yleensä täytä liikesalaisuuden kriteerejä. Vastakkaista näkemystä edustaa esimerkiksi Sappa 2018, s. 522. Sappa on esittänyt, että raakadata voi täyttää liikesalaisuuden kriteerit, jos sillä on taloudellista arvoa ja se pidetään salassa.

¹⁸² Pihlajarinne – Ballardini 2019, s. 117–118. Zech 2024, s. 59.

¹⁸³ Aplin 2024, s. 89. Drexl 2018, s. 92–93.

¹⁸⁴ Drexl 2016, s. 22. Komissio 2017. Sappa 2019, s. 414. Sappan mukaan ainoa tapa varmistaa tiedon hallinta algoritmiyhteiskunnassa on, se että yritys pitää datan itsellään de facto (tosiasiallinen hallussapito). Radauer – Bader - Aplin ym. 2022, s. 75. IPR University 2024, dia 10.

¹⁸⁵ WIPO 2024, s. 134.

¹⁸⁶ Sandeen - Aplin 2021, s. 6.

¹⁸⁷ Komissio 2017, s. 10–11.

voivat hankkia, käyttää ja ilmaista tietoa.¹⁸⁸ Eksklusiivinen omistusoikeus voisi puolestaan olla ristiriidassa tiedon vapaan käytön ja jakamisen periaatteiden kanssa¹⁸⁹. Liikesalaisuussuojan soveltaminen älytuotteiden tuottamaan dataan on kuitenkin haastavaa, koska suoja rajoittuu vain luvaton hankkimista, käyttämistä ja ilmaisemista vastaan. Vaikka datasäädös on vahvistanut liikesalaisuussuojan asemaa IoT- datan suojaamisessa, sen vahvuudet ja heikkoudet kaipaavat kriittistä tarkastelua. Seuraavassa kappaleessa tarkastellaan liikesalaisuuden määritelmän soveltumista dataan.

3.2.2 Tiedon salaisuus

Liikesalaisuusdirektiivin 2 artiklan 1 kohdan a alakohdan mukaan liikesalaisuutena suojataan tietoa, joka kokonaisuutena tai osiensa täsmällisenä kokoonpanona tai yhdistelmänä ei ole tällaista tietoa tavanomaisesti käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa. Yleisesti tunnettua tietoa ovat esimerkiksi ilmeiset tiedot sekä tietyllä teollisuuden alalla tai liiketoiminnassa laajasti tunnetut tiedot.¹⁹⁰ Edelleen julkisesta lähteistä peräisin olevat tiedot, työntekijöiden ammattitaitoon ja kokemukseen kuuluvat tiedot sekä ei-salainen know-how, eivät ole salaisia. Se, että tiedon tulee olla salaista ei kuitenkaan edellytä absoluuttista salaisuutta, vaan tieto voi olla rajoitetun henkilöpiirin tiedossa. Liikesalaisuutena suojatun tiedon salaisuus on siten suhteellista, jolloin tieto voi olla tunnettu esimerkiksi useissa saman alan yrityksissä.¹⁹¹ Lisäksi tieto, joka on helposti saatavilla esimerkiksi käänteismallinnuksen avulla, ei voi olla liikesalaisuus. Tieto on helposti selville saatavissa, jos se voidaan selvittää esimerkiksi yksinkertaisella tuotteen tarkastelulla tai muilla vähäisillä resursseilla, kuten etsimällä julkisista lähteistä, verkkosivuilta tai alan julkaisuista.¹⁹² Kuitenkin, jos tieto on mahdollista saada käänteismallinnuksen avulla, mutta sitä ei ole vielä hankittu, tieto säilyy salaisena. Edelleen, vaikka tieto olisi saatu käänteismallinnuksen avulla, salaisuus voi säilyä, jos tieto ei ole levinnyt laajalle yleisölle.¹⁹³ IoT-tuotteen luonteen mukaan vaihtelee se, mitkä tiedot ovat alan ammattilaisten ja kehittäjien tiedossa tai helposti saatavilla. Tiedot, jotka kuuluvat IoT-tutkijoiden yleiseen tietämykseen, eivät kuulu liikesalaisuuksien piiriin.

IoT-laitteiden keräämä data ei ole yleensä salaista, jos se on peräisin ympäristöstä, joka on kaikkien saatavilla. Sama data voi olla muiden valmistajien kerättävissä ja analysoitavissa

¹⁸⁸ Sappa 2019, s. 409–410. Drexl 2017, s. 269 ja 291. Leistner 2020, s. 25.

¹⁸⁹ Drexl 2016, s. 24.

¹⁹⁰ WIPO 2024, s. 21–22.

¹⁹¹ HE 49/2018, s. 83 ja HE 114/1978 vp s. 114.

¹⁹² WIPO 2024, s. 21–22. Vapaavuori 2019, s. 68. WIPO 2024, s. 21. Kuitenkin, jos näiden tietojen avulla luodaan uusi kokonaisuus, se voi tulla suojatuksi liikesalaisuutena. Esimerkiksi lähdekoodi voi olla julkisesti saatavilla, mutta sen pohjalta kehitetty kokonaisuus, kuten ohjelmisto, voi olla salainen.

¹⁹³ Aplin 2014, s. 11–12.

esimerkiksi käänteismallinnuksen avulla.¹⁹⁴ Siten sensoreiden keräämä data ei ole salaista, jos se on kerätty paikasta, josta myös muut voivat hankkia sen, kuten älyauton tieltä keräämä data.¹⁹⁵ Jos data tai algoritmi on sisällytetty fyysiseen esineeseen, joka on yleisesti saatavilla, kuka tahansa voi periaatteessa analysoida sen toimintaa ja päästä käsiksi kyseiseen tietoon. Lisäksi avoimessa verkossa jaetun datan salaisuutta ei voida taata, koska kuka tahansa voi purkaa sen. Nämä seikat puhuvat sen puolesta, että IoT-laitteiden keräämä tai tuottama data ja siihen sisältyvät algoritmit eivät välttämättä ole salaisia.¹⁹⁶ Myös IoT-laitteiden monimutkainen toimintaympäristö ja ominaisuudet tekevät salaisuuden säilyttämisestä haastavampaa verrattuna perinteisempiin datan keräystapoihin¹⁹⁷. IoT-laitteiden automaattinen, dynaaminen ja reaaliaikainen tiedonkeruu tekee datan arvioinnista ja hallinnasta monimutkaisempaa. Koska sensorien keräämä data muuttuu jatkuvasti, liikesalaisuussuoja koskee koko ajan muuttuvaa datakokonaisuutta.¹⁹⁸

Toisaalta tiedon säilyminen salaisena riippuu erityisesti siitä, miten tietoa suojataan.¹⁹⁹ Näin ollen data voi olla salaista, vaikka sen lähde olisi täysin näkyvillä, koska datan tallentaminen ja käsittely voivat suojata sen salassapitoa²⁰⁰. Lisäksi tiedon salaisuus voi liittyä tietoon kokonaisuutena tai yhdistelmänä eikä sen yksittäisiin osiin. Tällöin yksittäisen datan paljastuminen ei poista tietokokonaisuuden salaisuutta.²⁰¹ Toisin sanoen liikesalaisuus voi perustua tiedon rakenteeseen eikä itse dataan, jolloin tiedon paljastuminen eri rakenteessa ei välttämättä poista sen salaisuutta. Vaikka osa tiedoista olisi paljastunut, data on edelleen taloudellisesti arvokasta, jos se tuottaa liikesalaisuuden haltijalle kilpailuetua.²⁰² Tämä on tärkeää erityisesti IoT-laitteiden kohdalla, jotka keräävät valtavasti dataa, josta osa voi olla julkista tai tulla julkiseksi paljastumisen myötä. IoT-laitteiden keräämää dataa voidaan suojata liikesalaisuutena suurina kokonaisuuksina. Jos suuren datakokonaisuuden osa paljastuu, se ei automaattisesti tarkoita, että tietojen katsottaisiin menettäneen salaisuutensa kokonaisuutena tai yhdistelmänä.

Tieto katsotaan yleisesti tunnetuksi, jos se on kaikkien alan toimijoiden tiedossa. Tiedon salassapidon arvioinnissa on tärkeää määritellä, kuinka laajasti tai suppeasti kyseinen ala

¹⁹⁴ Sappa 2018, s. 521. Ks. myös Noto La Diega – Sappa 2020, s. 437–439.

¹⁹⁵ Drexl 2017, s. 269. Sen sijaan suljetusta ympäristöstä kerätty data, kuten tehdaskoneen keräämä data, säilyy salaisena.

¹⁹⁶ Noto La Diega – Sappa 2020, s. 437–439.

¹⁹⁷ Noto La Diega 2022, s. 8. Manzo 2019, s. 9.

¹⁹⁸ Drexl 2018, s. 93.

¹⁹⁹ Sappa 2019, s. 415.

²⁰⁰ Fia 2022, s. 925–926.

²⁰¹ Drexl 2018 s. 93.

²⁰² Manzo 2019, s. 9. Drexl 2018, s. 93.

käsitetään. Laajasti tulkittuna tieto voi olla salaista, vaikka se olisi alalla sisäisesti tunnettu, kunhan se ei ole ulkopuolisten toimijoiden saavutettavissa. Esimerkiksi tieto voi olla salainen alalle pyrkivälle yritykselle. Liikesalaisuuden asema säilyy, jos tiedon salassapito tuo sen haltijalle kilpailuetua ja tieto tosiasiallisesti pidetään salassa.²⁰³ Toisaalta, jos liikesalaisuuksia sisältävää dataa on jaettu vain rajatulle joukolle ja sen salassapito on valvottavissa, salaisuus voi säilyä²⁰⁴. Toisaalta on esitetty, että salaisuus säilyy vain, jos liikesalaisuuksia sisältävää dataa on luovutettu vain *hyvin* rajalliselle määrälle kolmansia henkilöitä ja on siten liikesalaisuuden haltijan hallittavissa²⁰⁵. Siten ei ole tarkkaa rajaa sille, milloin tieto on tullut yleisesti tunnetuksi. Salaisuuden suhteellisuus tarkoittaa, että tieto voi pysyä salaisena, vaikka se olisi esimerkiksi lisensoitu.²⁰⁶ Laajamittainen lisensointi voi kuitenkin johtaa salaisuuden menettämiseen, jos salassapito ei ole tehokasta. On myös esitetty, että voitaisiin määrittää jokin tietty henkilömäärä, jonka jälkeen tieto katsotaan yleisesti tunnetuksi, vaikka nämä henkilöt pitäisivät sen salassa. Jos tieto on laajasti lisensoitu eikä salassapitoa voida valvoa, riski yleisesti tunnetuksi tulemisesta kasvaa.²⁰⁷ Toisaalta on myös esitetty, että tieto voi säilyttää salaisuutensa, jos edes yksi markkinoilla toimiva kilpailija ei voi saada sitä käyttöönsä tai selvittää sitä helposti²⁰⁸. Jos käyttäjät tekevät aktiivisesti datapyyntöjä ja kolmannet osapuolet keräävät dataa useilta käyttäjiltä, riski tiedon muuttumisesta yleisesti tunnetuksi kasvaa.

Tiedon säilyminen salaisena riippuu sekä haltijan omista toimenpiteistä että ulkoisista tekijöistä, kuten muiden yritysten suojatoimenpiteistä ja teknologian kehityksestä²⁰⁹. Uusien teknologioiden, kuten big datan, kehittyminen voi vaikeuttaa tiedon salassapitoa. Suuret datamäärät ja kehittyneet analyysityökalut helpottavat tiedon yhdistämistä ja analysointia, mikä kaventaa liikesalaisuuksien aluetta.²¹⁰ On mahdollista, että yhä harvempi tieto täyttää salaisuuden kriteerin, jos se katsotaan helposti selville saatavaksi esimerkiksi big data -analyysin avulla.

Tiedosta voi tulla julkista myös datan haltijan vapaaehtoisten toimien seurauksena. Esimerkiksi tekniselle liikesalaisuudelle voidaan hakea patenttia patenttilain (550/1967) nojalla. Tällöin tieto muuttuu julkiseksi, jos se täyttää edellytykset patentin myöntämiseksi. Yritykset voivat päätyä hakemaan patenttia silloin, kun ne arvioivat, että kilpailijat voivat saada liikesalaisuuden

²⁰³ Vapaavuori 2019, s. 129.

²⁰⁴ Wiebe - Schur 2019, s. 816.

²⁰⁵ Wiebe - Schur 2019, s. 816.

²⁰⁶ e Silva 2014, 11.

²⁰⁷ Meitinger - Burri 2014, s. 2–3. Liikesalaisuuden haltijoiden määrän rajoittaminen lisää oikeusvarmuutta ja auttaa pitämään salaisuuksien määrän hallittavana.

²⁰⁸ De Werra 2015, s. 170.

²⁰⁹ Meitinger - Burri 2014, s. 3.

²¹⁰ De Werra 2015, s. 171–172. Nordberg 2020, s. 217–218.

selville laillisin keinoin, kuten tutkimalla markkinoilla olevia tuotteita.²¹¹ Yleisesti yritykset haluavat patentoida erityisesti sellaisia tietoja tai innovaatioita, jotka ovat helposti saatavilla, purettavissa tai nähtävillä käyttäjille²¹². Siten liikesalaisuussuojan edellyttämä tiedon salaisuus-kriteeri voidaan ikään kuin kiertää hakemalla patenttia. Tämä voi kuitenkin johtaa oikeuskiistoihin siitä, kuka katsotaan keksinnön tekijäksi, jos tieto on saatu esimerkiksi käänteismallinnuksen avulla liikesalaisuuden haltijalta.²¹³ Datasäädöksen velvoitteet voivat vaikuttaa yritysten strategioihin, jotka koskevat aineettoman varallisuuden suojaamista. Jos datasäädöksen seurauksena liikesalaisuuksien paljastuminen vaikuttaa todennäköisemmältä, tämä voi lisätä yritysten halukkuutta patentoida teknisiä liikesalaisuuksia.

3.2.3 Tiedon taloudellinen arvo

Toiseksi tiedolla on oltava taloudellista arvoa sen salaisuuden vuoksi, jotta se voi saada liikesalaisuussuojaa. Kyse on salassapitointressistä eli siitä, että tieto antaa haltijalleen kilpailuetua, koska se ei ole yleisesti tiedossa tai helposti selville saatavissa. Vastaavasti tiedon luvaton hankkiminen, käyttäminen tai paljastaminen voisi aiheuttaa sen haltijalle taloudellista vahinkoa.²¹⁴ Siten tiedon salaisuuden ja kaupallisen arvon välillä on oltava selvä syy-yhteys.²¹⁵ Kausaalisuhteen täyttyminen on osa taloudellisen arvon edellytystä, joten kriteeri ei täyty, jos tieto on kaupallisesti arvokasta datan haltijalle jostain muusta syystä. Esimerkiksi tekoälyn kehittämisessä hyödynnettävät tietokannat voivat olla kaupallisesti arvokkaita, mutta niiden arvo ei perustu salaisuuteen, jos ne on koottu julkisista lähteistä²¹⁶.

Pelkkä subjektiivinen salassapitointressi ei ole riittävää, vaan tiedolla on oltava myös objektiivisesti arvioituna taloudellista arvoa. Taloudellinen arvo voi ilmetä esimerkiksi siten, että tietoa hyödynnetään nykyisessä tai tulevassa elinkeinotoiminnassa. Jälkimmäisessä tapauksessa kyse on tiedon potentiaalisesta taloudellisesta arvosta, joka ei ole vielä aktualisoitunut. Vähäpätöinen tai vanhentunut tieto ei pääsääntöisesti voi saada liikesalaisuussuojaa.²¹⁷ Taloudellisen arvon voi osoittaa viittaamalla väärinkäyttöön, joka usein paljastaa liikesalaisuuden kaupallisen arvon. Mikäli väärinkäyttöä ei ole tapahtunut,

²¹¹ Vapaavuori 2019, s. 43–44.

²¹² Sandeen - Aplin 2021, s. 13.

²¹³ e Silva 2024, s. 16. On epäselvää, voiko henkilö, joka on saanut toisen liikesalaisuuden selville esimerkiksi käänteismallinnuksen avulla hakea patenttia ja tulla näin keksijäksi.

²¹⁴ Liikesalaisuusdirektiivin johdannon (14) mukaan – ”tiedolla olisi katsottava olevan kaupallista arvoa esimerkiksi silloin, kun sen luvaton hankinta, käyttö tai ilmaiseminen *todennäköisesti* vahingoittaisi sen suhteen laillista määräysvaltaa käyttävän henkilön etuja siten, että se heikentää kyseisen henkilön tieteellistä ja teknistä suorituskykyä, vahingoittaa hänen liiketoiminnallisia tai taloudellisia etujaan taikka heikentää hänen strategiaa asemaansa tai kilpailukykyään.”

²¹⁵ Drexl 2016, s. 23.

²¹⁶ Sandeen -Aplin 2021, s. 10–13. Lisäksi taloudellinen arvo ei perustu salassapitoon, jos data on kerätty julkisesta lähteestä. Radauer – Bader - Aplin ym. 2022, s. 79.

²¹⁷ HE 49/2018 s. 83–84. Vapaavuori 2019, s. 81.

datan haltija voi osoittaa arvon esimerkiksi investoinneilla tai sillä, että hän on hyödyntänyt dataa liiketoiminnassaan.²¹⁸

Liikesalaisuusdirektiivi ei edellytä, että tiedon taloudellisen arvon tulisi olla merkittävä. Onkin katsottu, että kyseessä on eräänlainen *de minimis* -vaatimus eli riittää, että tieto antaa sen haltijalle kilpailuetua ja sen arvo johtuu salassapidosta. Tiedolla ei ole taloudellista arvoa sen paljastumisen jälkeen, vaikka se olisi edelleen hyödyllistä haltijalle. Taloudellinen arvo on sitä suurempi, mitä enemmän hyötyä tiedosta voidaan saada tai mitä suurempia haittoja sen paljastuminen aiheuttaisi. Toisaalta, jos tiedon hankkiminen on vaikeaa, sen arvo on tyyppillisesti suurempi.²¹⁹ Lisäksi tieto voi olla hyödyllistä yritykselle esimerkiksi tehostamalla tuotantoprosessia, vaikka se ei suoraan lisäisi yrityksen voittoa.²²⁰ Siten ei-kaupalliset tiedot voivat olla myös taloudellisesti arvokkaita²²¹. Rajallisesti liikesalaisuutena voidaan suojata myös yhdistelmäliikesalaisuuksia, jotka koostuvat julkisesti saatavilla olevasta tiedosta, jotka on koottu ja järjestetty ainutlaatuisella tavalla²²².

Raakadatan taloudellinen arvo on usein vähäinen eikä yksittäinen data todennäköisesti täytä liikesalaisuuden suojan edellytyksiä.²²³ Esimerkiksi älykellon keräämät yksittäiset mittaukset tai teollisuuskäytössä olevan laitteen tuottamat luvut eivät tavallisesti ole taloudellisesti arvokkaita ilman yhteyttä muuhun dataan. Liikesalaisuusdirektiivin sanamuoto ja tavoitteet tukevat tätä tulkintaa. Liikesalaisuusdirektiivin tarkoituksena on lisätä tiedon jakamista ja innovointia, mitä yksittäisen datan suojaaminen ei yleensä edistä.²²⁴ Sen sijaan tietojen yhdistelmät, kuten koneiden tai tuotteiden keräämät datakokonaisuudet, voivat olla taloudellisesti arvokkaita ja siten oikeutettuja liikesalaisuussuojaan²²⁵. Liikesalaisuussuojaa voidaan siis myöntää datakokoelmille tai niiden yhdistelmille, mutta poikkeuksellisesti myös yksittäiset tiedot voivat saada suojaa. Esimerkiksi teollisessa prosessissa käytettävä kriittinen

²¹⁸ Aplin 2014, s. 10. Ratkaiseva merkitys taloudellisen arvon todentamisessa on vain suoralla näytöllä, kuten lisensointimaksuilla ja liikesalaisuuden käytöstä saaduilla lisätuloilla. Välillistä näyttöä voivat olla esimerkiksi investoinnit datan jalostamiseen. Radauer – Bader - Aplin ym. 2022, s. 78. Tieto on taloudellisesti arvokasta, jos se palvelee sen haltijan etuja eikä se riipu suoraan investoinneista, joita on tehty sen hankkimiseksi. Sappa 2019, s. 415.

²¹⁹ e Silva 2014, s. 18

²²⁰ Burri- Meitinger 2014, s. 3.

²²¹ De Werra 2015, s. 54.

²²² Graves – Macgillivray 2004, s. 261. Oikeuskirjallisuudessa on katsottu, että yhdistelmäliikesalaisuus ei voi olla ilmeinen, sen osien tulee liittyä toisiinsa toiminnallisesti ja sen tulee olla taloudellisesti arvokas eli arvokkaampi kuin osiensa summa. Tiukka tulkinta on perusteltua, koska se vähentää esteitä julkisen tiedon saatavuudelle.

²²³ Liikesalaisuusdirektiivin johdanto (14). Aplin - Radauer ym. 2023, s. 843.

²²⁴ Noto La Diega – Sappa 2020, s. 18–20. Drexl 2018, s. 92–93. Ks. myös Zech 2016, s. 6.

²²⁵ Komissio 2017b. Zech 2017, s. 2. Datan kerääminen, tallentaminen, analysointi ja uudelleenkäyttö muodostavat arvoketjun, jossa raakadata muuttuu kaupalliseksi hyödykkeeksi.

lämpötilakynnysarvo voi olla taloudellisesti merkittävä ja ansaita suojaa.²²⁶ Raakadata voi olla taloudellisesti arvokasta myös, jos se on ainutlaatuista, vaikeasti saatavissa tai sillä on erityinen yhteys tiettyyn kohteeseen, paikkaan, henkilöön tai organisaatioon. Lisäksi raakadata voi täyttää liikesalaisuuden edellytykset esimerkiksi, jos sen keräämiseen on käytetty patentoitua keksintöä tai muuta omistusoikeudella suojattua teknologiaa.²²⁷

Liikesalaisuussuoja voi koskea sekä useista laitteista kerätyn datan yhdistelmää että yksittäisen laitteen keräämän datan muodostamaa kokonaisuutta. Useista laitteista kerätty data on yleensä taloudellisesti arvokkaampaa kuin yhden laitteen keräämä tai tuottama data. Kuitenkin jo yksittäisen laitteen keräämän datan yhdistelmät voivat salaisuutensa ansiosta parantaa valmistajien kilpailukykyä markkinoilla. Näin on erityisesti, jos kyse on teknisestä tiedosta, jota käytetään verkkoon liitettyjen tuotteiden kehittämiseen tai jälkimarkkinapalveluiden tarjoamiseen. Lisäksi valmistaja voi harjoittaa liiketoimintaa keräämällä ja myymällä analysoitua dataa toissijaisilla markkinoilla.²²⁸ Taloudellisen arvon kannalta ei ole ratkaisevaa, onko datalle jo olemassa markkinat, vaikka monille verkkoon liitettyistä laitteista peräisin oleville datatyypeille on jo muodostunut markkinat²²⁹.

Lisäksi salassapidon ja taloudellisen arvon syy-yhteyden tulkintaan liittyy tulkinnanvaraisuutta. Laajan tulkinnan mukaan taloudellinen arvo voi perustua osittain datan analysointimahdollisuuksiin ja osittain siihen, että tieto tuottaa kilpailuetua sen salaisuuden vuoksi²³⁰. Toisin kuin liikesalaisuusdirektiivi olettaa, yksittäinen triviaalina pidetty tieto, voi muuttua arvokkaaksi, kun tietoa kerätään ja analysoidaan riittävän suuria määriä.²³¹ Siten tiedon taloudellinen arvo ei välttämättä perustu yksinomaan sen salaisuuteen. Sen arvo voi olla yhdistelmä analysoinnista syntyvää hyötyä ja kilpailuetua, joka saadaan tietojen pysyessä salassa.

Raakadata voi olla potentiaalisesti arvokasta, koska siitä voidaan löytää merkittäviä korrelaatioita esimerkiksi big data -analytiikan avulla. Kausaalisuhteen ei tarvitse ulottua kaikkiin yksittäisiin datan osiin, vaan riittää, että tieto on kokonaisuutena taloudellisesti

²²⁶ Komissio 2016, s. 10.

²²⁷ WIPO 2024, s. 132–133.

²²⁸ Drexl 2018, s. 94.

²²⁹ Komissio 2017b. Radauer – Bader – Aplin ym., s. 78.

²³⁰ Wiebe – Schur 2019, s. 817. Argumentoi sen puolesta, että salassapidon ja arvon välinen kausaalisuhde ei ole välttämättä tiukasti määritelty.

²³¹ Zech 2017, s. 6. Nordberg 2020, s. 217.

arvokasta sen salaisuuden vuoksi.²³² Liikesalaisuussuojaa ei kuitenkaan tulisi antaa niin sanotuille "mustan laatikon tiedoille" (eng. *black box*), jotka viittaavat tietoihin, joiden sisältöä tai hyötyä datan haltija ei tunne. Myös IoT-tuotteet voivat sisältää tietoja, jotka ovat monimutkaisia ja testaamattomina tai analysoimattomina niiden haltijalle tuntemattomia. Mustan laatikon tiedot eivät yleensä tarjoa niiden haltijalle kilpailuetua, mutta ne voivat myöhemmin osoittautua taloudellisesti arvokkaiksi. Tästä syystä on esitetty, että vain tiedon haltijalle ymmärrettävät ja hallittavissa olevat tiedot voivat olla taloudellisesti arvokkaita. Lisäksi voidaan väittää, että mustan laatikon tiedot eivät tuota kilpailuetua, koska datan haltija ei tunne niiden arvoa. Tästä seuraa, että datan väärinkäyttö ei myöskään aiheuta vahinkoa tiedon haltijalle.²³³ Oikeuskirjallisuudessa on esitetty, että potentiaalinen arvo tulisi määritellä datan luovutushetken perusteella. Tietoa ei voida jälkikäteen pitää arvokkaana, ellei sitä jo luovutushetkellä pidetty potentiaalisesti taloudellisesti arvokkaana.²³⁴ Näin ollen, jos tietoa ei alun perin arvioitu arvokkaaksi, sitä ei voida myöhemmin väittää potentiaalisesti arvokkaaksi.

Datasäädöksen soveltamisessa voi syntyä tilanteita, joissa datan haltija ei pysty etukäteen arvioimaan, onko jokin data taloudellisesti arvokasta. Ennen raakadatan analysointia voi olla mahdotonta tietää sen arvoa. Datan haltijan riskinä on, että esimerkiksi kolmas osapuoli analysoi dataa ja kehittää sen pohjalta mullistavan innovaation ilman, että datan alkuperäinen saa siitä hyötyä. Tästä syystä datan haltijalle voi olla edullisempaa suojata mieluummin liikaa kuin liian vähän dataa, jos data voi olla potentiaalisesti arvokasta. Liian laaja tulkinta, jossa vähäarvoiset tiedot nähdään arvokkaina analysoitavuuden perusteella, on ongelmallista, sillä yksittäinen data tai raakadata ei yleensä ole taloudellisesti arvokasta²³⁵. Vaikutusta lieventää se, että yksittäiset tiedon osat tai osat yhdistelmistä voivat olla julkisia, vaikka tietty kokonaisuus voi saada liikesalaisuussuojaa²³⁶. Siten liian laaja tulkinta suojan kohteeksi kelpaavista tiedoista on ristiriidassa direktiivin kanssa. Lisäksi datan haltijalle ei tulisi olla mahdollista väittää tiedon olevan potentiaalisesti arvokasta sen saataville asettamisen jälkeen, vaikka esimerkiksi kolmas osapuoli löytäisi datasta jokin arvokkaan korrelaation, jota datan haltija ei ole tunnistanut luovutushetkellä.

²³² Sappa 2018, s. 521. Drexl 2018, s. 30–32. Aracı 2019, s. 30–32. Ks. Nordberg 2020, s. 195. Big data tarkoittaa suurten data-aineistojen tietokonepohjaista käsittelyä, jossa korostuvat tilavuus, nopeus, monimuotoisuus ja datan luotettavuus.

²³³ Noto La Diega – Sappa 2020, s. 440–441. Tietoja, jotka ovat datan haltijalle tuntemattomia tai salattuja, voivat olla esimerkiksi päätöksentekomallin säännöt.

²³⁴ Radauer – Bader – Aplin ym. 2022, s. 79.

²³⁵ Fia 2022, s. 926. Wiebe 2017, s. 65.

²³⁶ Sandeen - Aplin 2021, s. 12.

3.2.4 Kohtuulliset toimenpiteet tiedon salassa pitämiseksi

Kolmanneksi liikesalaisuussuojaa voi saada vain tieto, jonka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin tiedon salassa pitämiseksi. Tämä kattaa erilaisia toimia, kuten fyysiset, tekniset ja organisatoriset toimenpiteet sekä oikeudenloukkauksiin puuttuminen. Se, kuinka salaisena tiedon pitää pysyä, jotta olisi ryhdytty kohtuullisiin toimenpiteisiin, ei voida tarkasti määritellä. Tiedon salaisuuden asteeseen vaikuttavat muun muassa tiedon luonne, kilpailutilanne ja liikesalaisuuden haltijan suhteet muihin tahoihin.²³⁷ Ennen kohtuullisiin toimiin ryhtymistä, on määriteltävä suojattava tieto eli yksilöitä liikesalaisuudet.²³⁸ Kohtuullisten toimenpiteiden on tarkoitus paitsi pitää tieto salassa, myös osoittaa liikesalaisuuden haltijan ulkopuolisille, että tieto on salassa pidettävää. Se, onko ryhdytty kohtuullisiin toimenpiteisiin vaikuttaa muun muassa siihen, voiko kolmas osapuoli saada vilpittömän mielen suojaa liikesalaisuuden väärinkäyttötilanteessa²³⁹. Kohtuullisten toimenpiteiden vaatimusta on pidetty liikesalaisuuden määritelmän haastavimpana kriteerinä, koska lainsäädäntö jättää sen tarkoituksella avoimeksi²⁴⁰. Oikeuskäytännössä kohtuullisten toimenpiteiden määrittely on osoittautunut olennaiseksi kriteeriksi. Yksi yleisimmistä puolustuksista liikesalaisuusriidoissa on väite siitä, että kantaja ei ole ryhtynyt riittäviin toimenpiteisiin liikesalaisuutensa suojaamiseksi.²⁴¹

Kohtuullisten toimenpiteiden edellytys ilmentää suhteellisuusperiaatetta. Toimenpiteiden arvioinnissa on kyse olosuhteiden kokonaisharkinnasta, jossa voidaan huomioida muun muassa tiedon arvo ja luonne, tiedon saatavuus ja yleinen tunnettuus, suojaustoimenpiteiden toteutettavuus, tiedon säilytystapa, tiedon jakaminen, suojaamiskeinot ja niiden jatkuvuus, toimialan käytännöt, liikesuhteiden rakenne, reagoiminen tietovuotoihin sekä yrityksen suhtautuminen tiedon salaisuuteen.²⁴² Mitä arvokkaampi tieto on kyseessä, sitä tiukemmin suojatoimenpiteitä arvioidaan. Käytännössä tulee ottaa huomioon, mitä suojakeinoja on mahdollista käyttää ja niiden kustannukset suhteessa tiedon arvoon.²⁴³ Kohtuutonta olisi vaatia

²³⁷ Vapaavuori 2019, s. 68–69. Myös Vapaavuori 2019, s. 87. Käytännössä liikesalaisuuden suojaamiskeinoja ovat muun muassa salassapitosopimukset, salassapidon korostaminen organisaation sisäisesti, tietotekniset ratkaisut, kuten käyttäjätunnukset ja salasana, sekä fyysiset suojatoimet, kuten lukitus ja kameravalvonta. Lisäksi yritysten tulee puuttua mahdollisiin ja jo tapahtuneisiin tietovuotoihin välittömästi. Liikesalaisuuden suoja edellyttää tapauskohtaista ja kokonaisvaltaista lähestymistapaa, jossa tiedon luonne, käyttöympäristö ja muut soveltamistilanteet voivat vaihdella

²³⁸ e Silva 2014, s. 21.

²³⁹ Radauer – Bader – Aplin ym. 2022, s. 80.

²⁴⁰ Aplin – Radauer – Bader – Searle 2023, s. 844–845.

²⁴¹ EUIPO 2023 s. 64. Tämä puolustus on menestynyt 59 %:ssa tapauksista, ja 23 %:ssa tapauksista kantajan vaatimus hylättiin tällä perusteella.

²⁴² KKO 2013:17. Vapaavuori 2019, s. 85–94.

²⁴³ Burri – Meitinger 2014, s. 3. Esimerkiksi vähemmän arvokkaat tiedot voivat vaatia vain perustason suojaa, kun taas arvokkaampia tietoja tulee suojata edistyneillä suojamekanismeilla. Radauer – Bader – Aplin ym. 2022, s. 80–81.

toimenpiteitä, joiden kustannukset ylittävät kilpailuedun, jonka liikesalaisuuden salassapito tuo sen haltijalle²⁴⁴. Esimerkiksi EU-tuomioistuimen asiassa C-355/12 otettiin huomioon kustannukset, teknologian käytettävyys ja toimenpiteiden tehokkuus teknologisten suojatoimenpiteiden määrittelyssä²⁴⁵. Toimenpiteiden arvioinnissa voidaan ottaa huomioon liikesalaisuuden arvo, rikkomuksen todennäköisyys ja teknologian kehitys.²⁴⁶ Kohtuullisten toimenpiteiden vaatimusta tulisi tulkita laajasti, sillä laaja tulkinta kannustaa yrityksiä jakamaan dataa ja vähentämään datan jakamisesta aiheutuvia transaktiokustannuksia, mikä on myös liikesalaisuussuojan tavoite²⁴⁷.

Kohtuullisten toimenpiteiden arvioinnissa voidaan ottaa huomioon sekä subjektiivisia seikkoja, kuten liikesalaisuuden haltijan olosuhteet ja toimenpiteiden kustannukset, että objektiivisia seikkoja, kuten yleiset standardit ja alan käytännöt²⁴⁸. Mitä kehittyneempi organisaatio on, sitä vaativampia ja monimutkaisempia suojatoimenpiteitä sen voidaan odottaa käyttävän²⁴⁹. EU-tuomioistuin ei ole toistaiseksi ottanut kantaa siihen, mitä seikkoja liikesalaisuuksien suojaamiseksi toteutetuissa kohtuullisten toimenpiteiden arvioinnissa tulisi erityisesti huomioida. Oikeuskirjallisuudessa on kuitenkin arvioitu, että EU-tuomioistuin saattaa omaksua Yhdysvaltojen tavoin suhteellisen ja kontekstuaalisen lähestymistavan. Lisäksi voidaan soveltaa matalaa objektiivista vähimmäiskynnystä, kuten salassapitosopimusten tai teknisten suojatoimenpiteiden käyttöä.²⁵⁰

Kohtuulliset toimenpiteet sisältävät tietojen suojaamisen sekä yrityksen sisällä että ulkopuolisia tahoja vastaan. Datasäädös korostaa toimenpiteiden tärkeyttä, erityisesti ulkopuolisten väärinkäytöksiltä ja paljastumiselta suojautumisessa, sillä se velvoittaa jakamaan dataa käyttäjille ja valitsemilleen kolmansille osapuolille. Kohtuulliset toimenpiteet voivat sisältää esimerkiksi dokumentointia pääsyoikeuksista, salassapitosopimuksia osapuolten välillä sekä teknologisia ratkaisuja, kuten palomureja, pääsyn rajoittamista, verkkosivustojen ja ulkoisen liikenteen kontrollointia sekä tiedonsiirtojen kirjaamista. Pilvipalveluissa suojatoimenpiteet voivat sisältää muun muassa tiedon salaamista ja palvelusopimuksia.²⁵¹

²⁴⁴ e Silva, 2014, s. 18–20.

²⁴⁵ Asia C-355/12 *Nintendo* kohta 33 ja 38. Suunta-antavana voi käyttää tätä EU-tuomioistuimen tapausta, joka koski kohtuullisia toimenpiteitä tietoyhteiskuntadirektiivin 6 artiklaa koskevassa tapauksessa.

²⁴⁶ Wiebe – Schur 2019, s. 817–818.

²⁴⁷ Leistner 2020, s. 233.

²⁴⁸ Aplin 2014, s. 10–11.

²⁴⁹ Radauer – Bader - Aplin ym. 2022, s. 80–81.

²⁵⁰ Radauer – Bader - Aplin ym. 2022, s. 80 ja 95.

²⁵¹ Mata 2018, s. 29–31. Sandeen- Aplin 2021, s. 17

Kohtuullisten toimenpiteiden arvioinnissa tulisi ottaa huomioon teknologian erityispiirteet ja erilaiset tavat, joilla dataa voi syntyä. IoT-teknologioissa dataa syntyy monista lähteistä, kuten sensoreista tai käyttäjien antamista syötteistä, mikä lisää tiedon hallinnan monimutkaisuutta.²⁵² IoT-laitteet keräävät ja siirtävät usein suuria määriä tietoa ja muodostavat verkon, joka on erityisen altis tietoturvahkille²⁵³. Oikeuskirjallisuudessa on esitetty, että kohtuullisia toimenpiteitä tulisi arvioida tiukemmin uusien teknologioiden kohdalla. Tämä johtuu siitä, että ne tekevät datan hallinnasta vaikeampaa, mikä edellyttää tiedon haltijalta erityistä huolellisuutta.²⁵⁴ Datasäädös voi lisätä tarvetta arvioida kohtuullisia toimenpiteitä tiukemmin, erityisesti silloin, kun tiedon paljastumisen riski kasvaa. Tämä edellyttää yrityksiltä datan jakamisen dokumentointia liikesalaisuuksien suojaamiseksi, kuten selkeitä sopimuksia ja teknisiä ratkaisuja, jotka vastaavat datan erityispiirteisiin ja riskitasoihin.

3.2.5 Liikesalaisuuksien yksilöinti

Datasäädöksen mukaan datan haltijan on yksilöitävä data, jota voidaan suojata liikesalaisuutena. Lisäksi datan jakamisesta pidättäytyminen tai sen keskeyttäminen edellyttää, että datan haltija yksilöi, mitä toimenpiteitä ei ole sovittu tai pantu täytäntöön sekä tapauksen mukaan, minkä liikesalaisuuksien luottamuksellisuus on vaarantunut²⁵⁵. Siten liikesalaisuudet tulee yksilöidä ennen liikesalaisuuksia sisältävän datan jakamista. Lisäksi, jos datan haltija haluaa myöhemmin vedota liikesalaisuussuojaan, sen tulee näyttää, minkä liikesalaisuuksien luottamuksellisuus on vaarantunut.

Liikesalaisuuksiin liittyy tunnistusongelma, koska niitä ei rekisteröidä. Lisäksi suoja menetetään tiedon paljastuessa²⁵⁶. Liikesalaisuuksien tunnistaminen on usein vaikeaa, koska liikesalaisuudet voivat olla laajoja ja vaikeasti rajattavia²⁵⁷. IoT-laitteet keräävät ja siirtävät valtavia määriä jäsentymätöntä raakadataa, jossa yksittäiset tietorivit eivät yleensä ole itsessään merkityksellisiä²⁵⁸. Tämän takia voi olla vaikea määrittää, mikä osa datasta muodostaa liikesalaisuuden. Lisäksi vain osa IoT-datasta saattaa olla suojattavissa, koska se voi sisältää

²⁵² Mata 2018, s. 29–31.

²⁵³ Hye - Rhee 2024, s. s.92–93.

²⁵⁴ Manzo 2019, s. 8–10. Pilvipalveluiden käyttö heikentää liikesalaisuuksien hallintaa, sillä tieto siirtyy osittain ulkopuoliseen valvontaan. Hernandez Gonzalez 2013, s. 248. Ks. myös Rowe 2009, s. 1–2. Uusien teknologioiden käyttö lisää liikesalaisuuksien paljastumisriskiä, sillä tiedon hallinta vaikeutuu ja sen säilyttäminen, käyttö ja siirtäminen helpottuvat. Tämä vaatii salaisuuden haltijalta entistä suurempaa huolellisuutta, sillä uudet teknologiat voivat osaltaan edesauttaa tietojen vuotamista. Myös Schiller – Aidoo – Fuhrer 2022, s. 15. IoT-laitteiden ominaisuuksien vuoksi perinteisten suojatoimenpiteiden, kuten monimutkaisten salaustekniikoiden käyttö, ei ole riittävää.

²⁵⁵ Datasäädös 4 artikla 6 kohta ja 5 artiklan 9 kohta.

²⁵⁶ Menell – Almeling – Cundiff ym. 2023, s.1–3.

²⁵⁷ Aplin 2024, s. 88.

²⁵⁸ IPR University 2023b. Käytännössä tulee olemaan vaikeaa erottaa raakadatasta ne osat, jotka voivat muodostavat liikesalaisuuden. IoT -tuotteet voivat tuottaa useita gigatavuja raakadataa lyhyessä ajassa.

myös julkisesti saatavilla olevaa tai helposti saavutettavissa olevaa tietoa. Liikesalaisuuden yksilöinti ei vielä osoita, että tiedot todella olisivat liikesalaisuuksia. Siten yksilöinti on muodollinen vaihe, joka ilmentää esimerkiksi datan haltijan käsitystä tiedon liikesalaisuusluonteesta. Lopullinen oikeudellinen arviointi tietojen liikesalaisuusluonteesta tehdään tuomioistuimessa ex post.²⁵⁹

Liikesalaisuuksien yksilöinti liittyy tiiviisti liikesalaisuuden määritelmään. Liikesalaisuuden haltijan tulee yksilöidä liikesalaisuudet ennen kuin se ryhtyy liikesalaisuusdirektiivin 2 artiklan 1 kohdan c alakohdan mukaisiin kohtuullisiin toimenpiteisiin salaisuuden säilyttämiseksi. Liikesalaisuuksien yksilöinti on siten edellytys sille, että kohtuulliset toimenpiteet voidaan toteuttaa tehokkaasti.²⁶⁰ Yksilöinnissä on kyse siitä, että liikesalaisuuden haltija ikään kuin suodattaa liikesalaisuudet muusta datasta²⁶¹. Tästä esimerkkinä on EU:n yleisen tuomioistuimen tapaus T-235/15 (*PariPharma v. EMA*), jossa tietokokonaisuutta ei voitu automaattisesti pitää luottamuksellisena²⁶².

Liikesalaisuuden yksilöintiin liittyy kysymyksiä siitä, kuinka paljon tietoa muodostaa yhden liikesalaisuuden ja kuinka suuri tietokokonaisuus voi olla yksi liikesalaisuus tai useita liikesalaisuuksia. Liikesalaisuuden määritelmä liikesalaisuusdirektiivissä ei sisällä suojattavan tiedon vähimmäis- tai enimmäisvaatimuksia. Tämä tarkoittaa, että liikesalaisuus voi olla yksinkertainen tieto, kuten luku tai lause sekä laaja kokonaisuus, kuten asiakaslista. On epäselvää, miten yksittäinen datakohde määritellään. Kyse voi olla siitä, kuinka pitkä bittijono muodostaa yhden dataelementin. Koska yleispätevää vastausta näihin kysymyksiin ei ole olemassa, liikesalaisuuden rajoja on tarkasteltava tapauskohtaisesti. Liikesalaisuuden muodostavan datan vähimmäismäärää koskevaa kysymystä olennaisempaa on arviona, milloin tietojen yhdistelmä tai kokoonpano voi saada suojaa.²⁶³ Siten liikesalaisuudeksi voidaan yksilöidä tietoja niiden laajuudesta riippumatta, kunhan laissa säädetyt edellytykset täyttyvät.²⁶⁴ Tähän viittaa myös se, että liikesalaisuuden kohde voi olla hyvin laaja ja periaatteessa mikä tahansa tieto saada suojaa²⁶⁵. Siten liikesalaisuudelle ei ole olemassa yleisesti hyväksyttyjä rajoja²⁶⁶. Liikesalaisuudeksi katsottavan tiedon vähimmäis- tai

²⁵⁹ Menell – Almeling – Cundiff ym. 2023, s. 3–4.

²⁶⁰ EUIPO 2023, s. 67–69.

²⁶¹ e Silva 2014, s. 21. Radauer – Bader – Aplin ym. 2022, s. 80.

²⁶² Ks. myös EU yleisen tuomioistuimen ratkaisu T-235/15 (*PariPharma v.EMA*) kohdat 76–86 ja 107, jossa koko CHMP-raportin sisältöä ei voitu pitää automaattisesti luottamuksellisena, vaan kantajan oli yksilöitävä ja osoitettava ne tiedot, joiden paljastuminen vaarantaisi sen taloudelliset edut.

²⁶³ Fia 2022, s. 926–927. Laaja datakokonaisuutta voidaan periaatteessa suojata samanaikaisesti sekä liikesalaisuutena että sui generis -tietokantasuojan alla.

²⁶⁴ Vapaavuori 2019 s.135–137.

²⁶⁵ e Silva, 2014, s. 3.

²⁶⁶ Searle 2021, s. 17.

enimmäismäärästä ei voi antaa yleispätevää määritelmää, vaan on tarkasteltava tapauskohtaisesti, täyttääkö tietty tietokokonaisuus liikesalaisuuden määritelmän.

Koska liikesalaisuudet voivat olla hyvin erilaisia, niiden tunnistamiselle ei ole olemassa yleistä muotoa²⁶⁷. Suositeltavaa on, että yksilöinti tehdään ensisijaisesti kirjallisesti. Esimerkiksi salassapitosopimuksessa voidaan määritellä tarkasti ne tiedot, joita pidetään liikesalaisuuksina. Lisäksi yksilöinti voi perustua myös osapuolten vakiintuneisiin kaupallisiin käytäntöihin, jolloin osapuolilla on yhteinen ymmärrys siitä, mitä pidetään liikesalaisuutena.²⁶⁸ Yksilöinnin muotoa olennaisempi kysymys liittyy kuitenkin siihen, kuinka tarkasti yksilöinti tulee tehdä. Oikeuskirjallisuudessa on esitetty, että asiakirjat ja tiedostot tulisi järjestää numeroidusti ja mahdollisissa muutoksissa numerointijärjestelmä tulisi säilyttää. Pelkkä viittaus asiakirjaan riittää, ellei koko asiakirjan sisältöä pidetä liikesalaisuutena. Lisäksi yksittäiset liikesalaisuudet tulisi osoittaa asiakirjan sisällä. Jos asiakirjassa on useita liikesalaisuuksia, on tarkennettava, mikä osa asiakirjasta liittyy kuhunkin liikesalaisuuteen.²⁶⁹ Yhdistelmäliikesalaisuuksien osalta on tärkeää selvittää, miten julkiset tai ei-salaiset tiedot yhdistyvät ainutlaatuisella tavalla, joka luo taloudellista arvoa. Negatiiviset liikesalaisuudet voidaan puolestaan yksilöidä kuvaamalla esimerkiksi toimimattomaksi todetut valmistusmenetelmät ja viittaamalla tutkimus- ja kehitystyöhön.²⁷⁰

Toisaalta yksilöinnin tarve voi tulla ajankohtaiseksi myöhemmin, jos liikesalaisuuden haltija hakee esimerkiksi kiello- tai korjaavia toimenpiteitä tietojensa suojaamiseksi. Tällöin on tarpeen yksilöidä ne liikesalaisuudet, joiden väitetään olevan vaarassa tai joita on loukattu.²⁷¹ Datasäädöksessä säädetty mahdollisuus keskeyttää datan jakaminen liikesalaisuuksien suojaamiseksi, voidaan rinnastaa tuomioistuimen määräämään väliaikaiseen kieltoon. Riittämätön yksilöinti voi johtaa esimerkiksi kieltihakemuksen hylkäämiseen.²⁷² Tähän liittyy kysymys siitä, kuinka tarkasti liikesalaisuudet tulee yksilöidä tuomioistuimessa. Prosessiekonomisista syistä oikeudenkäynneissä ei ole mahdollista yksilöidä jokaista liikesalaisuutta erikseen. Aineiston laajuus vaikuttaa siihen, millä tarkkuudella yksilöinti tulee tehdä. Suppeassa aineistossa voidaan tarkastella esimerkiksi asiakirja kerrallaan, muodostaako

²⁶⁷ Menell – Almeling – Cundiff ym. 2023, s. 4.

²⁶⁸ EUIPO 2023, s. 67–69.

²⁶⁹ Menell – Almeling – Cundiff ym. 2023, s. 7–10.

²⁷⁰ Menell – Almeling – Cundiff ym. 2023, s. 10–12.

²⁷¹ EUIPO 2023, s. 90.

²⁷² Esimerkiksi MAO 398/20, jossa kantaja väitti, että kaupallinen käsikirjoitus sisälsi liikesalaisuuksia, mutta ei yksilöinyt sen sisältöä selkeästi. Vastaavasti MAO 232/2023 kantaja ei osoittanut, että vastaaja olisi oikeudettomasti käyttänyt mitään liikesalaisuuksia, koska käyttäjätunnuksia ja salasanoja ei ollut selkeästi yksilöity liikesalaisuuksiksi. Tapauksessa MAO H71/2022 väliaikainen kiello hylättiin, koska kantajan vaatimus ei ollut riittävän yksilöity, erityisesti kantajan oikeuden loukkauksen tai sen välittömän toteutumisen osalta.

kyseinen asiakirja liikesalaisuuden. Laajassa aineistossa ei edellytetä niin yksityiskohtaista tarkastelua, vaan huomiota voi kiinnittää suurempiin kokonaisuuksiin. Käytännössä yksilöinti voi tapahtua esimerkiksi antamalla edustavia esimerkkejä liikesalaisuuksista.²⁷³ Yksilöinnin riittävyyttä arvioitaessa huomioidaan, täyttyvätkö sen tavoitteet, kuten se, että osapuolet voivat valmistautua tasapuolisesti prosessiin ja, että tuomioistuin tai viranomainen voi arvioida väitetyn väärinkäytön tarkasti.²⁷⁴ Toisaalta liian tiukat yksilöintivaatimukset voivat johtaa tahattomiin tietovuotoihin tai luottamuksellisuuden loukkauksiin²⁷⁵. Siten on tärkeää, että datan jakamisesta pidättäytyminen tai sen keskeyttäminen eivät perustu vain yleispiirteiseen yksilöintiin, mutta samalla on varmistettava, että liikesalaisuuden yksilöiminen ei vaaranna liikesalaisuuksia.

Liikesalaisuuksien yksilöinti ja analysointi voidaan joissain tapauksissa automatisoida algoritmien avulla, erityisesti suurissa IoT-datamassoissa. Aikaleimaus ja lohkoketjuteknologiat voivat auttaa liikesalaisuuksien tunnistamisessa. Datasäädös peräänkuuluttaa järjestelmiä, jotka mahdollistavat liikesalaisuuksien tehokkaan järjestämisen ja hallinnan. Yksilöinnin on oltava riittävän laajaa arvokkaan tiedon suojaamiseksi, mutta liiallista yleisyyttä on vältettävä, jotta liikesalaisuuden kriteerit täyttyvät ja liikesalaisuuksien määrä pysyy hallittavana.²⁷⁶ Datasäädöksen soveltamisessa yksilöinnin kohteena on todennäköisesti suuri datakokonaisuus. Käytännössä ei välttämättä pystytä tarkastelemaan esimerkiksi jokaista tiedostoa erikseen, vaan yksilöinti voidaan tehdä käyttämällä edustavia esimerkkejä ja tarkastelemalla dataa laajempina kokonaisuuksina. Tällainen data sisältää usein myös osittain julkista tietoa, jolloin datan haltijan on selitettävä tarkasti, miten nämä tiedot on yhdistetty ainutlaatuisella tavalla, jotta ne voidaan suojata liikesalaisuutena.

3.3 Liikesalaisuuden haltijan määrittäminen datataloudessa

Liikesalaisuusdirektiivin 2 artiklan 2 kohdan mukaan liikesalaisuuden haltija on luonnollinen henkilö tai oikeushenkilö, joka käyttää laillista määräysvaltaa liikesalaisuuteen. Haltija voi puolustautua oikeudenloukkauksia vastaan esittämällä lakiin perustuvia vaatimuksia. Liikesalaisuuden haltija voi olla esimerkiksi tiedon alkuperäinen luoja tai sopimusten perusteella määräysvallan saanut taho.²⁷⁷ Liikesalaisuuden haltijan oikeudet voivat kuulua yhdelle tai useammalle taholle itsenäisesti, rinnakkain tai rajoitetusti.²⁷⁸

²⁷³ Vapaavuori 2019 s.135–137.

²⁷⁴ Menell – Almeling – Cundiff ym. 2023, s. 2–3.

²⁷⁵ EUIPO 2023, s. 90–92.

²⁷⁶ WIPO 2024, s. 136.

²⁷⁷ HE 49/2018, s. 85.

²⁷⁸ Vapaavuori 2019, s. 203–206. Liikesalaisuusdirektiivi 2 artikla 2 kohta.

Verkottuneessa ympäristössä, kuten esineiden internetissä, liikesalaisuuden haltijan määrittäminen voi olla haastavaa. Tämä johtuu siitä, että datan keräämiseen osallistuu useita toimijoita.²⁷⁹ Yleensä valmistaja on liikesalaisuuden haltija, koska se hallitsee laitteen tuottamaa tai keräämää raakadataa ja sillä on intressi sen suojaamiseen. Verkkoon liitetyn tuotteen käyttäjänä toimiva yritys voi myös olla liikesalaisuuden haltija, jos se kerää dataa ja on sopinut tiedon salassapidosta valmistajan kanssa. Tällöin valmistaja ja käyttäjä voivat olla rinnakkaisia liikesalaisuuden haltijoita. Sen sijaan kuluttajat eivät voi olla liikesalaisuuden haltijoita, mutta valmistaja voi asettaa niille salassapitovelvoitteita. Liikesalaisuuksia voidaan hallita myös yhteisesti, jos useat tahot osallistuvat datan tuottamiseen ja käsittelyyn.²⁸⁰

Datan jakaminen pitkissä toimitusketjuissa lisää liikesalaisuuden haltijan määrittämisen vaikeutta, erityisesti jos dataa yhdistetään muihin aineistoihin tai jaetaan edelleen. Siten datan jakaminen eri tahoille voi hämärtää oikean liikesalaisuuden haltijan identiteettiä. Epäselvää on myös se, milloin henkilö tosiasiallisesti hallitsee tietoa niin, että hän voi esittää vaatimuksia oikeuksiensa loukkaamisen tilanteessa. Riittääkö esimerkiksi, että liikesalaisuuden haltija hallitsee vain olennaista osaa raakadatasta vai, onko hänen hallittava kaikkia raakadatan lähteitä erikseen.²⁸¹ Oikeuskirjallisuudessa on esitetty, että liikesalaisuuden haltija voidaan tunnistaa melko matalalla kynnyksellä²⁸². Sopimuksilla on keskeinen rooli vastuiden määrittelyssä ja siinä, kuka tai ketkä vastaavat tiedon tosiasiallisesta hallinnasta. Lopulta liikesalaisuuden haltijan asema määräytyy sen perusteella, kenellä on tosiasiallinen laillinen määräysvalta ja kenen oikeuksia on loukattu.²⁸³ Jos datan luomiseen osallistuu useita tahoja, yksi mahdollinen ratkaisu on määritellä datan haltijaksi yritys, joka on tehnyt merkittävimmän investoinnin datan keräämiseen ja käsittelyyn. Tämä on perusteltua erityisesti tilanteessa, joissa useat yritykset, jotka ovat osallistuneet datan keräämiseen ja siirtämiseen, ovat erimielisiä siitä, kenellä on oikeus vaatia lakiin perustuvia seuraamuksia²⁸⁴.

Datasäädöksessä säädettyjen roolien määrittely voi olla oleellinen osa liikesalaisuuden haltijan määrittelyä, erityisesti, jos dataa jaetaan useille osapuolille. Ennen kuin voidaan tarkasti määritellä, kuka on liikesalaisuuden haltija, on usein tarpeen hahmottaa, mikä osapuoli hallitsee, käyttää ja jakaa dataa. Datasäädöksen roolien määrittelyn haaste liittyy erityisesti siihen, että sama taho voi toimia monessa roolissa samanaikaisesti. Sama taho voi olla

²⁷⁹ Wiebe 2017, s. 65.

²⁸⁰ Drexl 2018, s. 95–96. Jos valmistaja toimittaa käyttäjän tehtaaseen laitteita, jotka keräävät sensorien avulla dataa, käyttäjällä voi olla tarve varmistaa, että valmistaja pitää datan salassa eikä jaa sitä kolmansille osapuolille.

²⁸¹ Nordberg 2020, s. 208–209.

²⁸² Nordberg 2020, s. 215.

²⁸³ Wiebe – Schur 2019, s. 816.

²⁸⁴ Manzo 2019, s. 9–10.

esimerkiksi datan käyttäjä, datan haltija ja datan vastaanottaja, jolloin roolien erot voivat hämärtyä. Datasäädöksessä datan haltija on taho, jolla on oikeus ja mahdollisesti velvollisuus jakaa dataa. Datan haltijan oikeus ja velvollisuus jakaa dataa perustuu siihen, että datan haltijalla on kyky käyttää dataa ja asettaa se saataville joko oikeudellisin tai tosiasiallinen keinoin. Epäselvää on se, miten käyttäjien omistusoikeudet, sopimukset ja tosiasiallinen hallinta vaikuttavat heidän oikeuksiinsa käyttää ja jakaa syntynyttä dataa.²⁸⁵ Jos käyttäjille annetaan "täydellinen pääsy tietoihin", liikesalaisuuden haltijan tunnistaminen voi vaikeutua.

Lähtökohtaisesti liikesalaisuus säilyy alkuperäisen haltijan omaisuutena, vaikka se luovutettaisiin toiselle yritykselle. Oikeuskirjallisuudessa on katsottu, että luovuttavan yrityksen liikesalaisuus voi muodostua vastaanottajan liikesalaisuudeksi, kunhan sitä käsitellään luovutustarkoituksen mukaisin rajoituksin. Vastaanottavalla yrityksellä voi myös olla lain tai sopimuksen perusteella oikeus jakaa liikesalaisuus edelleen, mikä voi johtaa siihen, että alkuperäisen liikesalaisuuden haltijan identiteetti hämärtyy.²⁸⁶ Kolmannella osapuolella voi olla käyttäjän kanssa tehdyn sopimuksen nojalla oikeus jakaa dataa toiselle kolmannelle osapuolelle, mikä voi vaikeuttaa oikean liikesalaisuuden haltijan tunnistamista. Datan haltija on usein myös liikesalaisuuden haltija, mutta datan haltija voi myös pitää halussaan toisen liikesalaisuuksia. Periaatteessa käyttäjä tai kolmas osapuoli voi tulla vastaanottamansa datan sisältämien liikesalaisuuksien haltijaksi. Se, missä määrin käyttäjä tai kolmas osapuoli saa käyttää liikesalaisuuden haltijan oikeuksia, riippuu kuitenkin sopimuksesta, kuten lisenssi- ja salassapitosopimuksesta.

3.4 Eräitä kriittisiä näkökulmia liikesalaisuuksien suojaan

3.4.1 Tasapaino datan haltijan edun ja dataan pääsyyn välillä

Immateriaalioikeusjärjestelmiä, kuten teollis- ja tekijänoikeussuojaa sekä liikesalaisuussuojaa, on kritisoitu niiden epätasapainosta tiedon haltijan eduksi. Nykyisessä immateriaalioikeusjärjestelmässä on puutteita, jotka rajoittavat sen kykyä edistää sosiaalisesti toivottavaa kehitystä ja yhteiskunnassa tavoiteltuja arvoja. Hyötylähtöinen lähestymistapa ("utility approach") ei ole kestävä maailmassa, jossa korostuvat esimerkiksi kestävä kehitys ja ympäristön suojelu.²⁸⁷ Taloudellisen tehokkuuden ja yksityisten kannustimien korostaminen voi estää julkisen edun toteutumista. Immateriaalioikeudet voivat esimerkiksi rajoittaa mahdollisuuksia korjata patentilla suojattuja tuotteita. Näitä järjestelmiä tulisi kehittää siten,

²⁸⁵ Wiedemann - Leicht 2023, s. 17–18.

²⁸⁶ Vapaavuori 2019, s. 130–135.

²⁸⁷ Ballardini- Kaisto – Similä 2021 s. 9. Immateriaalioikeuksien hyödyllisyysteoria keskittyy alkuperäisten tekijöiden tarpeisiin ja korostaa taloudellista tehokkuutta. Tällöin se hankaloittaa sosiaalisia teorioita, jotka korostavat kulttuuria ja muita vähemmän mitattavissa olevia arvoja, kuten ympäristönsuojelua.

että ne paremmin huomioivat yhteiskunnalliset edut, kuten ympäristönsuojelun, ja tasapainottavat yksityisen omistusoikeuden sekä yhteiskunnan tarpeet oikeudenmukaisemmin.²⁸⁸

Oikeuskirjallisuudessa on esitetty, että liikesalaisuusdirektiivi onnistuu melko hyvin tasapainottamaan liikesalaisuuden suojan tarpeet ja muiden osapuolten oikeudet ja edut²⁸⁹. Toisaalta on esitetty myös, että erilaisten älykkäiden laitteiden käyttäjien näkökulmasta sääntely ei tarjoa riittäviä poikkeuksia tai laillisia keinoja saada pääsyä tietoihin, jotka on suojattu liikesalaisuuksina. Tämän vuoksi liikesalaisuuksien suojelussa korostuu epätasapainoisesti liikesalaisuuden haltijoiden edut.²⁹⁰ Edelleen on esitetty, että liikesalaisuuslainsäädäntö painottaa usein oikeudenhaltijoiden kilpailuetuja yhteiskunnallisen edun ja sosiaalisen oikeudenmukaisuuden kustannuksella.²⁹¹ Siten liikesalaisuuksien suojaamisessa ei ole aina riittävästi huomioitu yhteiskunnallisia etuja²⁹². Immateriaalioikeuksien tavoin liikesalaisuussuojaa on siis kritisoitu siitä, että se ei ota riittävästi huomioon liikesalaisuuden haltijan ulkopuolisia intressejä.

Syvät salaisuudet (eng. "deep secrets") viittaavat liikesalaisuuksiin, joita ei voida paljastaa liikesalaisuussuojan rajoitusten tai poikkeusten kautta, mutta joiden paljastaminen saattaa olla välttämätöntä sosiaalisen hyvinvoinnin turvaamiseksi.²⁹³ Tällaisia liikesalaisuuksia voivat olla esimerkiksi valmistus-, diagnostiikka-, korjaus- ja komponenttitiedot, jotka ovat olennaisia esimerkiksi teknologian korjaamiseksi, mukauttamiseksi ja kierrättämiseksi. Lisäksi liikesalaisuuksien suojan piiriin kuuluvat algoritmit voivat aiheuttaa ongelmia perusoikeuksien näkökulmasta, koska tekoälyn tekemien päätösten tarkastaminen ei tällöin ole mahdollista. Jos elintärkeät "syvät salaisuudet", kuten kiertotalouden edistämiseen tai ympäristönsuojeluun liittyvät tiedot, jäävät paljastumatta, liikesalaisuuksien suoja ei täytä yhteiskunnan tarpeita, vaan pikemminkin rajoittaa mahdollisuuksia edistää yhteiskunnallisia arvoja.²⁹⁴ Datasäädöksen voi ajatella edistävän syvien liikesalaisuuksien saattamista käyttäjien, kolmansien osapuolten ja julkisen sektorin saataville. Tämä johtuu siitä, että kaikkea IoT-tuotteiden ja liitännäispalveluiden tuottama dataa ei ole mahdollista hankkia laillisin

²⁸⁸ Ballardini- Kaisto – Similä 2021, s. 3–4.

²⁸⁹ Leistner - Antoine 2023, s. 7. Tätä selittävät muun muassa direktiivin rajoitettu soveltamisala, poikkeukset ja suhteellinen täytäntöönpanokäytäntö.

²⁹⁰ Mata Agüero 2018, s. 54.

²⁹¹ Moore 2017, s. 2. Esimerkiksi algoritmien, joita käytetään rikosriskin arvioinnissa, läpinäkyväisyys voidaan kyseenalaistaa perusoikeuksien ja yhteiskunnan oikeudenmukaisuuden kannalta.

²⁹² Dreyfuss 2024, s. 4.

²⁹³ Dreyfuss 2024, s. 2–3.

²⁹⁴ Dreyfuss 2024, s. 7–8.

keinoin²⁹⁵. Lisäksi osa datasäädöksen soveltamisalaan kuuluvasta datasta voi olla sellaista, jonka paljastaminen on tarpeen tärkeiden yhteiskunnallisten tavoitteiden, kuten kestävän kehityksen, edistämiseksi.

Dataloudessa on korostunut tarve rajoittaa liikesalaisuussuojan liiallisista laajentumisista. Oikeuskirjallisuudessa on esitetty kaksi keinoa, joilla liikesalaisuussuojaa voitaisiin rajoittaa. Numerus clausus -periaate asettaa rajat sille, mitä aineettomia oikeuksia voidaan suojata, kun taas sosiaalisen funktion -periaate mahdollistaa liikesalaisuuksiin puuttumisen yhteiskunnallisten etujen, kuten turvallisuuden, kansanterveyden ja ympäristönsuojelun, perusteella. Numerus clausus -periaate voisi estää syntaktisten datakokonaisuuksien suojaamisen liikesalaisuuksina, kuten raakatiedon, joka ei ole analysoitu tai jalostettu. Datasäädöksessä on piirteitä sosiaalisen funktion periaatteesta, sillä siinä pyritään tasapainottamaan tietojen suojaaminen ja datan saatavuuden välinen jännite ottaen huomioon perusoikeudet ja yleinen etu. Datasäädös edistää kiertotaloutta ja ympäristönsuojelua tarjoamalla mekanismeja, jotka mahdollistavat esimerkiksi tuotteiden korjaamisen ja mukauttamisen ilman, että liikesalaisuuksien lainmukaiset tavoitteet vaarantuvat.²⁹⁶ Näin säädös tasapainottaa yhteiskunnan ja liikesalaisuuden haltijoiden etuja aiempaa oikeudenmukaisemmin. Kehitys on kuitenkin vasta alussa, ja liikesalaisuuksien suojan ja yhteiskunnallisten etujen tasapainottamisessa on yhä paljon tehtävää. Datasäädös havainnollistaa, kuinka liikesalaisuuksien suoja itsessään ei ole onnistunut riittävästi takaamaan oikeudenmukaista ja kilpailua edistävää pääsyä dataan.

3.4.2 Liikesalaisuussuojan oikeutus

Yleensä liikesalaisuussuojan olemassaoloa perustellaan taloudellisilla syillä. Taloudellisen perustelun mukaan liikesalaisuuksien suoja kannustaa yrityksiä innovoimaan ja vähentää liikesalaisuuksien suojaamiseen käytettäviä transaktiokustannuksia, jotka voidaan käyttää esimerkiksi tutkimus- ja kehitystoimintaan. Tämä lisää taloudellista tehokkuutta ja parantaa yritysten kilpailukykyä. Liikesalaisuussuojaa voidaan eräin varauksin perustella sosiaalisen sopimuksen teorialla, jonka mukaan suoja voi hyödyttää yhteiskuntaa edistämällä tiedon jakamista ja luomalla niin sanottuja spillover-vaikutuksia²⁹⁷. Liikesalaisuussuojan perustelut eivät kuitenkaan ole ongelmattomia. Kritiikki kohdistuu erityisesti siihen, että

²⁹⁵ Mata 2018, s. 36–41. Käänteismallinnus tai pelkkä fyysisen laitteen tutkiminen ei ole tehokas tapa hankkia teollista dataa.

²⁹⁶ Fia 2022, s. 940–944.

²⁹⁷ Sappa 2018, s. 522.

liikesalaisuuksien suoja ei vaadi tiedon julkistamista, ja se voi olla periaatteessa ikuinen. Tämä voi rajoittaa tiedon jakamista ja estää laajempaa yhteiskunnallista hyötyä.²⁹⁸

Liikesalaisuuksien taloudelliset ja innovaatiovaikutukset ovat edelleen huonosti tunnettuja²⁹⁹. Vaikka liikesalaisuuksien suoja perustellaan sillä, että se edistää innovointia ja estää vilpillistä liiketoimintaa, nämä vaikutukset on kyseenalaistettu³⁰⁰. Empiiristä näyttöä liikesalaisuussuojan investointi- ja talousvaikutuksista on edelleen vähän. Esimerkiksi Bone on esittänyt, että liikesalaisuuksien suojaaminen on perusteltua ainoastaan silloin, kun sen sosiaaliset edut ylittävät suojaamisesta aiheutuvat sosiaaliset kustannukset.³⁰¹ Tiedon salassapito voi aiheuttaa resurssihukkaa, hidastaa kehitystä, estää työntekijöiden liikkuvuutta ja vähentää tiedon jakamista. Lisäksi vilpillinen toiminta, kuten tietojen varastaminen tai petos, on jo kriminalisoitu, mikä voi tehdä liikesalaisuuksien siviilioikeudellisista mekanismeista osin tarpeettomia.³⁰² Liikesalaisuuksien suoja on myös kritisoitu siitä, että yritykset voivat suojata tietoja omilla keinoillaan, kuten sisäisin järjestelyin tai sopimuksin, ja jakaa tietoa halutessaan vapaaehtoisesti. Toisaalta on myös tilanteita, joissa liikesalaisuuksien suoja tarjoaa lisäkannustimia innovointiin, kuten monimutkaisissa tuotantoketjuissa tai tilanteissa, joissa tiedon pitäminen salassa olisi muuten liian kallista tai hankalaa.³⁰³ Näissä tapauksissa suojan edistää yhteiskunnan kannalta hyödyllistä kehitystä.

Liikesalaisuuksiin pääsyä koskevia sääntöjä tulee tarkastella huolellisesti, koska liikesalaisuudet ovat tärkeitä yritysten kilpailukyvyille. Liikesalaisuuksia ei voida kuitenkaan pitää täysin suojattuna, jos niihin pääsy on tärkeää markkinahäiriöiden korjaamiseksi tai kilpailun parantamiseksi. Esimerkkinä mainitaan EU:n yleisen tuomioistuimen Microsoft-tapaus T-201/04, jossa päätettiin, että tietyissä olosuhteissa kaupallisia salaisuuksia voidaan jakaa, jos se tukee kilpailua tai yleistä etua.³⁰⁴

Datasäädöksen yhteydessä on esitetty, että datan haltijan aseman suojele ei ole taloudellisesti perusteltua, koska IoT-tuotteiden osalta ei ole havaittu investointikannustimien puutetta, jota pitäisi suojella rajoittamalla datan saatavuutta. Tämä johtuu siitä, että alkuperäiset valmistajat voivat kompensoida tappioitaan hinnoittelemalla tuotteensa ja osallistumalla toissijaisille

²⁹⁸ Searle 2021, s. 7–9. Sosiaalisen sopimuksen teoria: Se antaa yksinoikeuden esimerkiksi keksintöön keksijälle ja hyötyä siitä taloudellisesti sekä kattaa kustannukset, joita se laittaa innovaatiotyöhön. Vastineeksi yhteiskunta hyötyy siitä, että innovaattorit julkistavat keksintöjä, mikä edistää tiedon kiertoa ja uusia innovaatioita.

²⁹⁹ Searle 2021, s. 25–26.

³⁰⁰ Bone 2014, s. 7–12. Risch 2010, s. 26–27.

³⁰¹ Bone 2014, s. 1.

³⁰² Dreyfuss 2024, s. 4–6.

³⁰³ Risch 2010, s. 10–15.

³⁰⁴ Ks. tarkemmin Leistner 2023, s. 929. Asia T-201/04, kohdat 643–, ja 289–290, jossa tuomioistuin rinnasti liikesalaisuudet immateriaalioikeuksiin.

markkinoille.³⁰⁵ Oikeuskirjallisuudessa on katsottu, että datasäädös vahvistaa datan haltijan asemaa tavalla, joka rinnastuu datan de facto omistusoikeuteen. Tämä ei ole taloudellisesti perusteltua, sillä ei ole näyttöä siitä, että yksinoikeudenkaltaisen oikeus kannustaisi datan haltijoita investoimaan IoT-datan tuottamiseen. Liikesalaisuuksien suojan osalta ei voida vielä antaa selvää vastausta siihen, miten se vaikuttaa yritysten datan jakamiseen datataloudessa.³⁰⁶ Tapauskohtaisesti voi kuitenkin ilmetä erityisiä kannustinongelmia, jotka riippuvat tilanteesta ja datan luonteesta. Liikesalaisuuksien ja muutenkin yhteiskunnan kannalta on hyödyllistä tunnistaa ne tilanteet, joissa liikesalaisuuksien suojaaminen edistää investointeja tiedon tuottamiseen. Datasäädöksen tulisi korostaa datan jakamisen hyötyjä, kuten innovoinnin, kilpailun ja käyttäjäkokemuksen parantamista, eikä liiallisesti painottaa jakamiseen liittyviä riskejä³⁰⁷. Datasäädökseen yhteydessä liikesalaisuussuojan merkitystä investointikannustimien suojaamisessa on korostettu, vaikka empiirinen näyttö tästä on kiistanalaista.

³⁰⁵ Kerber 2024, s. 5–6. Eckardt – Kerber 2023, s. 12

³⁰⁶ Radauer – Bader - Aplin 2022, s. 80.

³⁰⁷ Kerber 2022, s. 15–21.

4. LIIKESALAISUUSSUOJAN TULKINTA DATASÄÄDÖKSESSÄ

4.1 Sallitut datan käyttötarkoitukset suhteessa eri tahoihin

4.1.1 Käyttäjä

Datasäädöksen käyttöoikeudet määrittelevät, kuinka asetuksen nojalla saatua dataa voidaan käyttää. Lisäksi ne säätelevät siitä, kenelle dataa on sallittua jakaa ja, mitä ehtoja tähän liittyy. Datan käyttöoikeudella voi olla vaikutusta myös liikesalaisuuksien suojaan. Sääntely voi lisätä liikesalaisuuksien paljastumisen riskiä, mikäli siinä säädetään laajoista käyttöoikeuksista ja mahdollisuudesta jakaa datan haltijan tietoja eteenpäin. Seuraavaksi tarkastelen käyttäjän, kolmannen osapuolen, toisen kolmannen osapuolen sekä datan haltijan käyttöoikeuksia liikesalaisuussuojan näkökulmasta.

Käyttäjällä on oikeus käyttää dataa vapaasti mihin tahansa lailliseen tarkoitukseen. Käyttäjä voi esimerkiksi jakaa dataa kolmannelle osapuolelle jälkimarkkinapalvelun tarjoamiseksi.³⁰⁸ Käyttäjä voi jakaa dataa, joka ei sisällä henkilötietoja, kaupallisiin tai ei-kaupallisiin tarkoituksiin, tarvittaessa datan välityspalvelujen kautta³⁰⁹. Tämä mahdollistaa datan käytön esimerkiksi innovointiin tai useilta käyttäjiltä kerätyn datan yhdistämisen suureksi data-aineistoksi. Datan välityspalvelut voivat yhdistää eri käyttäjien dataa ja käyttöoikeuksia, mikä helpottaa laajojen ja yhdistettyjen tietoaaineistojen luomista. Toisaalta asetuksen toimivuuteen innovoinnin välineenä on suhtauduttu epäilevästi, koska kuluttajilla ei välttämättä ole riittävästi kannustimia datan keräämiseen, ja kerääminen voi aiheuttaa korkeita transaktiokustannuksia.³¹⁰

Datasäädös vahvistaa etenkin verkkoon liitettyjen tuotteiden ja niihin liittyvien palveluiden käyttäjien asemaa säätämällä laajoista käyttöoikeuksista.³¹¹ Käyttäjien oikeus käyttää dataa mihin tahansa lailliseen tarkoitukseen perustuu asetuksen tavoitteisiin perustuvaan tulkintaan. Käyttäjän oikeutta myydä haltijalta saatua dataa oman taloudelliseen hyötyynsä vuoksi on kritisoitu siitä, että laaja käyttöoikeus ei ole taloudellisesti perusteltua³¹². Tämä tarkoittaa, että

³⁰⁸ Datasäädös johdanto (30). Käyttäjän laajojen käyttöoikeuksien avulla edistetään muiden kuin henkilötietojen likvidien, oikeudenmukaisten ja tehokkaiden markkinoiden syntymistä unionissa.

³⁰⁹ Datasäädös johdanto (26) ja 4 artikla 14 kohta.

³¹⁰ Eckardt – Kerber 2023, s. 17. Kerber 2024, s. 5–6. Käyttäjakeskeisyys voi aiheuttaa niin sanottuja pullonkauloja, jotka rajoittavat kolmansien osapuolten mahdollisuuksia käyttää dataa. Kerber 2023, s. 131–132.

³¹¹ Eckardt – Kerber 2023, s. 14.

³¹² Ks. tavoitteista datasäädöksen johdanto (32) ja (119). Käyttäjien käyttöoikeuksien suppeampaa näkökulmaa ilmentää Komissio 2022a, s. 33, joka rajasi kolmansien osapuolten oikeudet käyttää dataa vain lisäarvopalveluihin. Käytännössä esimerkkeinä tällaisista palveluista mainitaan korjaus, vakuutus- tai data-analytiikkapalvelut. Komissio 2022a, s. 33. Myös Drexl – Banda - Gonzalez Otero –ym. (2022, s. 106 ja 11) kannattivat, että käyttäjä voisi jakaa dataa kolmannelle osapuolelle ainoastaan lisäarvopalvelun tarjoamiseksi käyttäjälle (tarkoituseräinen lähestymistapa). Lisäksi ehdotettiin, että soveltamisalaan kuuluva data tulisi laajentaa johdettuun ja pääteltyyn dataan. Ks. tarkemmin datan jakamisen taloudellisista perusteista ja käyttötarkoituksen rajoittamisen vaikutuksista kilpailuun ja markkinoiden toimivuuteen.

säädöksessä määritellään käyttäjien laajat oikeudet käyttää dataa omiin tarpeisiinsa sekä taloudellisen edun tavoittelemiseksi.

4.1.2 Kolmas osapuoli

Kolmas osapuoli voi käyttää tietoja vain käyttäjän kanssa sovittuihin tarkoituksiin ja ehdoilla. Lisäksi kolmannen osapuolen on poistettava data, kun sitä ei enää tarvita sovittuun tarkoitukseen, ellei käyttäjän kanssa ole toisin sovittu. Siten se, mihin tarkoituksiin kolmas osapuoli voi käyttää dataa määräytyy käyttäjän kanssa tehtävän sopimuksen ja käyttäjän suostumuksen perusteella. Käyttäjä voi päättää, mitä kolmas osapuoli saa tehdä datalla (ns. postiviinen vaikutus). Toisaalta käyttäjä voi myös määrittää, mitä kolmas osapuoli ei saa tehdä datalla tai estää kolmannen osapuolen pääsyn dataan (ns. negatiivinen vaikutus).³¹³

Liikesalaisuudet on säilytettävä, ja niitä saa ilmaista kolmansille osapuolille vain siltä osin kun se on ehdottoman välttämätöntä käyttäjän ja kolmannen osapuolen välillä sovitun käyttötarkoituksen täyttämiseksi³¹⁴. Siten osapuolten tulee sopia, mihin tarkoitukseen liikesalaisuuksia sisältävä data annetaan käyttöön. Sopimuksessa tulee määritellä käyttötarkoitukset ja selventää, että datan suora tai epäsuora käyttö on sallittua, jos se on ehdottoman välttämätöntä käyttötarkoituksen täyttämiseksi. Sopimus sitoo myös muita mahdollisia kolmansia osapuolia, jotka tiesivät tai joiden olisi pitänyt tietää esimerkiksi, että alkuperäinen kolmas osapuoli rikkoi sopimusvelvoitteitaan liikesalaisuuksia sisältävien tietojen paljastamisessa tai käytössä.³¹⁵

Riitatilanteissa voi olla epäselvää, kuka päättää, milloin datan jakaminen on ehdottoman välttämätöntä. Tämä voi olla datan haltija, datapyynnön tekijä tai molemmat osapuolet yhteisymmärryksessä. Tällöin datan haltija saattaa pyrkiä rajoittamaan datan jakamista kiistämällä sen tarpeellisuuden sovittuun käyttötarkoitukseen nähden.³¹⁶ Lisäksi kansallinen toimivaltainen viranomainen voi käsitellä valituksia, jotka liittyvät asetuksen rikkomuksiin, mukaan lukien liikesalaisuuksien suojaamiseen³¹⁷. Datan haltijan on tärkeää olla tietoinen käyttäjän ja kolmannen osapuolen sopimasta käyttötarkoituksesta, koska datan haltija sopii kolmannen osapuolen kanssa liikesalaisuuksien suojaamisesta.³¹⁸ Liikesalaisuuksien

³¹³ Datasäädös 6 artikla 1 ja 2 kohta. Ducuing 2022, s. 19.

³¹⁴ Datasäädös 5 artikla 9 kohta. Datasäädös 19 artikla 3 kohta, jonka mukaan, jos datapyynnön on tehnyt julkisen sektorin elin, datan jakaminen sallitaan vain siltä osin, kun sen ”ehdottoman välttämätöntä 15 artiklan mukaisen pyynnön tarkoituksen saavuttamiseksi”. Datasäädöksen 17 artiklassa säädetään velvollisuudesta toimittaa perusteltu pyyntö.

³¹⁵ Leistner – Antoine 2022, s. 99–100.

³¹⁶ Leistner – Antoine 2022, s. 90.

³¹⁷ Datasäädös 37 artikla 5 kohta b alakohta.

³¹⁸ Datasäädös 6 artikla 2 kohta c alakohta. Hennemann – Ebner – Karsten 2023, s. 54.

suojaamisen kannalta on erityisen tärkeää, että kolmannen osapuolen käyttöoikeudet määritellään tarkasti.

Kolmannella osapuolella ei ole oikeutta pyytää dataa suoraan valmistajalta, vaan aloitteen datan jakamiseen tekee aina käyttäjä. Lisäksi kolmannen osapuolen mahdollisuudet hyödyntää dataa riippuvat käyttäjän kanssa sovituista ehdoista. Käyttäjä ja kolmas osapuoli voivat sopia datan jakamisesta mihin tahansa tarkoitukseen, ellei asetuksessa toisin säädetä. Jos kolmannella osapuolella on pääsy useilta käyttäjiltä kerättyyn dataan, se voi hyödyntää yhdistettyjä datakokoelmia, jotka saattavat sisältää myös todennäköisemmin liikesalaisuuksia.³¹⁹ Käyttäjällä on keskeinen rooli kolmannen osapuolen käyttöoikeuden rajojen määrittelyssä, mikä voi vaikuttaa myös datan haltijan liikesalaisuuksien suojaan. Kun tietoa jaetaan kolmannelle osapuolelle, se on sallittua vain tiettyyn käyttötarkoitukseen, mutta käyttäjällä ei ole vastaavaa rajoitusta. Tätä on kritisoitu siitä, että liikesalaisuussuojan ei pitäisi vaihdella sen mukaan, kenelle dataa jaetaan.³²⁰

4.1.3 Toinen kolmas osapuoli

Kolmannet osapuolet, jotka vastaanottavat dataa voivat myydä edelleen vastaanottamaansa dataa toiselle kolmannelle osapuolelle käyttäjän kanssa tehdyn sopimuksen perusteella. Asetuksessa datan jakaminen toiselle kolmannelle osapuolelle ei rajoitu pelkästään jälkimarkkinapalveluiden tarjoamiseen käyttäjille, vaan dataa saa jakaa myös muissa tarkoituksissa käyttäjän suostumuksella. Lisäksi edellytetään, että kolmas osapuoli toteuttaa kaikki datan haltijan ja kolmannen osapuolen välillä sovitut tarvittavat toimenpiteet liikesalaisuuksien luottamuksellisuuden säilyttämiseksi.³²¹ Siten käyttäjä säilyttää kontrollin dataansa ja voi sallia jakamisen ilman, että se olisi tarpeen palvelun tarjoamiseksi käyttäjälle³²².

Kolmannen osapuolen käyttöoikeuteen liittyy kysymys siitä, kuinka pitkälle käyttäjä voi hallita dataa arvoketjun myöhemmissä vaiheissa. Jos kolmas osapuoli haluaa jakaa dataa toiselle kolmannelle osapuolelle (esimerkiksi kolmas osapuoli B, joka jakaa tietoja toiselle kolmannelle osapuolelle C), tämä on mahdollista vain käyttäjän kanssa tehdyn sopimuksen perusteella. On epäselvää, voiko käyttäjä kieltää datan siirtämisen edelleen kolmannelle osapuolelle (esimerkiksi C ja jakaa tietoa D:lle). Ei näytä olevan estettä sille, että käyttäjä hyödyntää datan siirto-oikeuttaan useita kertoja suhteessa eri kolmansiin osapuoliin ja tarkoituksiin. Käyttäjä voi

³¹⁹ Bird&Bird 2022.

³²⁰ Drexl – Banda - Gonzalez Otero ym. 2022, s. 101. Picht 2022, s. 38–39.

³²¹ Datasäädös 6 artikla 2 kohta c alakohta. Vt. Komissio 2022d, 6 artikla 2 kohta c alakohta. Lopullisessa asetuksessa annettiin kolmansille osapuolille laajempi oikeus jakaa dataa toisille kolmansille osapuolille, kunhan käyttäjän kanssa sovitaan asiasta.

³²² Drexl – Banda - Gonzalez Otero ym. 2022, s. 122 ja 7.

vaatia oikeuksiaan ainoastaan niitä kolmansia osapuolia kohtaan, joiden kanssa hän on tehnyt sopimuksen.³²³ Lisäksi datan edelleen jakaminen on sallittua vain, jos kolmas osapuoli toteuttaa datan haltija kanssa sovitut tarvittavat toimenpiteet liikesalaisuuksien luottamuksellisuuden säilyttämiseksi³²⁴.

4.1.4 Datan haltija

Datan haltijan käyttöoikeuden määrittely on liikesalaisuuksien kannalta olennaista silloin, kun käyttäjä on oikeushenkilö, joka hankkii IoT-tuotteita ja niihin liittyviä palveluja kaupalliseen käyttöön. Tällöin käyttäjä voi toimia myös liikesalaisuuden haltijana.³²⁵ Datan haltija saa käyttää dataa vain tarkoitukseen, josta se on sopinut käyttäjän kanssa. Siten datasäädös vaatii uudenlaista datankäyttösopimusta käyttäjän ja datan haltijan välillä, jossa määritellään, miten datan haltija voi hyödyntää käyttäjän laitteen käytön perusteella syntyvää ei-henkilökohtaista dataa³²⁶. Lisäksi datan haltijan mahdollisuutta jakaa käyttäjältä peräisin olevaa dataa on rajoitettu. Datasäädöksen 4 artiklan 14 kohdan mukaan datan haltijat eivät saa asettaa tuotteen dataa, joka ei ole henkilötietoja, kolmansien osapuolten saataville kaupallisiin tai ei-kaupallisiin tarkoituksiin muutoin kuin käyttäjän kanssa tekemänsä sopimuksen täyttämiseksi. Edelleen datan haltijoiden on sopimusteitse velvoitettava kolmannet osapuolet olemaan jakamatta edelleen niiltä vastaanotettua dataa.

4.2 Kielletyt datan käyttötarkoitukset

4.2.1 Kilpaileva tuote

Käyttäjä, kolmas osapuoli tai julkisen sektorin toimija ei saa käyttää asetuksen perusteella saamaansa dataa kehittääkseen verkkoon liitetyn tuotteen, joka kilpailee sen verkkoon liitetyn tuotteen kanssa, josta data on peräisin, eikä tässä tarkoituksessa jakaa dataa kolmannen osapuolen kanssa³²⁷. Olennaista on se, että kielto ei koske kokonaan uusien palveluiden, mukaan lukien tuotteeseen liittyvien palveluiden kehittämistä, jotka kilpailevat alkuperäisen datan haltijan tarjoamien palveluiden kanssa.³²⁸ Datasäädös ei rajoita myöskään kokonaan uusien tuotteiden kehittämistä, jotka eivät ole alkuperäisen tuotteen läheisiä korvikkeita. Tuote

³²³ Ducuing 2022, s. 19–21. Komissio 2022d. Datasäädösehdotuksessa käyttäjään valta hallita käyttöä rajoittui vain ensimmäiseen kolmanteen osapuoleen (B).

³²⁴ Datasäädös 6 artikla 2 kohta c alakohda.

³²⁵ Drexl 2018, s. 106. Kun dataa kerätään käyttäjiltä, kuten kaupallisilta ostajilta tai yrityksiltä, tämä tieto voi sisältää liikesalaisuuksia, jotka koskevat esimerkiksi tuotantomenetelmiä tai taloudellista tilannetta.

³²⁶ Datasäädös 4 artikla 13 kohta. Kerber 2024, s. 3–4.

³²⁷ Datasäädös 6 artikla 2 kohta e alakohda. Datasäädös 19 artikla 2 kohta a alakohdan mukaan sektorin elinten, komission, Euroopan keskuspankin ja unionin elinten osalta kiellettyä on myös se, että kehittää verkkoon liitetyn tuotteeseen liittyvän *palvelun*, joka kilpailee datan haltijan verkkoon liitetyn tuotteen tai siihen liittyvän palvelun kanssa.

³²⁸ Leistner – Antoine 2022, s. 88. Tuotteen kanssa kilpaileva palvelu voi olla esimerkiksi virtuaaliassistentti, jos se on olennainen osa IoT-tuotteen toimintaa.

kilpailee toisen tuotteen kanssa, kun tuotteet ovat ominaisuuksiensa, hintansa ja aiotun käyttönsä perusteella käyttäjien vaihdettavissa tai korvattavissa. Se, käytetäänkö datasäädöksen mukaista dataa kilpailevan tuotteen kehittämiseen, riippuu siitä, kilpaileeko uusi tuote alkuperäisen kanssa samoilla tuotemarkkinoilla. Markkinoiden määrittely tehdään unionin kilpailulainsäädännön vakiintuneiden periaatteiden perusteella.³²⁹

Säännöksen tavoitteena on estää datan käyttö taloudellisen hyödyn hankkimiseksi datan haltijan kustannuksella jäljitelmällä tuotteita, josta data on peräisin. Toisaalta käyttöoikeuden rajoitukset voivat luoda niin sanottuja pullonkauloja verkkoon liitettyjen tuotteiden markkinoille.³³⁰ Kilpailukielto voi vahvistaa valmistajien markkina-asemaa estämällä jälkimarkkinapalveluiden tarjoajien, joilla on usein hyvä tuntemus alasta ja kaupalliset suhteet, pääsyn päämarkkinoille³³¹. On myös esitetty, että rajoitus on tarpeeton, koska tuotteiden valmistajien immateriaalioikeudet tarjoavat jo riittävän suojan IoT-tuotteille³³². Kilpailevan tuotteen määrittelyssä on tärkeää välttää liian matalaa kynnystä, jotta datan käyttö ei estyisi. Jos tuotteet määritellään liian helposti kilpaileviksi alkuperäisen tuotteen kanssa, se voi vähentää kolmansien osapuolten halukkuutta hyödyntää dataa, mikä puolestaan hidastaa innovaatiota ja jälkimarkkinoiden kehittymistä.³³³ Tämä pätee erityisesti tilanteisiin, joissa käyttäjä tai kolmas osapuoli ovat jo kehittäneet vastaavan tuotteen³³⁴.

Datasäädöksen mukaan kiellettyä on myös jakaa dataa kilpailevan tuotteen kehittämisen tarkoituksessa kolmannen osapuolen kanssa. Sanamuoto viittaa kolmannen osapuolen tai käyttäjän tietoisuuteen tiedon luonteesta ja siitä, että vastaanottaja käyttää dataa tässä tarkoituksessa. Jos kolmas osapuoli (B) saa datan haltijalta (A) dataa, jota se jakaa edelleen toiselle kolmannelle osapuolelle (C), kilpailevan tuotteen kehittämisen kielto koskee myös C:tä. Datasäädöksessä ei edellytetä, että esimerkiksi kolmas osapuoli tiesi tai sen olisi pitänyt olla tietää datan alkuperästä, mikä laajentaa mahdollisuutta soveltaa mahdollisia seuraamuksia myös sellaisiin, jotka eivät olleet tietoisia. Toisaalta voidaan olettaa, että esimerkiksi käyttäjä oli tietoinen, jos hän osallistui liikesalaisuutta loukkaavaan toimintaan, kuten kilpailevan tuotteen tuotantoon³³⁵.

Kilpailevan tuotteen soveltamiseen liittyy myös tulkinannavaraisuutta. Esimeriksi, milloin tuote katsotaan niin uudeksi, että se ei kilpaile datan haltijan tuotteen kanssa. Entä, miten datan

³²⁹ Datasäädös johdanto (32). Leistner – Antoine 2022, s. 89.

³³⁰ Datasäädös johdanto (32). Graef – Husovec 2022, s. 2.

³³¹ Botero Arcila – Groza 2023, s. 28.

³³² Martens 2023, s. 1 ja 16–17.

³³³ Graef – Husovec 2022, s. 2. Leistner – Antoine 2022, s. 88–89.

³³⁴ Mylly 2024 s. 385.

³³⁵ Aplin 2014 ks. s. 22–23.

haltija voi osoittaa, että kolmas osapuoli kehitti kilpailevan tuotteen juuri datasäädöksen nojalla saatujen tietojen perusteella. Lisäksi tietojen alkuperän jäljittäminen voi olla vaikeaa, jos tietoja jaetaan suurelle määrälle kolmansia osapuolia ja yhdistetään eri lähteistä olevia tietoja.³³⁶ On myös epäselvää, kenellä on todistustaakka siitä, että kilpailevan tuotteen kehittäminen perustuu alkuperäisestä tuotteesta saatuun dataan³³⁷. Datan haltijan voi olla vaikeaa näyttää toteen, että tuotteen kehittämisessä on käytetty juuri alkuperäisestä tuotteesta peräisin olevaa dataa. Sen sijaan käyttäjällä ja kolmannella osapuolella on helpompi esittää näyttöä siitä, että tuotteen kehittämisessä saadut tiedot on hankittu muulla tavalla, kuten itsenäisen kehitystyön avulla. Datasäädöksessä ei ole asetettu mitään kynnystä sille, kuinka paljon datasäädöksen nojalla saatua dataa on sallittua käyttää kilpailevan tuotteen kehittämisessä. Kynnys lienee matalammalla kuin esimerkiksi liikesalaisuutta loukkaavan tavarankohdalla, joka edellyttää, että esimerkiksi suunnittelussa on saatu merkittävää hyötyä laittomasti hankitusta, käytetystä tai ilmaistusta liikesalaisuudesta³³⁸.

Jos liikesalaisuuksia sisältävää dataa on käytetty kilpailevan tuotteen kehittämiseen, sovellettavaksi voi tulla myös liikesalaisuusdirektiivin 2 artiklan 4 kohdan liikesalaisuutta loukkaava tavara³³⁹. Liikesalaisuuslainsäädännön soveltaminen ei kuitenkaan edellytä, että tuote kilpailee alkuperäisen datan haltijan tuotteen kanssa. Sen sijaan datasäädöksen kilpailevan tuotteen soveltaminen on kiellettyä riippumatta siitä, onko tuotteen kehittämisessä käytetty dataa liikesalaisuuksia vai muuta dataa.

4.2.2 Datan analysoinnin rajoitukset ja käänteismallinnuksesta sopiminen

Datasäädöksen 4 artiklan 10 kohdan mukaan käyttäjä ei saa käyttää datapyynnön perusteella saatua dataa johtaakseen siitä tietämystä valmistajan tai tapauksen mukaan datan haltijan taloudellisesta tilanteesta, varallisuudesta tai tuotantomenetelmistä. Sama soveltuu myös kolmasiin osapuoliin suhteessa datan haltijaan. Lisäksi kolmannen osapuolet eivät saa käyttää saamaansa dataa johtaakseen tietoa siitä, miten datan haltija käyttää dataa.³⁴⁰ Siten käyttäjän osalta datan käyttörajoitus on suppeampi, sillä se koskee vain artiklassa lueteltujen tietojen hankkimista. Asetus ei rajoita käyttäjää tai kolmatta osapuolta käyttämästä dataa muulla tavalla, joka heikentäisi datan haltijan kaupallista asemaa markkinoilla³⁴¹. Sen sijaan datan haltijan mahdollisuutta analysoida käyttäjien tai kolmansien osapuolten dataa on rajoitettu enemmän. Datan haltija ei saa edellä mainittujen kieltojen lisäksi käyttää verkkoon liitetyn tuotteen tai

³³⁶ Graef – Husovec 2022, s. 2.

³³⁷ Leistner – Antoine 2022, s. s. 88–89.

³³⁸ Liikesalaisuusdirektiivin 2 artiklan 4 kohta.

³³⁹ Mylly 2024, s. 387.

³⁴⁰ Datasäädös 6 artikla 2 kohta e alakohta.

³⁴¹ Vt. Datasäädös 6 artikla 2 kohta e alakohta ja 4 artiklan 10 kohta.

liitännäispalvelun dataa millään muullakaan tavalla, joka voisi heikentää käyttäjän tai kolmannen osapuolen kaupallista asemaa markkinoilla, joilla se toimii³⁴². Käyttäjän kaupallista asemaa voi heikentää datan käyttäminen esimerkiksi neuvottelutilanteissa tai sen yhdistäminen laajempiin tietokantoihin³⁴³. Siten säännös laajentaa käyttäjien liikesalaisuussuojaa rajoittamalla datan haltijoiden mahdollisuuksia hyödyntää dataa tavalla, joka voisi paljastaa tietoja esimerkiksi käyttäjän tuotantomenetelmistä.³⁴⁴

Datasta johtaminen viittaa raakadatan analysointiin ja käsittelyyn, jonka avulla voidaan saada tietoa, joka voi olla hyödyksi liiketoiminnassa. Pelkkä raakadatan kerääminen ei ole kiellettyä, vaan katsotaan asetuksen mukaiseksi datan vastaanottamiseksi. Kiistoja voi syntyä siitä, milloin kyse on pelkästä keräämisestä ja milloin analysoimalla johdetaan asetuksessa mainittua lisätietoa. Lisäksi datan haltijan kerätessä käyttäjän dataa voi olla epäselvää, milloin tämä heikentää käyttäjän kaupallista asemaa markkinoilla. Suhteessa kolmanteen osapuoleen datan analysoinnin rajoitus ei ole pakottava, vaan erikseen on säädetty, että kolmas osapuoli voi antaa luvan tällaiseen käyttöön ja se voi peruuttaa luvan milloin tahansa³⁴⁵. Kolmas osapuoli voi hyväksyä laajemman käytön, jos se arvioi laajempien käyttöoikeuksien hyötyjen ylittävän haitat. Tämä on ongelmallista käyttäjän kannalta, jos datan haltija saa kolmannen osapuolen suostumuksen perusteella selville tietoja, jotka heikentävät käyttäjän asemaa.³⁴⁶ Liikesalaisuussuojan ei tulisi vaihdella eri käyttäjien kohdalla sen mukaan, onko kolmas osapuoli antanut datan haltijalle luvan johtaa datasta tietoja.

Datan analysoitavuutta koskeva artikla rajoittaa tietojen hankkimista myös käänteismallinnuksen avulla. Datasäädöksen mukaan datan käyttäminen käänteismallinnukseen on sallittua³⁴⁷. Kyse on lähinnä selventävästä säännöksestä³⁴⁸, koska liikesalaisuusdirektiivi sallii jo käänteismallinnuksen esimerkiksi kilpailevan tuotteen kehittämiseksi³⁴⁹. Datasäädös kuitenkin asettaa käänteismallinnukselle rajoituksia, joita liikesalaisuusdirektiivissä ei ole säädetty. Ennen datasäädöstä käänteismallinnuksen käyttöä koskevat rajoitukset perustuivat sopimusten varaan. Liikesalaisuusdirektiivissä ei myöskään ole rajoituksia, jotka estäisivät datan hyödyntämisen tietojen johtamiseksi esimerkiksi taloudellisesta tilanteesta. Siten datasäädös rajoittaa laillisia keinoja hankkia liikesalaisuus.

³⁴² Datasäädös 4 artikla 13 kohta ja 5 artikla 6 kohta.

³⁴³ Datasäädös johdanto (27).

³⁴⁴ Ducuing 2022, s. 25–26.

³⁴⁵ Datasäädös 5 artikla 6 kohta.

³⁴⁶ Picht 2022, s. 20.

³⁴⁷ Datasäädös johdanto (32).

³⁴⁸ Aholainen – Schröder 2024.

³⁴⁹ Vapaavuori 2019, s. 115.

Liikesalaisuuksien suojan kannalta datasäädöksen 4 artiklan 10 kohdan rajoitus on olennainen, koska datan analyysin tuloksena voi paljastua kilpailuetua tarjoavia tietoja. Yleisesti käänteismallinnusta rajoittavien sääntöjen tavoitteena on suojata datan haltijan investointikannustimia³⁵⁰. Tämä on olennaista, koska datan analysointi voi johtaa liikesalaisuuksien paljastumiseen, vaikka jaettaisiin vain esimerkiksi luottamuksellisia tietoja³⁵¹. Lisäksi datan analysointia rajoittavat säännökset pyrkivät tasapainottamaan datan haltijan oikeudet ja innovoinnin edistämisen. Tämä tasapaino on kuitenkin herättänyt kritiikkiä, sillä säädöksen tulkinnallinen epäselvyys ja laaja soveltamisala voivat vähentää IoT-datan tuottamiseen liittyviä investointi- ja innovointikannustimia³⁵².

Yritykset, jotka käyttävät kehittyneitä datan analysointiteknologioita hyötyvät mahdollisuudesta analysoida dataa.³⁵³ Teknologian kehittyminen vaikuttaa siihen, millainen merkitys käänteismallinnuksella on liikesalaisuuksien suojan kannalta.³⁵⁴ Uudet teknologiat, kuten big data ja tekoäly, mahdollistavat prosessien ja tuotteiden käänteisen suunnittelun aiempaa resurssitehokkaammalla tavalla. Uusien teknologioiden avulla voidaan myös yhdistää dataa monista eri lähteistä ja analysoida suuria datamassoja, josta voidaan tehdä johtopäätöksiä ja ennusteita.³⁵⁵ Samalla ne tekevät liikesalaisuuksien suojaamisesta entistä vaikeampaa, mikä voi johtaa siihen, että liikesalaisuuksia paljastuu epäsuorasti esimerkiksi keräämällä ja analysoimalla valtavia määriä vähäarvoista dataa³⁵⁶. Asetuksen myötä esimerkiksi yrityksillä on käytössään enemmän dataa, joka voi helpottaa tuotteiden käänteismallinnusta. Se, miten hyvin asetuksen tuomat mahdollisuudet otetaan käyttöön, vaikuttaa siihen, laajentaako asetukset mahdollisuuksia hankkia liikesalaisuuksia laillisilla keinoilla.

Datasäädös saattaa luoda painetta valmistajille rajoittaa käänteismallinnusta sopimusten avulla, jos ne arvioivat liikesalaisuuksien olevan vaarassa paljastua. Erityisesti metadata voi tehdä raakadatasta tai esikäsittelystä datasta ymmärrettävää, mikä helpottaa sen analysointia³⁵⁷. Asetus voi siis antaa arvokasta dataa käyttäjille ja kolmansille osapuolille, jotka haluavat

³⁵⁰ Mylly 2024, s. 388.

³⁵¹ EPRS 2023, s. 8–9. AIOTI nosti esiin, että luottamuksellisten tietojen paljastaminen, voi johtaa liikesalaisuuksien paljastumiseen.

³⁵² Krämer – Colangelo – Richter 2023, s. 41. Esimerkiksi datan haltijat eivät ehkä tiedä, mitä toimia rajoitus kattaa.

³⁵³ Mylly 2024, s. 388.

³⁵⁴ Vapaavuori 2015, s. 115.

³⁵⁵ Nordberg 2020, s.211–212

³⁵⁶ Nordberg 2020, s. 210 ja 217–218.

³⁵⁷ WIPO 2024, s. 134.

selvittää liikesalaisuudet tutkimalla markkinoilla olevia tuotteita tai kehittämällä uusia innovaatioita.

Liikesalaisuusdirektiivi sallii sopimusehdot, jotka rajoittavat käänteismallinnusta ja itsenäistä kehitystyötä esimerkiksi lisenssisopimuksissa. Sopimuksella voidaan siis rajoittaa käänteismallinnusta, mutta kansallisella lailla voidaan rajoittaa tällaisia sopimusehtoja. Direktiiviä on tulkittu niin, että käänteismallinnusta ei saa rajoittaa sopimuksilla massamyyntituotteiden osalta. Sen sijaan valmistajat voivat yksipuolisesti määrätä vuokraus-, leasing- tai lisenssisopimusten ehdot, mukaan lukien ehdot, jotka estävät käänteisen suunnittelun tai purkamisen.³⁵⁸ Lisäksi sopimuksella voidaan kieltää liikesalaisuuksien ilmaiseminen ja käyttäminen, jos ne on hankittu käänteismallinnuksen avulla.³⁵⁹

Kansallisella lailla ei ole hyväksyttyä kieltää käänteismallinnusta täysin, vaan täytyy kunnioittaa direktiivin poikkeuksia. Kuitenkin direktiivin artikla 4 mahdollistaa kansalliset poikkeamat liikesalaisuuksien suojan laajentamiseksi eli jäsenvaltio voi laajentaa, mutta ei supistaa sitä, mitä pidetään liikesalaisuuden laittomana hankintana, käyttönä tai paljastamisena.³⁶⁰ Eli erot jäsenvaltioiden välillä voivat liittyä siihen, rajoitetaanko vapautta tehdä käänteismallista rajoittavia sopimusjärjestelyitä. Käänteismallinnusta rajoittavat sopimusehdot heikentävät kilpailua ja innovointia³⁶¹. Se, missä määrin hyväksytään käänteismallinnuksen kieltävät sopimuslausekkeet, ratkaistaan viime kädessä EU-tuomioistuimessa³⁶².

Käänteismallinnuksen kieltävien sopimusten täytäntöönpanokelpoisuus voi vaihdella EU:n jäsenvaltioiden välillä. Mahdollisuutta rajoittaa käänteismallinnusta sopimuksilla tulisi tulkita suppeasti, koska se on poikkeus sen sallivasta lähtökohdasta. Oikeuskirjallisuudessa on esitetty, että käänteismallinnuksen rajoituksia, jotka menevät pidemmälle kuin asetuksessa on säädetty, ei välttämättä sallita. Datan haltija ei voi yksipuolisesti asettaa datan käytölle muita rajoituksia, joita ei ole nimenomaisesti säädetty asetuksessa, koska ne voivat olla kohtuuttomia datasäädöksen 13 artiklan 5 kohdan nojalla.³⁶³

³⁵⁸ Aplin 2020, s. 14. Liikesalaisuusdirektiivin 3 artiklan 1 kohdan b alakohta ja johdanto (16). Ks. myös Nordberg 2020, s. 211–214. HE 49/2018, s. 59 ja 87.

³⁵⁹ Aplin 2020, s. 13.

³⁶⁰ Nordberg 2020, s. 214. Liikesalaisuusdirektiivi 1 artikla 1 kohta.

³⁶¹ Liikesalaisuusdirektiivin johdanto (16).

³⁶² Nordberg 2020, s. 217–218.

³⁶³ Mylly 2024, s. 388–389. Datasäädös 13 artikla 5 kohta. Sopimusehdon on oletettava olevan kohtuuton, jos sillä on jokin seuraavista tarkoituksista tai vaikutuksista: c) sillä estetään sopimuspuolta, jolle ehto on asetettu yksipuolisesti, käyttämästä toimittamaansa tai tuottamaansa dataa sopimuksen voimassaoloaikana tai rajoittaa mainitun datan käyttöä siinä määrin, että kyseisellä osapuolella ei ole oikeutta käyttää, kerätä, saada käyttöönsä tai valvoa tällaista dataa eikä hyödyntää tällaisen datan arvoa asianmukaisella tavalla.”

Suomessa ei ole toistaiseksi rajoitettu liikesalaisuuslailla sopimuksia, jotka kieltävät käänteismallinnuksen. Jos datan haltija voi sopimuksin rajoittaa käänteismallinnusta, voiko tämä estää datan paljastumisen ja tarjota liikesalaisuuksille vahvemman suojan kuin datasäädöksessä on alun perin on tarkoitettu. Siten ei ole selvää, täyttyykö datasäädöksen tehokasta soveltamista koskeva tavoite vai luodaanko sen sijaan tehottomuutta, mikäli sallitaan käänteismallinnusta rajoittavat sopimusehdot, jotka menevät pidemmälle kuin asetuksessa on säädetty. Innovointi ja kilpailun edistäminen kärsivät, jos sallitaan datan haltijoiden ottaa käyttöön laajat rajoitukset käyttää dataa käänteismallinnukseen.

4.3 Toimenpiteet liikesalaisuuksien suojaamiseksi

4.3.1 Oikeasuhteisista toimenpiteistä sopiminen

Datasäädöksen 4 artiklan 6 kohdan ja 5 artiklan 9 kohdan mukaan liikesalaisuudet on säilytettävä ja niitä saa ilmaista vain sillä edellytyksellä, että datan haltija ja käyttäjä toteuttavat ennen niiden ilmaisemista kaikki tarvittavat toimenpiteet niiden luottamuksellisuuden säilyttämiseksi, erityisesti suhteessa kolmansiin osapuoliin. Datan haltijan tai, kun kyse ei ole samasta henkilöstä, liikesalaisuuden haltijan, on yksilöitävä data, joka on suojattu liikesalaisuuksina, mukaan lukien asiaankuuluva metadata ja sovittava käyttäjän kanssa oikeasuhteisista teknisistä ja organisatorisista toimenpiteistä, jotka ovat tarpeen jaettavan datan luottamuksellisuuden säilyttämiseksi erityisesti suhteessa kolmansiin osapuoliin. Jos kolmas osapuoli asettaa vastaanottamaansa dataa toisen kolmannen osapuolen saataville, toisen kolmannen osapuolen on toteutettava kaikki datan haltijan ja ensimmäisen kolmannen osapuolen välillä sovitut tarvittavat toimenpiteet liikesalaisuuksien luottamuksellisuuden säilyttämiseksi³⁶⁴. Lisäksi datan haltija on yksin vastuussa liikesalaisuutena suojattavan datan yksilöimisestä ennen datan jakamista (*ex ante*)³⁶⁵. Tämä tarkoittaa, että datan haltijan on erotettava liikesalaisuudet muista luottamuksellisista tiedoista, koska liikesalaisuuksien suojaamiseksi tarkoitettuja mekanismeja ei voi soveltaa muihin tietoihin.³⁶⁶

Yksinkertaisimmillaan datasäädöksen datanjakomekanismi rakentuu kolmen sopimussuhteen ympärille: datan haltijan ja käyttäjän, datan haltijan ja kolmannen osapuolen sekä käyttäjän ja kolmannen osapuolen välillä. Ensimmäinen sopimussuhde muodostuu datan haltijan, kuten tuotteen valmistajan, ja käyttäjän välisestä kauppasopimuksesta, jossa sovitaan esimerkiksi tuotteen myynti- tai vuokrausehdoista ja datan jakamisesta. Toiseksi käyttäjän ja kolmannen

³⁶⁴ Datasäädös 6 artikla 2 artiklan c alakohta.

³⁶⁵ Komissio 2022d. Vt. datasäädösehdotuksen 5 artikla 8 kohdan mukaan *datan luonne liikesalaisuutena* ja toimenpiteet luottamuksellisuuden säilyttämiseksi on täsmennettävä datan haltijan ja kolmannen osapuolen välisessä sopimuksessa.

³⁶⁶ Hannes & Snellman 2024.

osapuolen välillä solmitaan palvelusopimus, joka kattaa esimerkiksi tuotteen huoltoa koskevat ehdot. Kolmanneksi datan haltija ja käyttäjän valitsema kolmas osapuoli tekevät datanjakosopimuksen, jossa määritellään datan luovutuksen ehdot. Lisäksi, jos tuotteen valmistaja ja liitännäispalveluntarjoaja ovat eri tahoja, syntyy neljäs sopimussuhde, jossa käyttäjä ja liitännäispalveluntarjoaja solmivat erillisen sopimuksen.³⁶⁷ Liikesalaisuuksien suojaamisesta tulee siis sopia käyttäjän ja datan haltijan sekä kolmannen osapuolen ja datan haltijan välillä.

Datasäädöksessä velvoitetaan datan haltija sopimaan toimenpiteistä käyttäjän kanssa. Tämä ei kuitenkaan estä datan haltijaa vapaaehtoisesti jakamasta dataa myös ilman erillisiä toimenpiteitä³⁶⁸. Datasäädöksen sanamuodosta käy kuitenkin ilmi, että datan haltijalla voi olla hallussaan kolmannen osapuolen liikesalaisuuksia, jolloin luottamuksellisuuden säilyttäminen on tarpeen.³⁶⁹ Mikäli datan haltija asettaa datan saataville ilman kyseisen kolmannen osapuolen suostumusta, se voi syyllistyä salassapitosäännösten rikkomiseen³⁷⁰.

Datasäädös edellyttää, että tekniset ja organisatoriset toimenpiteet ovat oikeasuhteisia. Oikeasuhteisten toimenpiteiden tulee olla vähintään kohtuullisia, jotta tiedot voivat ylipäätään saada liikesalaisuussuojaa³⁷¹. Oikeasuhteisuuden vaatimus voidaan käsittää siten, että asetuksessa tarkoitettujen toimenpiteiden tulee olla suhteellisia dataan haltijan, käyttäjään ja kolmannen osapuolen kannalta.³⁷² Oikeasuhteisuus asettaa kohtuullisille toimenpiteille ylärajan, joka perustuu siihen, mitä voidaan pitää suhteellisenä eri osapuolten näkökulmasta. Toimenpiteet, jotka ylittävät kohtuullisiksi katsottavat toimenpiteet, hyödyttävät yleensä yksinomaan liikesalaisuuden haltijaa, mutta voivat olla hyväksyttäviä, jos ne ovat asianmukaisia.³⁷³ Oikeasuhteisten toimenpiteiden vaatimus estää datan haltijaa käyttämästä väärin neuvotteluvoimaansa vaatimalla käyttäjältä tai kolmannelta osapuolelta ylimitoitettuja tai muuten kohtuuttomia suojatoimenpiteitä³⁷⁴. Toisaalta toimenpiteiden tulee olla tarpeen datan luottamuksellisuuden säilyttämiseksi eli toimenpiteiden tulee olla riittävän tehokkaita suojaamaan tietoja. Datasäädöksen myötä datan haltijan tulee siis ottaa huomioon datan käyttäjien ja vastaanottajien intressit ennen datan jakamista. Tämä kaventaa datan haltijan

³⁶⁷Krogerus 2024.

³⁶⁸ Hennemann – Ebner – Karsten 2023, s. 45.

³⁶⁹Picht 2022, s. 20. Komissio 2022d. Datasäädösehdotuksessa kysymys kolmannen osapuolen liikesalaisuussuojasta suojasta jäi avoimeksi.

³⁷⁰ Picht 2022, s. 38–39. Datasäädös 5 artikla 9 kohta ja 4 artikla 6 kohta.

³⁷¹ Liikesalaisuusdirektiivin 2 artiklan 1 kohdan c alakohda.

³⁷² Mylly 2024, s. 386.

³⁷³ Mylly 2022, s. 1459–1465.

³⁷⁴ Mylly 2024, s. 386. Radauer – Bader – Aplin ym. 2022, s. 90. Leistner – Antoine 2022, s. 90.

itsenäistä päätäntävaltaa liikesalaisuuksien suojaamisesta ja rajoittaa osittain sopimusvapauden laajuutta.

Johtoa oikeasuhteisuuden arvioinnissa huomioon otettavista seikoista voi saada liikesalaisuusdirektiivistä, jonka mukaan tuomioistuimen tulee ottaa huomioon oikeasuhteisuus arvioidessaan toimenpiteitä, kuten kiello- ja korjaustoimenpiteitä³⁷⁵. Siten toimenpiteiden oikeasuhteisuuden arvioinnissa tulisi ottaa huomioon ainakin liikesalaisuuden arvo ja muut erityispiirteet, kuten datakokonaisuuden laajuus. Kilpailuasemaan vaikuttavaa dataa, kuten markkina- ja kilpailukriittisiä tietoja, voidaan suojata tiukemmin kuin sellaista teknistä tai luovaa osaamista (know-how), joka ei ole yhtä arkaluontoista³⁷⁶. Lisäksi on arvioitava mahdolliset riskit, jotka liittyvät kolmansien osapuolten pääsyyn tai tiedon väärinkäyttöön. Olennaista on tarkastella, mitä teknisiä ja organisatorisia toimenpiteitä datan haltija on jo toteuttanut sen suojaamiseksi ja, ovatko nämä toimenpiteet riittäviä ja soveltuvia datan suojaamiseksi.

4.3.2 Tekniset ja organisatoriset toimenpiteet datan suojaamisessa

Datasäädöksen mukaan datan haltija voi vaatia sekä teknisiä että organisatorisia suojatoimenpiteitä. Tällaisia toimenpiteitä voivat olla esimerkiksi mallisopimusehdot³⁷⁷, salassapitosopimukset, tiukat pääsyprotokollat, tekniset standardit³⁷⁸ ja käytännesääntöjen soveltaminen. Tekniset toimenpiteet voivat puolestaan sisältää esimerkiksi salauksen tai älysopimusten³⁷⁹ hyödyntämistä tiedon väärinkäytön estämiseksi³⁸⁰. Yleensä organisatoriset toimenpiteet tarkoittavat käytäntöjä ja toimia, joilla rajoitetaan pääsyä tietoihin, kuten pääsyrajoitusten määrittäminen liiketiloihin tai datan säilyttämiseen. Teknologiset suojausmenetelmät puolestaan tarkoittavat digitaalisten oikeuksien hallintaa ja salauksen käyttöä.³⁸¹ Datan haltijalla on intressi ryhtyä toimenpiteisiin, jotka suojaavat liikesalaisuuksia,

³⁷⁵ HE 49/2018, s. 100. Liikesalaisuusdirektiivi 11 artikla 2 kohta ja 13 artikla 1 kohta. Mylly (2022, s. 1460–1461) on luokitellut oikeussuojakeinojen suhteellisuuden arvioinnissa huomioon otettavat neljään ryhmään: 1) liikesalaisuuden haltijan liittyvät, 2) oikeudenloukkaajan toimintaan liittyvät, 3) osapuolten etujen tasapainottaminen sekä 4) kolmansien osapuolten ja julkisen edun vaikutukset. Lista ei ole tyhjentävä, vaan muitakin seikkoja voidaan ottaa tapauksen mukaan huomioon.

³⁷⁶ Leistner – Antoine 2022, s. 10 ja 68. Leistner 2021 s. 929. Kilpailuprosessiin liittyviin liikesalaisuuksiin (esim. hinnoittelutiedot, asiakasprofiilit) pääsy-oikeudet tulisi myöntää tiukemmin ja vain, jos se on tarpeen kilpailun edistämiseksi.

³⁷⁷ Datasäädös 41 artiklan mukaan komission on määrä antaa ei-sitovia mallisopimusehtoja, joka koskevat muun muassa koskevat datan saatavuutta ja käyttöä ja liikesalaisuuksien suojaa (12.9.2025 mennessä).

³⁷⁸ Datasäädös johdanto (31). Asetus suosittelee teknisten standardien sekä käytännesääntöjen laatimista erityisesti liikesalaisuuksien suojaamiseksi.

³⁷⁹ Datasäädös 2 artikla 1 kohta 39 alakohta: älysopimuksella ”tietokoneohjelmaa, jota käytetään sopimuksen tai sen osan automaattiseen toteuttamiseen sähköisten tietueiden sarjan avulla ja siten, että niiden eheys ja niiden kronologisen järjestyksen oikeellisuus varmistetaan”.

³⁸⁰ Datasäädös 11 artikla 1 kohta.

³⁸¹ Fia 2020, s. 5–7.

joten säännöstä teknisistä ja organisatorisista toimenpiteistä voi pitää lähinnä selventävänä³⁸². Luottamuksellisten tietojen suoja tulisi nähdä olennaisena osana IoT-laitteiden kokonaisturvallisuutta ja sen tavoitteita. Suojatoimenpiteiden suunnittelussa on huomioitava IoT-laitteiden erityispiirteet, kuten niiden jatkuva yhteys internettiin sekä rajalliset resurssit laskentatehon, muistin ja energiankulutuksen osalta.³⁸³ Datasäädös asettaa teknisille toimenpiteille vähimmäisvaatimuksia, mutta jättää yrityksille liikkumavaraa valita sopivimmat käytännöt.

Datasäädöksen 11 artiklan mukaan datan haltija voi ottaa käyttöön asianmukaisia teknisiä suojatoimenpiteitä. Näitä toimenpiteitä voidaan käyttää estämään laitton pääsy dataan sekä varmistamaan datan saataville asettamista koskevien sopimusehtojen ja tiettyjen datasäädöksen 4, 5, 6, 8 ja 9 artiklojen noudattaminen. Artiklat, joihin viitataan liittyvät datanjakotilanteisiin esimerkiksi datan haltijan ja käyttäjän tai kolmannen osapuolen välillä sekä yritysten välisissä suhteissa. Teknisillä toimenpiteillä ei saa syrjiä datan vastaanottajia, estää käyttäjien tai datan vastaanottajien tiettyjä oikeuksia eikä loukata kolmannen osapuolen oikeuksia, jotka perustuvat unionin oikeuteen tai sen nojalla annettuun kansalliseen lainsäädäntöön.³⁸⁴ Liian laajat tekniset suojatoimet voivat antaa datan haltijoille liiallista valtaa rajoittaa käyttäjien pääsyä dataan ilman asianmukaisia rajoituksia³⁸⁵.

Teknisistä toimenpiteistä on muualla lainsäädännössä erilaisia määräyksiä, jotka tulee huomioida. Jos suojattu aineisto sisältää sekä tekijänoikeuden että datasäädöksen suojaamaa dataa, tulee noudattaa lisäksi, mitä tietoyhteiskuntadirektiivin 6 artiklassa säädetään teknisistä toimenpiteistä.³⁸⁶ Lisäksi, jos aineisto kattaa sekä henkilötietoja että ei-henkilötietoja, siihen soveltuu sekä datasäädös että yleinen tietosuojasetus. Yleisen tietosuojasetuksen nojalla rekisterinpitäjän ja henkilötietojen käsittelijän tulee toteuttaa asianmukaiset tekniset- ja organisatoriset toimenpiteet, jotka ovat erityisesti kohdennettu henkilötietojen suojaan³⁸⁷. Liikesalaisuuksien suojaamisessa voisi noudattaa samanlaista lähestymistapaa teknisiin ja organisatorisiin toimenpiteisiin kuin tietosuojalainsäädännön yhteydessä.

Tekniset suojaukset, kuten koodin ja sen taustalla olevan algoritmin hämärtäminen, salaustasojen tiukat pääsyvalvonnat, sekä valtuuttamattoman pääsyn tai kopioinnin estäminen, ovat erityisen

³⁸² Grafenstein 2022, s. 3.

³⁸³ Schiller – Aidoo – Fuhrer 2022, s. 6–7 ja 15.

³⁸⁴ Datasäädös johdanto (57).

³⁸⁵ Moscon 2023 s. 2–3 ja 13.

³⁸⁶ De Noyette – Stähler - Margoni 2024, s. 20.

³⁸⁷ GDPR 32 artikla. GDPR johdanto (78). Rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava asianmukaiset tekniset ja organisatoriset toimenpiteet, kuten pseudonymisointi, salaustasojen tiukat pääsyvalvonnat, sekä valtuuttamattoman pääsyn tai kopioinnin estäminen, ovat erityisen

tärkeitä liikesalaisuuksien suojaamisessa³⁸⁸. Tekniset suojaustoimenpiteet ovat ratkaisevan tärkeitä liikesalaisuuksien suojaamisessa digitaalisessa ympäristössä. Näihin kuuluu tekniset pääsyn rajoitukset sekä tekniset valvontamekanismit. Salauksessa voidaan erottaa symmetrinen ja epäsymmetrinen salaus. Salausmetodeja on erilaisia. Symmetrisessä salauksessa käytetään samaa avainta tietojen salaamiseen ja purkamiseen, kun taas epäsymmetrisessä salauksessa käytetään kahta eri avainta. Homomorfinen (eng. homomorphic encryption) salaus on tekniikka, joka mahdollistaa tietojen analysoimisen ja käsittelyn, vaikka ne ovat edelleen salattuja. Homomorfisen salauksena avulla dataa voidaan käsitellä ilman, että se puretaan salaamattomaan muotoon. Turvallinen monen osapuolen laskenta (eng. Secure multiparty computation, SMC) tarkoittaa menetelmää, jossa kukin osapuoli syöttää omat tietonsa laskentaan ja saa käyttöönsä vain oman osuutensa tuloksista ilman pääsyä muiden tietoihin kokonaisuudessaan. Yhteenvedona voidaan todeta, että kaksi viimeistä salauskeinoa ovat tehokkaita liikesalaisuuksien suojaamisessa, koska ne mahdollistavat datan käytön, ilman että liikesalaisuudet paljastuvat. Nämä teknologiat, samoin kuin lohkoketjuteknologian käyttäminen dataan, mahdollistavat liikesalaisuuksien suojaamisen³⁸⁹. Se, ovatko toimenpiteet liikesalaisuusdirektiivin mukaan kohtuullisia, riippuu toimenpiteiden kustannuksista ja toteuttamiskelpoisuudesta³⁹⁰. Toisin sanoen ei voida edellyttää esimerkiksi teknisiä toimenpiteitä, joiden kustannukset ylittävät tietojen suojaamisesta saatavat hyödyt.

Organisatoriset toimenpiteet painottuvat erityisesti henkilöstön kouluttamiseen ja datan hallinnan käytäntöjen selkeyttämiseen. Näihin toimenpiteisiin kuuluu, että tiedot ovat saatavilla ja käytettävissä vain niille henkilöille tai tahoille, joilla on ennalta määritelty tarve ja tarkoitus datan käyttöön. Tämä koskee sekä fyysistä pääsyä että digitaalista käyttöä³⁹¹. Pääsyä arkaluonteisiin tietoihin tulee rajoittaa ja tärkeisiin tietoihin minimoida tehokkaasti. Organisatorisia toimenpiteitä tukevat sopimukset, kuten salassapitosopimukset, jotka velvoittavat kaikkia datan käsittelyyn osallistuvia suojaamaan liikesalaisuuksia.³⁹² Sopimukset eivät kuitenkaan yksin riitä, koska datan jakamien ja pääsyyn oikeutettujen osapuolten määrän kasvu tekevät sopimuksista haavoittuvia. Liikesalaisuuksien suojatoimenpiteiden tulee mahdollistaa sekä liikesalaisuuksien suojaaminen että dataan pääsy.³⁹³

³⁸⁸ WIPO 2024, s. 55–56.

³⁸⁹ Hauck 2021, s. 25–28.

³⁹⁰ Wiebe – Schur 2019, s. 819–821.

³⁹¹ WIPO 2024, s. 53–54. Esimerkkejä tällaisista keinoista ovat valvontajärjestelmät, pääsyräjoitukset, tunnistautumisjärjestelmät ja menettelyohjeet. Mylly 2024, s. 385.

³⁹² Wiebe – Schur 2019, s. 819. Salassapitosopimuksista ks. tarkemmin Vapaavuori 2019. Oesch 2024, s. 176–211.

³⁹³ Wiebe-Schur 2019, s. 818–819.

4.4 “Liikesalaisuuksien käsijarru”-mekanismi

4.4.1 Oikeus pidättäytyä tai keskeyttää datan jakaminen

Datasäädöksen 4 artiklan 7 kohdan ja 5 artiklan 10 kohdan mukaan datan haltija voi pidättäytyä liikesalaisuuksiksi määritetyn datan jakamisesta tai tapauksen mukaan keskeyttää sen, jos liikesalaisuuksien luottamuksellisuutta ei voida säilyttää. Näin on tapauksessa, jossa 1) tarpeellisista toimenpiteistä ei päästä sopimukseen, 2) käyttäjä tai kolmas osapuoli ei toteuta sovittuja toimenpiteitä tai 3) heikentää liikesalaisuuksien luottamuksellisuutta. Tällaisissa tapauksissa datan haltijan on ilmoitettava datan jakamisen pidättäytymisestä tai keskeyttämisestä kansalliselle toimivaltaiselle viranomaiselle, ja yksilöitävä, mitä toimenpiteitä ei ole sovittu tai pantu täytäntöön, sekä tapauksen mukaan minkä liikesalaisuuksien luottamuksellisuus on vaarantunut. Datan haltijan päätös on perusteltava asianmukaisesti, ja toimitettava käyttäjälle tai kolmannelle osapuolelle kirjallisesti ilman aiheetonta viivästystä.

Käytännössä datasäädös edellyttää, että kansallinen viranomainen arvioi datan haltijan päätöksen laillisuuden tapauskohtaisesti. Arvioinnissa otetaan huomioon muun muassa se, onko sopimuksen puuttuminen seurausta siitä, että datan haltija vaatii suhteettomia toimenpiteitä liikesalaisuuksien suojaamiseksi. Jos sopimus on olemassa, mutta käyttäjä tai kolmas osapuoli ei noudata sovittuja toimenpiteitä, arvioidaan, ovatko nämä toimenpiteet kohtuullisia ja toteutettavissa. Lisäksi huomioidaan, onko käyttäjä tai kolmas osapuoli toteuttanut toimenpiteet sopimuksen mukaisesti tai onko luottamuksellisuus muuten vaarantunut. Viranomaisen tulee arvioida myös, onko ylipäätään tehty pätevä liikesalaisuusväite eli täyttääkö tieto liikesalaisuudelle asetetut ehdot ja pystyykö datan haltija osoittamaan tämän.³⁹⁴ Jotta datan haltijan päätös voidaan hyväksyä, siinä tulee vedota objektiivisiin seikkoihin. Pelkkä subjektiivinen epäluottamus esimerkiksi kolmatta osapuolta kohtaan, ei itsessään muodosta asianmukaista perustetta. Joka tapauksessa kynnys keskeyttää datan jakaminen liikesalaisuuksien turvaamiseksi on matalampi kuin kynnys kieltäytyä kokonaan jakamasta liikesalaisuuksia sisältävää dataa. Tämän tulee vaikuttaa myös siihen, millä perusteilla keskeytyspäätös voidaan hyväksyä.

Liikesalaisuuksien suojaamisen haasteena on varmistaa suojatoimenpiteiden toteutus ja ylläpito, erityisesti kun dataa jaetaan toiselle kolmannelle osapuolelle, johon datan haltijalla ei ole suoraa sopimussuhdetta. Koska toissijaisella kolmannelle osapuolella ei ole ilmoitusvelvollisuutta, datan haltijan valvontamahdollisuudet ovat rajalliset. Oikeuskirjallisuudessa on katsottu, että datan haltija voi keskeyttää tiedon jakamisen

³⁹⁴ De Noyette – Stähler - Margoni 2024, s. 15–16.

ensisijaiselle kolmannelle osapuolelle, jos toinen kolmas osapuoli esimerkiksi siirtää dataa eteenpäin ilman käyttäjän suostumusta tai riittäviä suojausmekanismeja. Siksi on olennaista sopia ensimmäisen kolmannen osapuolen kanssa ilmoitusvelvollisuudesta ja jakamisen keskeyttämisoikeudesta.³⁹⁵

Datasäädöksen mukainen oikeus pidättäytyä tai keskeyttää datan jakaminen on hyödyllinen erityisesti tilanteessa, jossa datan haltijan hallussa on toisen osapuolen liikesalaisuuksia. Tällöin datan jakamisesta kieltäytyminen voi olla vastoin datasäädöstä. Toisaalta datan haltija voi datan saataville asettamisella rikkoa salassapitovelvollisuuksia.³⁹⁶ Siten sääntely osaltaan estää datan haltijaa joutumasta kohtuuttomaan tilanteeseen.

4.6.2 Oikeus kieltäytyä datan jakamisesta

Datasäädöksen 4 artiklan 8 kohdan ja 5 artiklan 10 kohdan mukaan datan haltija voi tapauskohtaisesti ja poikkeuksellisesti evätä pääsypyynnön liikesalaisuuksia sisältävään dataan. Tämä on mahdollista, jos datan haltija pystyy poikkeuksellisissa olosuhteissa osoittamaan, että liikesalaisuuksien ilmaisemisesta aiheutuu sille erittäin todennäköisesti vakavaa taloudellista vahinkoa, vaikka käyttäjä tai kolmas osapuoli on toteuttanut vaaditut tekniset ja organisatoriset toimenpiteet. Kieltäytymisestä on ilmoitettava kansalliselle toimivaltaiselle viranomaiselle, ja päätös on perusteltava objektiivisin seikoin sekä toimitettava käyttäjälle tai kolmannelle osapuolelle kirjallisesti ilman aiheetonta viivytystä.

Perustelujen tulee nojata asianmukaisesti objektiivisiin seikkoihin, kuten liikesalaisuuksien suojan täytäntöönpanokelpoisuuteen kolmansissa maissa, pyydetyn datan luonteeseen ja luottamuksellisuuden tasoon tai tuotteen ainutlaatuisuuteen ja uutuuteen. Lista ei ole tyhjentävä, joten myös muita perusteluja voi käyttää tapauskohtaisesti. Perusteluissa voidaan ottaa huomioon myös datan saataville asettamisesta aiheutuva kielteinen vaikutus kyberturvallisuuteen.³⁹⁷ Tämä on ymmärrettävää, koska liikesalaisuudet ovat erityisen alttiita kyberhyökkäyksille niiden korkean taloudellisen arvon ja salassapitovaatimusten vuoksi.³⁹⁸

Asetuksen johdanto-osan mukaan vakava taloudellinen vahinko tarkoittaa vakavia ja korjaamattomia taloudellisia menetyksiä³⁹⁹. Datasäädösehdotukseen sisältyi vielä lisäys, jonka mukaan vakavat taloudelliset vahingot uhkaavat datan haltijan toimintakykyä tai aiheuttavat vakavan konkurssiriskin⁴⁰⁰. Liikesalaisuuksia sisältävän datan jakamisesta kieltäytyminen on

³⁹⁵ Datasäädös 6 artikla 2 kohta c alakohta. Noyette - Stähler - Margoni 2023, s. 9–10.

³⁹⁶ Drexl – Banda - Gonzalez Otero ym. 2022, s. 102–203.

³⁹⁷ Datasäädös johdanto (31).

³⁹⁸ Ettredge - Yijun 2018, s. 564. Atkinson 2019, s. 6.

³⁹⁹ Datasäädös johdanto (31).

⁴⁰⁰ Neuvosto 2023, kohta 28a.

siis sallittua vain, jos liikesalaisuuksien ilmaiseminen uhkaa yrityksen elinkelpoisuutta. Datasäädös erottelee niin sanotusti tavalliset liikesalaisuudet ja erityisen arvokkaat liikesalaisuudet, joiden ilmaiseminen voi johtaa vakavaan taloudelliseen vahinkoon⁴⁰¹. Käytännössä vain pieni osa yritysten hallussa olevista liikesalaisuuksista on erittäin arvokkaita⁴⁰². Siten minkä tahansa suoran taloudellisen vahingon mahdollisuus ei riitä perusteeksi evätä datapyyntöä. Kynnys ei välttämättä ylity, vaikka datan jakaminen paljastaisi kriittisiä tietoja tuotteen toiminnasta tai merkittävästi lisäisi riskiä liikesalaisuuksien tai immateriaalioikeuksien paljastumisesta esimerkiksi takaisinmallinnuksen avulla.⁴⁰³ Tällöin datan haltijalla voi kuitenkin olla oikeus keskeyttää datan jakaminen esimerkiksi, jos käyttäjä ei toteuta kaikkia sovittuja toimenpiteitä liikesalaisuuksien suojaamiseksi. Sen sijaan EU:n yleisen tuomioistuimen oikeuskäytännössä on katsottu esimerkiksi, että uuden tieteellisen päätelmän tai innovatiivisen strategian paljastaminen voi vakavasti vaarantaa oikeushenkilön kaupalliset edut⁴⁰⁴. Nämä ovat esimerkkejä perustelujen objektiivisista seikoista, jotka voivat liittyä tuotteen uutuuteen tai ainutlaatuisuuteen.

Objektiiviset seikat, jotka voivat perustella pääsyyntöön epäämistä voivat liittyä myös liikesalaisuuksien suojan täytäntöönpanokelpoisuuteen kolmansissa maissa. Kolmannen maan lain nojalla tehty pyyntö voi olla ristiriidassa liikesalaisuuksien suojaa koskevien EU:n sääntöjen tai kansallisen lainsäädännön kanssa. Tällöin on tärkeää arvioida, noudattaako kyseisen maan oikeusjärjestelmä oikeasuhteisuuden periaatetta, antaako se selkeät perustelut päätöksille ja tarjoaako se vastaanottajalle mahdollisuuden valittaa päätöksestä tuomioistuimeen.⁴⁰⁵

Datasäädöksen soveltamisalaan kuuluvaa dataa voidaan lähtökohtaisesti asettaa saataville ilman, että siitä aiheutuu erittäin todennäköisesti vakavaa taloudellista vahinkoa datan haltijalle. Toiseksi oletuksena on, että liikesalaisuuksia sisältävän datan luottamuksellisuus voidaan taata suojatoimenpiteillä. Poikkeuksellisten olosuhteiden määrittely edellyttää tapauskohtaista arviointia. Poikkeukselliset olosuhteet voivat olla käsillä, jos oikeasuhteisia teknisiä ja organisatorisia suojaustoimenpiteitä ei ole käytettävissä⁴⁰⁶. Erittäin todennäköisesti viittaa

⁴⁰¹ Freshfields 2023.

⁴⁰² Searle 2021, s. 17.

⁴⁰³ ZVEI 2023, s. 5–8.

⁴⁰⁴ Asia T-235/15 (PariPharma vEMA) kohdat 71 ja 108. Tapauksessa on viitattu Euroopan parlamentin ja neuvoston asetukseen (EY) N:o 1049/2001, erityisesti sen 4 artiklan 2 kohtaan, koskien asiakirjojen saantia yleisön tutustuttavaksi. Tuomioistuin korosti, että yrityksen on kuvattava "konkreettisesti ammatillinen ja kaupallinen merkitys, joka kyseisillä tiedoilla on kantajalle" sekä osoitettava "konkreettisesti ja tosiasiallisesti", millä tavoin kilpailijat voisivat hyötyä tiedon julkistamisesta markkinoille pääsyä varten.

⁴⁰⁵ Datasäädös johdanto (101).

⁴⁰⁶ Freshfields 2023.

siihen, että jotain tapahtuu lähes varmasti. Vahingon katsotaan tapahtuvan erittäin todennäköisesti, kun syy-seuraussuhde on selkeä. Tällöin liikesalaisuuden haltijalla on perusteltu syy epäillä, että datan jakamisesta aiheutuisi vakavaa vahinkoa.

Käyttäjä tai kolmas osapuoli, joka haluaa riitauttaa datan haltijan päätöksen datapyynnön epäämisestä, datan jakamisesta pidättymisestä tai sen keskeyttämisestä, voi tehdä valituksen toimivaltaiselle viranomaiselle. Viranomaisen on ilman aiheetonta viivytystä päätettävä, aloitetaanko datan jakaminen tai jatketaanko sitä ja millä edellytyksillä. Viranomaisen tulee päättää, onko todennäköistä, että datan haltijalle aiheutuu vakavaa taloudellista haittaa tietojen paljastumisesta⁴⁰⁷. Jos datan haltija ja käyttäjä eivät pääse sopimukseen datan jakamisen ehdoista, on epäselvää, millä keinoilla ja kuinka tehokkaasti liikesalaisuudet suojataan. Vaihtoehtoisesti käyttäjä voi sopia datan haltijan kanssa asian saattamisesta riidanratkaisuelimen käsiteltäväksi.⁴⁰⁸ Viranomaismenettely ei rajoita oikeutta hakea muutosta jäsenvaltion toimivaltaisessa tuomioistuimessa. On olennaista, että viranomaiset toimivat ripeästi, jotta datan haltijat eivät voi käyttää tätä mahdollisuutta perusteettomasti viivyttääkseen datan saataville asettamista, johon datasäädöksen 4 artiklan 1 kohta velvoittaa ilman aiheetonta viivästystä.

Oikeus pidättyä datan jakamisesta tarkoittaa datan haltijan veto-oikeutta, jonka avulla se voi evätä datapyynnön ja asettaa arvokkaat liikesalaisuudet etusijalle suhteessa dataan pääsyyn. Vaikka datan haltijalle on annettu mahdollisuuksia vedota liikesalaisuuksien suojaan, tietojen suojaamisen on arvioitu muuttuvan vaikeammaksi asetuksen myötä⁴⁰⁹. Käytännössä datan haltijoille annettu mahdollisuus voi johtaa siihen, että datan haltijat pyrkivät manipuloimaan datan jakamisen prosessia⁴¹⁰. Toisaalta kynnys datapyynnön epäämiselle on asetettu korkealle⁴¹¹. Poikkeuksen soveltamisalaa tulisi tulkita niin, että se soveltuu vain erityisissä ja hyvin rajallisissa tilanteissa⁴¹². Käytännössä liikesalaisuuksiin vetoaminen voi olla riskialtista ja kallista. Viime kädessä datasäädöksen soveltamiskäytäntö määrittää, kuinka herkästi datan haltijat vetoavat tähän mahdollisuuteen olla jakamatta dataa⁴¹³.

4.5 Datan luvaton käyttö ja luovuttaminen

Tilanteessa, jossa datan haltija kieltäytyy tai pidättäytyy jakamasta dataa, syynä voi olla esimerkiksi vastaanottajan syyllistyminen väärinkäytöksiin, kuten harhaanjohtamiseen tai

⁴⁰⁷ De Noyette – Stähler - Margoni 2024, s. 15–16.

⁴⁰⁸ Datasäädös 4 artikla 9 kohta ja 5 artikla 12 kohta ja johdanto (31).

⁴⁰⁹ Hannes & Snellman 2023.

⁴¹⁰ Mylly 2024, s. 368 ja 387.

⁴¹¹ Hannes & Snellman 2023.

⁴¹² Mylly 2024, s. 387.

⁴¹³ Keltto 2024. Hannes & Snellman 2023.

datan luvattomaan käyttöön. Tällöin datan haltija voi pyytää oikaisutoimenpiteitä, kuten tuotannon lopettamista tai myynnin keskeyttämistä. Datan haltijan pyyntöjä tulee arvioida suhteessa osapuolten etuihin⁴¹⁴.

Datasäädöksen 11 artiklan 2 kohdan mukaan datan haltija tai, kun ei ole kyse samasta henkilöstä, liikesalaisuuden haltija voi esittää kolmannelle osapuolelle, käyttäjälle tai datan vastaanottajalle pyyntöjä, jos sopimuksen tai luovutuksen ehtoja ei noudateta. Luvaton datankäyttöä vastaan suojaavat toimet voivat koskea liikesalaisuuksia tai muuta dataa. Datasäädöksen 11 artiklan 3 kohdan mukaan suojaustoimenpiteitä voidaan pyytää, jos kolmas osapuoli tai datan vastaanottaja on a) käyttänyt väärin datan haltijan teknisen infrastruktuurin puutteita⁴¹⁵, antanut vääriä tietoja datan haltijalle tai käyttänyt harhauttavia tai pakottavia keinoja, b) käyttänyt dataa luvattomaan tarkoitukseen, kuten kilpailevan verkkoon liitetyn tuotteen kehittämiseen, c) luovuttanut dataa luvatta toiselle osapuolelle, d) laiminlyönyt tekniset ja organisatoriset toimenpiteet, e) muuttanut tai poistanut teknisiä suojatoimenpiteitä. Datasäädöksen 11 artiklan 2 kohdan nojalla pyyntö voi koskea a) datan poistamista, b) datan perustella tuotettujen tuotteiden, johdetun datan ja palveluiden tuotannon lopettamista, c) ilmoituksen tekemistä käyttäjälle luvattomasta käytöstä tai d) korvauksen maksamista datan haltijalle. Artiklan b) kohdan vaatimus edellyttää lisäksi, että tällainen toimenpide ei ole suhteeton datan haltijan, liikesalaisuuden haltijan ja käyttäjän etuihin nähden ja on olemassa vakava riski, että kyseisen datan laitton käyttö aiheuttaa merkittävää haittaa datan haltijalle, liikesalaisuuden haltijalle tai käyttäjälle.⁴¹⁶ Asetuksen 11 artiklan 4 kohdan mukaan pyyntö voidaan esittää käyttäjille vain jos, käyttäjä ei pidä voimassa teknisiä ja organisatorisia toimenpiteitä liikesalaisuuksien suojaamiseksi tai muuttaa tai poistaa datan haltijan teknisiä suojatoimenpiteitä.⁴¹⁷

Datasäädöksen 11 artiklan 2 kohdan b alakohdan tarkoituksena on tasapainottaa käyttäjälle ja kolmannelle osapuolelle asetettavat ankarat seuraamukset sekä liikesalaisuuden haltijalle aiheutuvat haitat. Säännöksen sanamuodon perusteella vaikuttaa kuitenkin siltä, että siinä korostuu ensisijaisesti datan haltijan kaupallisten etujen suojaaminen. Oikeuskirjallisuudessa on esitetty, että toimenpiteitä tulisi soveltaa vain hyvin poikkeuksellisissa tilanteissa, sillä säädetyt toimenpiteet ovat luonteeltaan ankaria. Toistaiseksi ei ole kehitetty selkeitä menetelmiä, joiden perusteella voitaisiin arvioida, onko luvaton uudelleenkäyttö aiheuttanut merkittävää vahinkoa datan haltijalle tai onko liiketoiminnan lopettaminen kohtuullinen

⁴¹⁴ Datasäädös johdanto (57).

⁴¹⁵ Datasäädös 4 artikla 11 kohta ja 5 artiklan 5 kohta.

⁴¹⁶ Datasäädös 11 artikla 2 kohta b alakohhta.

⁴¹⁷ Krogerus 2024. Ks. myös datasäädös johdanto (57).

toimenpide datan luvattomasta käytöstä. Datan haltijalla on todistustaakka siitä, että toimenpiteet, kuten tavaroiden tuotannon lopettaminen, eivät ole suhteettomia tai että niiden laiminlyönti aiheuttaa merkittävää haittaa. On kuitenkin epäselvää, millainen näyttö riittää osoittamaan vaatimusten rikkomisen. Samalla jää epäselväksi, millaisia todisteita käyttäjältä vaaditaan väitteiden kumoamiseksi. Tulkita selkeytyy todennäköisesti komission ohjeiden tai ennakkotapausten myötä.⁴¹⁸ Lopulta asia tarkentuu oikeuskäytännön ja viranomaisten päätöksentekokäytännön kautta.⁴¹⁹

Datasäädös täydentää olemassa olevaa liikesalaisuussäätelyä muun muassa säätämällä uusista oikeussuojakeinoista liikesalaisuuksien suojaamiseksi. Lisäksi liikesalaisuusdirektiivissä säädettyt oikeussuojakeinot ovat voimassa.⁴²⁰ Koska datasäädöksen oikeussuojakeinot soveltuvat myös muuhun dataan kuin liikesalaisuuksiin, niiden soveltamisala on liikesalaisuusdirektiiviä laajempi⁴²¹. Koska sääntely on osittain päällekkäistä, voi lähteä siitä, että asetuksessa mainitaan liikesalaisuudet lähinnä selventävässä tarkoituksessa⁴²².

Datasäädöksen 11 artiklassa säädetty toimenpiteet ovat osittain päällekkäisiä oikeussuojakeinojen kanssa, joista säädetään liikesalaisuusdirektiivissä. Liikesalaisuusdirektiivi mahdollistaa kielto- ja korjaavatoimenpiteet, kun liikesalaisuus on hankittu, käytetty tai paljastettu laittomasti. Lisäksi direktiivi tarjoaa mahdollisuuden vahingonkorvaukseen, jos oikeudenloukkaaja osapuoli tiesi tai olisi pitänyt tietää toimivansa laittomasti.⁴²³ Liikesalaisuusdirektiivi edellyttää myös, että tuomioistuin arvioi toimenpiteiden oikeasuhteisuuden ottaen huomioon muun muassa perusoikeudet ja yleisen edun.⁴²⁴

Datasäädöksessä säädetty oikeussuojakeinot kuitenkin eroavat liikesalaisuusdirektiivin seuraamuksista monella tavalla. Ensinnäkin liikesalaisuusdirektiivin mukaiset toimenpiteet edellyttävät tuomioistuimen päätöstä, kun taas datasäädöksen toimenpiteet voidaan määrätä haltijan tai tapauksen mukaan, kun kyse ei ole samasta henkilöstä, liikesalaisuuden haltijan tai käyttäjän pyynnöstä. Toiseksi datasäädöksen toimenpiteet voidaan määrätä kolmatta osapuolta vastaan riippumatta siitä, tiesikö se tai olisiko sen pitänyt tietää toimivansa lainvastaisesti. Kolmas keskeinen ero liittyy arvioinnissa huomioon otettaviin seikkoihin. Lukuun ottamatta datasäädöksen 11 artiklan 2 kohdan b alakohdan soveltamista, suhteellisuusperiaate ei ole

⁴¹⁸ Atik 2022, s. 20–21.

⁴¹⁹ Grafenstein 2022, s. 28. Ks. Datasäädös 10 artikla ja 36 artikla.

⁴²⁰ Euroopan komissio 2024, s. 7 ja 29. Komissio 2022a, s. 144.

⁴²¹ Mylly 2024, s. 386–387. Datasäädös kieltää minkä tahansa datan (ei siis vain liikesalaisuuksien), joka on peräisin alkuperäisen datan haltijan tuotteesta, käyttämisen kilpailevan tuotteen kehittämiseen.

⁴²² IPR University 2024.

⁴²³ Ks. Liikesalaisuusdirektiivin 12 ja 14 artiklat.

⁴²⁴ Liikesalaisuusdirektiivi 13 artikla 1 kohta a-h alakohdat.

selkeästi huomioon otettava seikka seuraamuksia määrättäessä. Siten datasäädös 11 artikla 2 kohta antaa vahvemman mekanismin kielto- ja korjaustoimenpiteiden käyttöön kuin liikesalaisuusdirektiivi. Näin ollen datasäädöksen mukaisia seuraamuksia on mahdollista soveltaa laajemmin kolmansia osapuolia vastaan. Liikesalaisuusdirektiivi ei myöskään ulotu johdettuun dataan, toisin kuin datasäädöksen 11 artiklan 2 kohdan b) alakohta.

5. JOHTOPÄÄTÖKSET

Liikesalaisuussuoja on yksi yleisimmin käytetyistä keinoista aineettoman varallisuuden suojaamiseksi niin EU:ssa kuin maailmanlaajuisesti⁴²⁵. Liikesalaisuusdirektiivin 2 artiklan liikesalaisuuden määritelmä soveltuu melko joustavasti IoT-dataan. IoT-ympäristössä salassapidon haasteita lisäävät datan dynaamisuus, keräysympäristön avoimuus sekä yksittäisten osien helppo saatavuus tai paljastuminen⁴²⁶. Tästä huolimatta salaisuus voi säilyä, jos tieto pysyy salassa kokonaisuutena. IoT- datan salaisuus liittyy usein datakokonaisuuteen, yhdistelmään tai sen erityiseen rakenteeseen. Tämä tarkoittaa, että data voi säilyä salaisena, vaikka yksittäinen tieto olisi muiden nähtävissä ja helposti saatavissa, kuten yleiseltä tietä kerätty data. Lisäksi liikesalaisuusdirektiivin edellyttämä salaisuus on suhteellista, mikä mahdollistaa tiedon jakamisen yrityksen ulkopuolelle, kuten lisensoinnin kautta. Kuitenkin laajamittainen jakaminen voi johtaa tietojen muuttumiseen yleisesti tunnetuiksi. Tällöin liikesalaisuusasema voi vaarantua erityisesti, jos datan vastaanottajat eivät suojaa tietoja riittävästi.⁴²⁷ Tämä herättää kysymyksen siitä, kuinka laajalle tieto voi levitä säilyttäen salaisuutensa ja milloin se muuttuu yleisesti tunnetuksi kyseisellä toimialalla. Jos datan haltijat pitävät liikesalaisuuksien paljastumista todennäköisempänä datasäädöksen myötä, he voivat olla halukkaampia suojaamaan tietoja immateriaalioikeuksilla, kuten patenteilla.

Samoin yksittäisellä raakadatalla ei todennäköisesti ole taloudellista arvoa, mutta yhdistelmät tai ainutlaatuisesti järjestetyt datakokonaisuudet voivat olla oikeutettuja liikesalaisuussuojaan. Taloudellisen arvon kynnyks on matala, koska liikesalaisuusdirektiivi ei edellytä, että tiedon arvo olisi merkittävä. Siksi on tärkeää välttää liian laajaa tulkintaa siitä, mitkä tiedot ovat taloudellisesti arvokkaita. Raakadatan taloudellinen arvo perustuu usein mahdollisuuteen käsitellä ja analysoida sitä⁴²⁸. Datan taloudellisen arvon tulee olla datan haltijan ennakoitavissa ja perustua sen salassapitoon, mikä luo selkeän yhteyden salaisuuden ja taloudellisen arvon välille. Pelkkä mahdollisuus, että tieto voisi joskus olla hyödyllistä esimerkiksi big data -analyysissä, ei tee siitä automaattisesti taloudellisesti arvokasta. Tämä korostaa sitä, ettei esimerkiksi kaikkea raakadataa voida pitää potentiaalisesti arvokkaana vain siksi, että sitä voidaan analysoida. Lisäksi potentiaalisesti arvokkaaksi tulisi katsoa vain sellainen tieto, jonka datan haltija on luovutushetkellä tunnistanut taloudellisesti arvokkaaksi. Liian laaja tulkinta

⁴²⁵ Wiebe - Schur 2019, s. 814.

⁴²⁶ Banterle 2018, s. 7.

⁴²⁷ Banterle 2018, s. 7. Komissio 2016, s. 10–11.

⁴²⁸ Banterle 2018, s. 7. Komissio 2016, s. 10–12. Jokainen dataan myönnetty lisenssi tuo mukanaan riskin, että hallinta katoaa, jos lisenssinsaaja ei noudata vaatimuksia datan asianmukaisesta suojaamisesta.

taloudellisesta arvosta voi johtaa siihen, että vähäarvoiset tiedot tulkitaan liikesalaisuuksiksi vastoin liikesalaisuusdirektiiviä.

Kohtuullisten toimenpiteiden määritelmän avoimuus ja tilannekohtaisuus, tekee siitä haastavimman kriteerin. Kohtuullisten toimenpiteiden vaatimus kytkeytyy liikesalaisuuksien yksilöintiin ja datan haltijan määrittelyyn, mikä voi olla vaikeaa IoT-ympäristössä. Liikesalaisuudet on yksilöitävä ennen kohtuullisiin toimenpiteisiin ryhtymistä, mikä on edellytys liikesalaisuuksien tehokkaalle suojalle. Siten yksilöintivaatimus on osa liikesalaisuuden määritelmää. Kohtuullisten toimenpiteiden vaatimus liittyy siihen, miten datan haltija kykenee hallitsemaan ja suojaamaan tietoa. Erityisesti IoT-tuotteiden muodostamassa verkottuneessa ympäristössä voi olla vaikeaa määrittää, kuka on todellinen liikesalaisuuden haltija. Datasäädös voi johtaa lukuisten sopimusten olemassaoloon useiden käyttäjien ja kolmansien osapuolten kanssa. Tämä tekee liikesalaisuuksina suojattavien tietojen salassapidon hallinnasta lähinnä illuusion.

Oikeuskirjallisuudessa on myös esitetty, että datasäädös luo uudenlaisen liikesalaisuuden alalajin, joita voidaan nimittää tietosalaisuuksiksi (eng. data secrets). Tietosalaisuuksia luonnehtii erityisesti toimivaltaisten viranomaisten ennakkoarviointi ja teknisten suojakeinojen korostaminen, mikä erottaa ne perinteisistä liikesalaisuuksista. Viranomaiset arvioivat etukäteen, mitkä tiedot voivat saada liikesalaisuussuojaa ja miten tietoja tulee suojata. Viranomaiset käsittelevät datan haltijoiden ilmoituksia tietojen jakamisen pidättäytymisestä sen keskeyttämisestä ja kieltäytymisestä sekä käyttäjien sekä kolmansien osapuolten valituksia. Viranomaisten päätökset vaikuttavat siihen, millaisia liikesalaisuuksien suojatoimenpiteitä sovelletaan ja kuinka datanjakamisen ehdot määritellään.⁴²⁹ Toiseksi datasäädös korostaa teknisten suojatoimenpiteiden merkitystä. Nämä keinot menevät perinteistä liikesalaisuussuojaa pidemmälle ja voivat laajentaa liikesalaisuuden suojan vaikutuksia suhteessa kolmansiin osapuoliin.⁴³⁰ Viranomaisten käytäntöjen yhtenäisyys ja teknisten toimenpiteiden käytön laajuus ovat avainasemassa siinä, millaiseksi uusi liikesalaisuuden alalaji muodostuu. Yhtenäinen käytäntö edistää oikeusvarmuutta ja ennakoitavuutta, mikä on olennaista, kun yritykset suojaavat liikesalaisuuksiaan.

Liikesalaisuusdirektiivin ja datasäädöksen tavoitteet eivät välttämättä ole täysin ristiriidassa, vaikka ne aluksi voivat vaikuttaa siltä. Tämä johtuu siitä, että direktiivi pyrkii myös edistämään tiedon kiertoa suojaamalla liikesalaisuuksia. Liikesalaisuussuojan tavoitteena on suojata tietoja

⁴²⁹ Wiedemann - Leicht 2024, s. 14–24 ja 24–26.

⁴³⁰ Wiedemann - Leicht 2024, s 19–23.

ja varmistaa yrityksille kannustimet investointeihin ja innovaatioihin⁴³¹. Kuitenkin on ilmeistä, että liikesalaisuuksien suojaaminen ei aina edistä yritysten investointihalukkuutta, mikä on havaittu myös IoT-datan kohdalla⁴³². Siten tarvitaan lisää empiiristä tutkimusta siitä, milloin liikesalaisuuksien suojaaminen on taloudellisesti perusteltua.

Liikesalaisuuksien suoja on kritisoitu siitä, että se korostaa liikaa liikesalaisuuden haltijan yksityisiä etuja. Onkin esitetty, että suojaamisessa tulisi huomioida yhä enemmän yhteiskunnan etu, kuten ympäristön suojeleminen sekä kuluttajien ja muiden yritysten oikeudet. Viimeistään datastrategian myötä on selvää, mikä merkitys datan saatavuuden ja sen yhdisteltävyyden parantamisella on niin käyttäjien, yritysten ja julkisen sektorin kannalta. Datasäädös edistää datan saatavuutta ja sen käyttöä, esimerkiksi IoT-tuotteiden korjaus- ja huoltopalveluissa, tukien samalla kestävä kehityksen tavoitteiden toteutumista ilman, että liikesalaisuudet vaarantuvat. Siten datasäädös mahdollistaa dataan pääsyn ja liikesalaisuuksien suojan tasapainottamisen aiempaa oikeudenmukaisemmin.

Datasäädöksessä pyritään tasapainottamaan dataan pääsy ja liikesalaisuuksien suoja. Datasäädöksen mukaan liikesalaisuuksia sisältävää dataa voidaan luovuttaa vain, jos käyttäjä tai kolmas osapuoli toteuttaa toimenpiteet tiedon salassa pitämiseksi. Lisäksi datasäädöksessä annetaan datan haltijalle mahdollisuus pidättäytyä tai keskeyttää datan jakaminen liikesalaisuuksiin vetoamalla. Lisäksi datasäädöksen 4 artiklan 8 kohta ja 5 artiklan 11 kohta antaa datan haltijalle mahdollisuuden kieltäytyä datan jakamisesta kokonaan, jos liikesalaisuuden ilmaisemisesta aiheutuisi erittäin todennäköisesti vakaavaa taloudellista vahinkoa. Tämä asettaa liikesalaisuuksien suojan etusijalle datan jakamiseen nähden, mikä voi vaikeuttaa dataan pääsyn edistämistä. Liikesalaisuussuojan ensisijaisuus suhteessa datan jakamiseen korostaa datan haltijan etuja⁴³³.

Datasäädöksessä käytetyt liikesalaisuuksia suojaavat turvalausekkeet voivat johtaa väärinkäyttöihin, jos liikesalaisuussuojan avulla estetään datan jakaminen tai sen uudelleenkäyttö⁴³⁴. Lisäksi julkisten ja yksityisten intressien eli datan avoimuuden ja liikesalaisuussuojan välillä ei ole välttämättä mahdollista tehdä järkevää kompromissia.⁴³⁵ Se,

⁴³¹ Liikesalaisuusdirektiivin johdanto (2).

⁴³² Eckardt – Kerber 2023, s. 24.

⁴³³ Moscon 2023, s. 14–15.

⁴³⁴ Geiregat 2022, s. 27.

⁴³⁵ Noto La Diega 2022, s. 19–20. Datasäädöksessä olisi voitu mahdollistaa dataan pääsy kaikissa tilanteissa. Tällainen sääntelymalli on valittu esimerkiksi digimarkkinasäädöksessä (DMA), jossa datan avoimuus on priorisoitu ilman, että sitä rajoitetaan liiallisesti immateriaalioikeuksilla.

että datasäädöksessä datan jakaminen ei ole sallittua kaikissa tapauksissa, on omiaan lisäämään sääntelyn monimutkaisuutta, tehottomuutta ja epävarmuutta. Se, ettei ristiriitaa ole ratkaistu datan jakamisen eduksi, voi vaikeuttaa säädöksen tavoitteiden toteutumista ja hidastaa datatalouden kehitystä.⁴³⁶ Liikesalaisuuksien suojan korostaminen heikentää siten asetuksen tehokkuutta⁴³⁷.

Datasäädöksessä todetaan, että teollis- ja tekijänoikeuksia on kunnioitettava ja on tärkeää säilyttää kannustimet investoida dataa tuottaviin IoT -tuotteisiin⁴³⁸. Viimeksi mainittu viittaa liikesalaisuuksien suojaan. Kuitenkin datasäädöstä ei voida tulkita niin, että esimerkiksi liikesalaisuussuoja saisi etusijan IoT-tuotteiden datan pääsy- ja käyttöoikeuksiin nähden⁴³⁹. Kun viranomaiset käsittelevät datasäädöksen nojalla datan haltijan ilmoituksia sekä käyttäjien ja kolmansien osapuolten valituksia, päätöksissä on tärkeää varmistaa, että dataan pääsy ja liikesalaisuuksien suoja ovat oikeudenmukaisessa tasapainossa. Liikesalaisuussuojaa tulee tulkita datasäädöksessä tarkkarajaisesti ja rajoitetusti, jotta se ei muodosta perusteettomasti estettä datan jakamiselle. Liikesalaisuuden haltijan on riittävän tarkasti yksilöitävä, mikä osa datasta on liikesalaisuus, jotta liikesalaisuuksien suojaan voidaan ylipäättään vedota. Erityistä huomiota tulee kiinnittää datan jakamisesta pidättäytymistä tai sen keskeyttämistä koskevan päätöksen perusteluiden riittävyys ja hyväksyttävyyteen. Edelleen datan jakamisesta kieltäytyminen tulee olla viimesijainen keino. Datasäädöksessä annettu mahdollisuus kieltäytyä kokonaan datan jakamisesta on tarkoitettu suojaamaan erittäin arvokkaita liikesalaisuuksia, joiden paljastuminen uhkaisi datan haltijan liiketoiminnan edellytyksiä. Perusteltua olisi lähteä siitä, että liikesalaisuussuoja voi estää datan jakamisen vain, jos datan haltija menettäisi kokonaan kilpailukyvyn tai kannustimet investoida⁴⁴⁰. Liikesalaisuussuojan soveltamisessa painopisteen tulisi siirtyä yhä enemmän datan saatavuuden parantamiseen yhteiskunnan eduksi.

Liikesalaisuussuoja ei anna yksinoikeutta tietoon immateriaalioikeuksien tavoin. Liikesalaisuussuojan on tarkoitus olla vuotava eli siihen kuuluu, että suoja voidaan menettää, jos esimerkiksi kilpailija keksii saman tiedon itsenäisen kehitystyön tuloksena. Liikesalaisuuksia ei suojata EU:n perusoikeuskirjan mukaisena perusoikeutena, mikä antaa liikkumavaraa rajoittaa suojaa, kun se on tarpeen yhteiskunnan laajempien etujen

⁴³⁶Wiedemann - Leicht 2024, s. 29–30.

⁴³⁷Leistner - Antoine 2023, s. 6.

⁴³⁸Datasäädös johdanto (30). Kerber 2024, s. 2.

⁴³⁹Drexl – Banda – Gonzalez ym. 2022, s.7–8.

⁴⁴⁰Shakya 2014, s. 53.

saavuttamiseksi⁴⁴¹. Eri rajoitusperusteista johtuvat haitalliset vaikutukset voidaan hyväksyä, jolloin liikesalaisuussuojaa voidaan rajoittaa laajemmin.

Se, miten käytännössä asetuksen soveltamisessa tasapainotetaan dataan pääsy ja liikesalaisuuksien suojaaminen ratkeaa kansallisten toimivaltaisten viranomaisten, kansallisten tuomioistuinten ja viime kädessä EU-tuomioistuimen oikeuskäytännössä⁴⁴². Lisäksi Euroopan komissio tulee tarkastelemaan liikesalaisuuksien käsijarru -mekanismien toimivuutta ja sen vaikutusta liikesalaisuuksien suojaan⁴⁴³. Se, lisääkö asetus oikeudenkäyntien määrää jää nähtäväksi. Jos datan jakaminen aiheuttaa yritykselle korkeita kustannuksia esimerkiksi valvonnan ja täytäntöönpanon takia, se voi johtaa käytännössä tehottomuuteen. Tällöin se voi johtaa oikeudenkäynteihin tai jopa siihen, että yritykset päätyvät pitämään tietonsa salassa.⁴⁴⁴ Datasäädöksen vaikutuksia liikesalaisuussuojan kannalta heikentää kuitenkin se, että asetus ei koske johdettua tai pääteltyä dataa, joka esimerkiksi raakadataa todennäköisemmin täyttää liikesalaisuuden määritelmän. Siten asetuksessa sallitaan liikesalaisuuksien lisensointi vain hyvin rajalliseen määrään dataan.⁴⁴⁵ EU:ssa onkin valmisteilla verkkoon liitettyjä autoja koskevaa tiukempaa sääntelyä, koska ajoneuvojen osalta on tärkeää mahdollistaa myös muuhun kuin raakadataan pääsy⁴⁴⁶.

Se, miten datan saatavuus kehittyy kansainvälisesti, on myös olennaista. Käytännössä erilaisilla standardeilla, jotka koskevat datan avoimuutta ja immateriaalioikeuksien kunnioittamista voi olla suuri merkitys. Yhdistyneet kansakunnat (YK) solmi 22.9.2024 globaalin digitaalisen sopimuksen, jonka tavoitteena on kehittää avoin, vapaa ja turvallinen digitaalinen tulevaisuus. Sen tavoitteena on kehittää standardeja datan käyttöön, joilla varmistetaan datan turvallinen liikkuminen ja immateriaalioikeuksien suoja.⁴⁴⁷ Lisäksi YK on sitoutunut kehittämään vuoteen 2030 mennessä standardeja, jotka helpottavat datan käyttöä⁴⁴⁸. Nämä voivat vaikuttaa siihen, millaiseksi liikesalaisuuksien suojan ja datan jakamisen tasapaino muodostuu.

⁴⁴¹ Aracı 2019, s. 53. Liikesalaisuuksien suoja ei kuulu EU:n perusoikeuskirjan 17 artiklan 2 kohdan soveltamisalaan. Liikesalaisuusdirektiivin johdannon (21) mukaan liikesalaisuussuoja ”ei saisi vaarantaa tai heikentää perusoikeuksia ja -vapauksia tai yleistä etua, kuten yleistä turvallisuutta, kuluttajansuojaa, kansanterveyttä tai ympäristönsuojelua, eikä se saisi vaikuttaa työntekijöiden liikkuvuuteen”.

⁴⁴² Freshfields 2023. Hynönen - Leino -Bützow 2023, s. 487–488.

⁴⁴³ Datasäädös 49 artikla.

⁴⁴⁴ Risch 2010, s. 39–41.

⁴⁴⁵ Alpin 2024, s.91.

⁴⁴⁶ Komissio 2022c.

⁴⁴⁷ YK 2024a, s. 16.

⁴⁴⁸ YK 2024b s. 11.