

Datan käsite ja sen vaikutus datan jaettavuuteen EU:n datasäädöksen perusteella

Taloudellinen toiminta, sopimus ja vastuu
Tutkielma

Laatija:
Essi Laakkonen

12.6.2026

Tutkielma

Oppiaine: Oikeustiede

Tekijä: Essi Laakkonen

Otsikko: Datan käsite ja sen vaikutus datan jaettavuuteen EU:n datasäädöksen perusteella

Ohjaaja: Mika Viljanen

Sivumäärä: 65 sivua

Päivämäärä: 12.6.2026

Tutkielman kohteena on Euroopan unionin datasäädös, joka asettaa datan haltijoille velvoitteen jakaa verkkoon liitettyjen tuotteiden tai niihin liittyvien palveluiden käytöstä syntynyttä dataa käyttäjien ja kolmansien osapuolien kanssa. Säädöksen soveltamisalaan kuuluu verkkoon liitettyjen laitteiden sekä näihin liittyvien palveluiden tuottama, helposti saatavilla oleva data, sekä relevantti metadata. Jaettava data on laadultaan raakadataa tai esikäsiteltyä dataa, kun taas johdettu data ei kuulu säädöksen soveltamisalaan.

Tutkielman pääasiallisena tarkoituksena on ensinnäkin selvittää, minkälainen data kuuluu datasäädöksen soveltamisalaan ja erityisesti selvittää esikäsitellyn datan käsittelytoimenpiteiden määritelmää, ja kuinka ne eroavat johdetun datan käsittelytoimenpiteiden määritelmästä. Rajanvedolla on suuri merkitys, sillä se määrittää, minkälaista dataa datan haltijoiden tulee jakaa säädöksen nojalla. Tutkielman toinen päätutkimuskysymys kohdistuu siihen, millaisilla toimenpiteillä datan haltija voi minimoida datan, joka kuuluu datasäädöksen soveltamisalaan ja näin ollen minimoida laitteen käyttäjälle tai kolmannelle osapuolelle jaettavan datan määrän. Tutkielmassa selvitetään myös dataan kohdistuvaa sääntelyä ennen datasäädöstä, sekä niitä lähtökohtia ja tavoitteita, josta datasäädös on syntynyt.

Tutkielma on lainopillinen, ja tutkielman metodina on käytetty käytännöllistä lainoppia. Tutkielman tarkoituksena on selvittää voimassa olevan oikeuden sisältö ja tuottaa tulkintasuosituksia datasäädöksen oikeusnormeista sekä säädöksen sisältämistä oikeudellisista käsitteistä.

Tutkielman tuloksena selvisi, että datasäädöksen datan käsite on koko säädöksen soveltamisen perusta, ja sen vuoksi sen määrittely on erityisen tärkeää. Tutkielmassa selvitettiin, että datan käsite erityisesti esikäsitellyn datan käsitteen osalta sisältää tulkinnanvaraisuutta. Datan käsitteellä on suuri merkitys siihen, kuuluuko datan haltijoiden jakaa tuotteidensa dataa käyttäjille tai kolmansille osapuolille. Datan haltijat voivat hyödyntää kolmea eri strategiaa, joilla datan jakamista voisi minimoida: henkilötietostrategia, tekninen strategia sekä oikeudellinen strategia. Kaikissa strategioissa keskiössä on datan käsite, ja erityisesti kahdessa ensimmäisessä datan esikäsittelyn ja johdetun datan välinen rajanveto. Oikeudellisen strategian keskiössä on liikesalaisuuksien suoja, jonka hyödyntäminen vaatii liikesalaisuuden kriteeristön soveltamista datasäädöksen perusteella jaettava datan käsitteeseen.

Avainsanat: Datasäädös, data, datan jakaminen, reunalaskenta, liikesalaisuuksien suoja

Sisällys

Datan käsite ja sen vaikutus datan jaettavuuteen EU:n datasäädöksen perusteella	I
Lähteet.....	V
Lyhenteet.....	X
1 Johdanto.....	1
1.1 Tutkielman tausta.....	1
1.2 Teoreettinen viitekehys ja aineisto	3
1.3 Tutkimuskysymykset ja työn rakenne	4
1.3.1 Tutkimuskysymykset ja aiheen rajausta	4
1.3.2 Tutkielman rakenne	6
2 Miten dataa ja sen jakamista säänneltiin ennen datasäädöksen voimaantuloa?.....	7
2.1 Datan määritelmä	7
2.2 Millaista suojaa datan haltija on saanut datalle?	9
2.2.1 Immateriaalioikeudet.....	9
2.2.2 Sui generis -oikeus/ Tietokantadirektiivi	11
2.2.3 Liikesalaisuuden suoja	12
2.3 Millä perusteella dataa on täytynyt jakaa?	13
2.3.1 Kilpailuoikeudelliset säännökset.....	13
2.3.2 Yleinen tietosuojasäädös	14
2.4 Hajanainen sääntely vallitsevana oikeustilana	15
3 Datasäädöksen lähtöpiste: Lock-in tilanne	17
3.1 Tosiasiallisen hallinnan strategia	17
3.2 EU:n datastrategia	19
3.3 Ratkaisu lock in -tilanteen murtamiseen	21
4 Data datasäädöksessä.....	24
4.1 Datasäädöksen soveltamisala: verkkoon liitetty tuote sekä liitännäispalvelu.....	24
4.2 Helposti saatavilla oleva data sekä metadata	25
4.3 Raakadata	27

4.4	Esikäsitelty data	29
4.4.1	Esikäsitellyn datan käsite datasäädöksessä	30
4.4.2	Millaista on datan käsittely, joka ei edellytä merkittäviä investointeja?	32
5	Datan jakamisvelvoite.....	34
5.1	Datan haltijan velvollisuus jakaa dataa datasäädöksen nojalla.....	34
5.1.1	Datan jakamiseen liittyvät osapuolet	34
5.1.2	Datasäädöksen sisältämät velvoitteet datan jakamiselle	36
5.2	Millä perusteella kolmannella osapuolella on oikeus saada dataa?.....	37
5.2.1	Käyttäjän pyynnön perusteella tapahtuva datan jakaminen	37
5.2.2	Datan jakaminen datan haltijan ja kolmannen osapuolen välisen sopimuksen perusteella	39
5.3	Mihin IoT-laitteen tuottamaa dataa saa käyttää?	39
5.4	Poikkeukset datan jakamisvelvoitteeseen	41
5.4.1	Johdettu data	41
5.4.2	Muut mahdolliset poikkeustilanteet.....	42
6	Datan jakamisen minimoinnin strategiat	44
6.1	Tekninen strategia: johdetun datan tallentaminen	44
6.1.1	Reunalaskenta.....	45
6.1.2	Reunalaskentamenetelmän soveltaminen datasäädöksen soveltamisalaan kuuluvaan dataan	46
6.2	Privacy by design -järjestelmäsuunnittelu	48
6.3	Oikeudellinen strategia: liikesalaisuuksien suoja.....	50
6.3.1	Datan jakamisesta kieltäytyminen liikesalaisuusperusteella	51
6.3.2	Millainen data voidaan katsoa liikesalaisuudeksi?	52
6.3.3	Missä tilanteissa datan haltija voi rajoittaa datan jakamista liikesalaisuuksien suojaamisen perusteella?	55
7	Johtopäätökset	60
7.1	Mitä datasäädöksen soveltaminen tarkoittaa laitteen valmistajan tai datan haltijan näkökulmasta.....	60
7.2	Datan käsitteen määrittely suunnannäyttäjänä.....	61
7.3	Strategiat, joilla datan jakamista voidaan minimoida	63

Lähteet

Kirjallisuus

- Alastalo, Marja - Faisal, Kamrul - Salokannel, Marjut – Snell, Karoliina – Tupasela, Aaro – Ylikoski, Petri, Mitä data on? Teoksessa 50 Myyttiä tekoälystä ja datasta. Marianne Mäkelin, Elisa Silvennoinen, Kati Mäkitalo. Tampere: Vastapaino, 2025.
- Bützow, Alexander – Honkasalo, Pessi – Hynönen, Kalle – Leino, Saara – Rantanen Iiris, Datasäädös: käytännön käsikirja. Kauppakamari 2025.
- De Noyette, Ella – Stähler, Leander – Margoni, Thomas, Data Secrets: The Data Act's New Trade Secrets Framework.
- Drexl, Josef, Data Access and Control in the Era of Connected Devices. Study on Behalf of the European Consumer Organisation BEUC 2018.
- Drexl, Josef, The (Lack of) Coherence of Data Ownership with the Intellectual Property System. In Transition and Coherence in Intellectual Property Law: Essays in Honour of Annette Kur, Cambridge Intellectual Property and Information Law 2020 s. 213–223.
- Ducuing, Charlotte, An Analysis of IoT Data Regulation under the Data Act Proposal through Property Law Lenses. CiTiP Working Paper 2022.
- Eckardt, Martina – Kerber, Wolfgang, Designing the Bundle of Rights on IoT Data: The EU Data Act. Andrassy Working Paper Series in Economics and Business Administration No 54 2024.
- Farkas, Thomas J., Data Created by the Internet of Things: The New Gold without Ownership." Revista la Propiedad Inmaterial 23: 5-18. 2017. HeinOnline.
- Geiregat, Simon, The Data Act: Start of a New Era for Data Ownership? September 8, 2022. Saatavilla myös SSRN: <https://ssrn.com/abstract=4214704> or <http://dx.doi.org/10.2139/ssrn.4214704>
- Hynönen, Kalle – Leino, Saara - Bützow, Alexander, Euroopan datatalouden uudet säännöt: tarkastelussa datasäädös ja tekoälyasetus. Defensor Legis 3/2023 s. 466–488.
- Jain, Richa, Big Data and Competition Law: Navigating Trade Practices in the Digital Age. Journal of Law, Market & Innovation vol. 2025 no. 1 s. 63-88.

- Jane, V.A. – Arockiam, L, Survey on IoT Data Preprocessing. Turkish Journal of Computer and Mathematics Education Vol 12 No. 9 s. 238-244.
- Keller, Milla, Datajuridiikka: paremmat pelisäännöt datataloudelle. Helsinki: Alma Insights 2025.
- Kerber, Wolfgang, EU Data Act: Will new user access and sharing rights on IoT data help competition and innovation? Journal of Antitrust Enforcement, 12/2024, s.234-240.
- Kerber, Wolfgang, Governance of IoT Data: Why the EU data will not fullfill its objectives. GRUR International, Volume 72, Issue 2, February 2023, s. 120–135.
- Kim, Daria – Kwok, Man Wai, Data Usability as a Parameter of Rights and Obligations under the EU Data Act." Journal of Intellectual Property, Information Technology and Electronic Commerce Law 15, no. 2 2024, s. 139-155.
- Koolen, Christof, Understanding the Internet of Things, kirjassa "Protecting EU Consumers in Internet of Things Ecosystems", s.19-51. Oxford University Press, Oxford 2025.
- Krishnamurthi, Rajalakshmi – Kumar, Adarsh – Gopinathan, Dhanalekshmi – Nayyar, Anand - Qureshi, Basit, An Overview of IoT Sensor Data Processing, Fusion, and Analysis Techniques. Sensors 2020/20, s.1-23.
- Leistner, Matthias - Antoine, Lucie, Attention, Here Comes the EU Data Act! A Critical In-Depth Analysis of the Commission's 2022 Proposal. Journal of Intellectual Property, Information Technology and Electronic Commerce Law 13, no. 3 2022, s. 339-349. HeinOnline.
- Martens, Bertin, Data Access, Consumer Interests and Social Welfare: An Economic Perspective (2020). Available at SSRN: <https://ssrn.com/abstract=3605383> or <http://dx.doi.org/10.2139/ssrn.3605383>
- Martens, Bertin – De Streel, Alexandre – Graef, Inge – Tombal, Thomas – Duch-Brown, Nestor, Business-to-Business data sharing: An economic and legal analysis. JRC Digital Economy Working Paper 2020-05.
- Mylly, Ulla-Maija, Trade Secrets and the Data Act. IIIC (2024) 55, s.368-393.
- Raitio, Juha – Tuominen, Tomi, Euroopan unionin oikeus. 3. uudistettu painos, Alma Insights 2025.

Vapaavuori, Tom, Liikesalaisuudet ja salassapitosopimukset. 3. uudistettu painos, Alma Talent Oy 2020.

Villa, Seppo – Airaksinen, Manne – Alen-Savikko, Anette – Bärlund, Johan – Jauhiainen, Jyrki – Kaisanlahti, Timo – Kanervo, Joel – Knuts, Mårten – Kuoppamäki, Petri – Kymäläinen, Seppo – Mansnerus, Juli – Mähönen, Jukka – Pihlajarinne, Taina – Raitio, Juha – Viitanen, Klaus, Yritysoikeus. 5. uudistettu painos, Alma Insights 2024.

Wong-Toropainen, Sanna, Euroopan unionin datasääntely: käsikirja viiteen asetukseen. Edilex Lakitieto 2025.

Virallislähteet

Komission tiedonanto Euroopan parlamentille, Neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Euroopan datastrategia. (COM (2020) 66 Final) 19.2.2020.

HE 211/1992, Hallituksen esitys Eduskunnalle laiksi tekijänoikeuslain ja tekijänoikeuslain muuttamisesta annetun lain voimaantulosäännöksen 2 momentin muuttamisesta vp.

Euroopan komissio, Frequently asked Questions Data Act. version 1.4., 22.1.2026.

Oikeustapaukset

Case T-201/04 Microsoft Corp. v Commission of the European Communities

Muut lähteet

Datasäädös.

<https://digital-strategy.ec.europa.eu/fi/policies/data-act> luettu 29.4.2026.

Datasäädös selitettynä. Euroopan komissio. <https://digital-strategy.ec.europa.eu/fi/factpages/data-act-explained> luettu 7.4.2026

Datatalousosaamisen perusteita perusopetukseen ja toiselle asteelle <https://www.oph.fi/fi/digiosaaminen/datatalousosaamisen-perusteita-perusopetukseen-ja-toiselle-asteelle/mihin-0> luettu 29.4.2026

EU:n datasäädös - uudet säännöt datan jakamiselle. Insta.

<https://www.insta.fi/fi/kyberturvallisuus/ajankohtaista/nakemyksia/uudet-saannot-datan-jakamiselle/> luettu 18.4.2026

EU:n tekijänoikeuslainsäädäntö - tietokantojen suoja. Euroopan komissio.

<https://digital-strategy.ec.europa.eu/fi/policies/protection-databases> luettu 5.3.2026

Euroopan digitaalista tulevaisuutta rakentamassa – kysymyksiä ja vastauksia.

https://ec.europa.eu/commission/presscorner/detail/fi/qanda_20_264 luettu 29.5.2026

Eurooppalainen datastrategia.

<https://digital-strategy.ec.europa.eu/fi/policies/strategy-data> luettu 29.5.2026.

Mikä on henkilötieto? Tietosuojavaltuutetun toimisto. <https://tietosuoja.fi/mika-on-henkilotieto> luettu 28.4.2026.

Mitä on edge computing eli reunalaskenta? NordVPN

<https://nordvpn.com/fi/blog/reunalaskenta/?srsltid=AfmBOOp2dLkERHvRBldkjKzlljJFI Eef8fgY9BIHDO-hTteDnM-WV0x-> luettu 6.5.2026.

Questions and Answers – Data protection reform.

https://ec.europa.eu/commission/presscorner/detail/en/memo_15_6385 luettu 2.6.2026

Tepa-termipankki: reverse engineering

<https://termipankki.fi/tepa/fi/haku/reverse%20engineering> luettu 26.5.2026.

Tieteen termipankki: raakadata <https://tieteentermipankki.fi/wiki/Nimitys:raakadata> luettu 7.4.2026

Tietoa data-asetuksesta. Trafi.com <https://www.traficom.fi/fi/datatalous-ja-datan-valittaminen/tietoa-data-asetuksesta#accordion-62338> luettu 29.5.2026.

What Is Edge Computing? Hazelcast.com

<https://hazelcast.com/foundations/software-architecture/edge-computing/> luettu 30.4.2026.

What is Edge Computing? HPE.

<https://www.hpe.com/fi/en/what-is/edge-computing.html> luettu 6.5.2026.

Why and what do we need to know about data pre-processing? UK Data Service

<https://blog.ukdataservice.ac.uk/data-pre-processing/> luettu 7.5.2026.

Yleinen tietosuoja-asetus. Your Europe.

https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_fi.htm luettu 29.4.2026

Lyhenteet

Datasäädös	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
EU	Euroopan unioni
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
IoT	Internet of Things
Liikesalaisuusdirektiivi	Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943, julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta
SEUT	Sopimus Euroopan unionin toiminnasta
Tietokantadirektiivi	Euroopan parlamentin ja neuvoston direktiivi 96/9/EY tietokantojen oikeudellisesta suojasta

1 Johdanto

1.1 Tutkielman tausta

Data on kehittynyt nopeasti yhdeksi talouskehityksen keskeisimmistä tekijöistä, sillä se muun muassa tarjoaa mahdollisuuden kehittää uudenlaisia tuotteita ja palveluita, mahdollistaa tuotteiden ja palveluiden yksilöllistämisen sekä luo paremmat edellytykset päätöksenteolle.¹ Datan nousua talouskehityksen kärkeen havainnollistaa se, että tuotetun datan määrä on kasvanut moninkertaisesti vuodesta 2018 vuoteen 2025.² Aiemmin vallitseva tilanne on ollut se, että pieni joukko yksityisiä toimijoita hallitsi isoa osaa datasta, jonka EU katsoi heikentävän uusien tuotteiden kehitystä, yritysten kasvua ja innovointia.³ Euroopan unionin komissio onkin reagoinut datan kasvavaan määrään sekä huomionut datan arvon taloudellisena tekijänä. EU:n komissio julkaisi helmikuussa 2020 EU:n datastrategian 2020-luvulle, jonka tarkoituksena on muun muassa tarkentaa datan jakamiseen ja hallinnointiin sekä digitaalisten palveluiden toimintaan ja kilpailuun liittyviä vaatimuksia.⁴

Yksi EU:n datastrategian sisällöistä on datasäädös. Komission näkemys oli, että EU:ssa tarvittiin sääntelyä, jolla datan jakamiseen ja hallinnointiin voidaan vaikuttaa ja näin EU:n sisämarkkinoilla pystytään datan vapaa liikkuvuus sekä parempi pääsy dataan.⁵ 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 muuttamisesta⁶ (myöhemmin datasäädös) sääntelee verkkoon liitettyjen laitteiden ja niiden liitännäispalveluiden käytöstä syntyvän datan jakamista ja käyttöä.⁷ EU:n datasäädös tuli voimaan 11.1.2024, ja sen soveltaminen on alkanut 12.9.2025, muutamaa poikkeusta lukuun ottamatta.⁸

Datasäädöksessä säädetään datan jakamisesta yritysten (B2B), yritysten ja kuluttajien välillä (B2C) sekä yritysten ja julkisen sektorin toimijoiden välillä (B2G), ja sen tavoitteena on antaa

¹ COM (2020) 66 Final

² COM (2020) 66 Final

³ COM (2020) 66 Final

⁴ Keller 2025, s. 15.

⁵ Keller 2025, s. 19.

⁶ 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. Annettu 13.12.2023.

⁷ Butzow ym. 2025, s.13.

⁸ Butzow ym. 2025, s.16.

käyttäjille paremmat mahdollisuudet hallita verkkoon liitettyjen tuotteiden tuottamaa dataa.⁹ Datasäädös on muuttanut oikeustilaa, sillä se on tuonut mukanaan datan jakamiseen ja käyttöön pakottavaa sääntelyä.¹⁰ Datasäädös asettaa erilaisia velvoitteita yrityksille, jotka valmistavat verkkoon liitettyjä tuotteita. Datasäädöksessä säädetään siitä, miten yritysten tulee ottaa huomioon verkkoon liitettyjen tuotteiden tuottama data laitteiden suunnittelussa, valmistamisprosessissa sekä tuotteisiin liittyvissä palveluissa. Datasäädös velvoittaa yritykset suunnittelemaan ja valmistamaan verkkoon liitettyt tuotteet ja niihin liittyvät palvelut niin, että niiden data sekä metadata on oletusarvoisesti suoraan käyttäjän saatavilla helposti, turvallisesti ja maksutta.¹¹ Näin ollen datasäädöksen voimaantulo on tuonut muutoksia muun muassa yritysten sisäisiin prosesseihin, laitteiden ja tuotteiden suunnitteluun sekä siihen, miten yritykset toimivat tuotteiden tuottaman datan kanssa.

Verkkoon liitettyjen laitteiden tuottama data on yrityksille arvokasta, sillä sen avulla yritykset voivat muun muassa saada tietoa laitteiden toiminnasta sekä niiden käyttäjistä ja näin ollen yritykset voivat kehittää laitteita edelleen. Yritykset ovatkin kohdelleet dataa kuin omaisuuttaan, vaikka varsinkin ei-henkilötietoja sisältävään dataan liittyvä sääntely tai sen oikeudellinen suoja ylipäättään on ollut hajanaista.¹² Datan haltijat ovat nähneet datan taloudellisena hyödykkeenä, ja pitäneet tästä syystä datan hallinnan itsellään. Taloudellisesta näkökulmasta datan yksinoikeudella ja tiedon suojaamisella on ollut suuri merkitys: mikäli jokaisella taholla on vapaa pääsy kaikkeen dataan, se romahduttaa datan hinnan ja sen myötä vaikuttaa negatiivisesti markkinoihin ja talouteen.¹³ Näin ollen voidaan olettaa, että datan haltijoiden intressissä on edelleen pyrkiä minimoimaan jaettavan datan määrää.

Datasäädöstä ei kuitenkaan sovelleta täysin rajoituksetta kaikkeen olemassa olevaan dataan, vaan säädöksen soveltamisalan kuuluvat verkkoon liitettyjen (Internet of Things, myöhemmin IoT) laitteiden ja niihin liittyvien palveluiden tuottamaan dataan.¹⁴ IoT-laitteita ovat esimerkiksi älykellot, älyjääkaapit, glukosimonitorit, älyautot sekä jotkut teollisuuden laitteet.¹⁵ Sädös asettaa velvoitteen datan jakamiselle tuotetun datan, liitännäispalveludatan sekä välittömästi saatavilla olevan datan osalta, ja velvoitteet kohdistuvat nimenomaisesti dataan,

⁹ Tietoa data-asetuksesta.

¹⁰ Butzow ym. 2025, s.11.

¹¹ Butzow ym. 2025, s.75.

¹² Keller 2025, s.200.

¹³ Martens ym. 2020, s.4.

¹⁴ Hynönen – Leino – Butzow 2023, s. 471.

¹⁵ ks. kattavampi luettelo IoT-laitteista Koolen 2025, s.37.

jota ei ole merkittävästi muokattu, sillä jalostettu tai analysoitu data ei kuulu säädöksen soveltamisalaan.¹⁶

Edellä selostettu datasäännöksen aineellinen soveltamisala ei ole täysin ongelmaton. Ensinnäkin säädöstä ei sovelleta kaikkeen IoT-laitteiden tuottamaan dataan, vaan johdettu data sekä sellainen data, joka ei ole helposti saataville, jäävät asetuksen soveltamisalan ulkopuolelle. Toiseksi se, mitä säädöksessä mainituilla ”päättelyllä tai johdetulla tiedolla, jonka tuottamiseen on käytetty lisäinvestointeja” tarkoitetaan, on määritelmänä laaja. Ongelmana siis on, että säädöksessä ei ole selvästi määritelty datan käsitettä, jolloin soveltuvan datan ala jää epäselväksi, ja mahdollisesti myös kapeaksi.¹⁷

1.2 Teoreettinen viitekehys ja aineisto

Tämä tutkimus on oikeustieteellinen, ja tutkimuksen metodina on lainoppi. Lainopillisen tutkimuksen tiedonintressinä on voimassa oleva oikeus ja normit, ja tutkimuksella selvitetään voimassa olevan oikeuden sisältöä.¹⁸ Lainopillisella tutkimuksella on kaksi suuntausta, teoreettinen lainoppi sekä käytännöllinen lainoppi. Teoreettinen lainoppi systematisoi voimassa olevaa oikeutta muun muassa käsitteiden, oikeusperiaatteiden sekä teorioiden avulla.¹⁹ Käytännöllisen lainopin tarkoituksena on tuottaa tulkintasuosituksia voimassa olevan oikeuden sisällöstä.²⁰ Tässä tutkimuksessa tulen käyttämään tutkimusmetodina käytännöllistä lainoppia. Tutkielman tavoitteena on selvittää voimassa olevan oikeuden sisältö sekä tuottaa tulkintasuosituksia datasäädöksen datan käsitteestä sekä säädöksen soveltamisalasta.

Koska tutkimuksen tavoitteena on tuottaa tulkintasuosituksia, tutkimuksessa tullaan käyttämään erilaisia tulkintametoodeja tulosten saavuttamiseksi. Ensisijainen metodi tutkielmassa tulee olemaan sanamuodon mukainen tulkinta, eli säädöstekstille annetaan sen arkikielen mukainen merkitys. Tutkielmassa tullaan hyödyntämään myös historiallista tulkintaa selvittämällä datasäädöksen esitöitä sekä komission lausuntoja, sekä käyttämään analogista tulkintaa.²¹

¹⁶ Hynönen – Leino – Butzow 2023, s. 473.

¹⁷ Kerber 2023, s. 126.

¹⁸ Hirvonen 2011, s. 21–22.

¹⁹ Hirvonen 2011, s. 25.

²⁰ Hirvonen 2011, s. 25.

²¹ Tulkintametoodeista ks. Hirvonen 2011, s.38–40.

Tutkielma pohjautuu pääasiassa datasäädökseen sekä sen valmisteluaineistoon, oikeustieteelliseen kirjallisuuteen sekä julkaistuihin oikeustieteellisiin artikkeleihin. Pääasiallinen aineisto kooostuu EU-oikeudellisesta, dataoikeudellisesta sekä kilpailuoikeudellisesta kirjallisuudesta. Tutkielman keskiössä on EU:n datasäädös.

Tutkielmassa on käytetty tekoälyä tutkielman suunnitteluvaiheessa aiheen kartoittamiseen, sekä myöhemmässä vaiheessa tiedonhakuun. Tekoälyalustana on käytetty ChatGPT-työkalua. Tutkielmassa on myös käytetty DeepL-työkalua tekstin kääntämiseen.

1.3 Tutkimuskysymykset ja työn rakenne

Tutkielman keskeisenä ideana on selvittää, mitä datan käsitteellä tarkoitetaan EU:n datasäädöksessä ja millä edellytyksillä datan haltija voi minimoida datan jakamisen laitteen käyttäjän tai kolmannen osapuolen kanssa. Keskeisimpänä tiedonintressinä on datasäädöksen 2 artiklan määritelmät sekä relevantit resitaalikappaleet, jotka käsittelevät säädöksen soveltamisalaan kuuluvaa dataa, sekä säädöksen 4 ja 5 artiklan velvoitteet datan jakamiselle.

1.3.1 Tutkimuskysymykset ja aiheen raja

Tutkielmassa käsiteltävät tutkimuskysymykset on jaettu neljään eri tutkimuskysymykseen, joista kaksi ensimmäistä ovat tutkielman aihetta taustoittavia kysymyksiä, ja kaksi viimeistä ovat tutkielman päätutkimuskysymykset. Tutkimuskysymykset ovat seuraavat:

1. Mitkä olivat datan suojaamisen ja jakamisen sääntelyn lähtökohdat ennen datasäädöstä?
2. Mikä oli datan haltijoiden datastrategia ennen datasäädöstä, ja millä tavalla EU on pyrkinyt edistämään datan jakamista sisämarkkinoilla?
3. Miten datan käsite on määritelty säädöksessä, ja millaisia vaatimuksia jaettavalla datalla on?
4. Millä edellytyksillä datasäädös velvoittaa jakamaan dataa, ja millaisin menetelmin datan haltija voi minimoida säädöksen soveltamisalaan kuuluvan datan?

Ensimmäisen tutkimuskysymyksen tavoitteena on selvittää, miten dataa ja sen jakamista on säännelty ennen EU:n datasäädöstä. Tarkoituksena on selvittää, minkälainen lainsäädäntö on vaikuttanut dataan ja sen jakamiseen. Tarkoituksena on myös selvittää, millaista suojaa yritys

on datalleen saanut lainsäädännön valossa, ja millaisin ehdoin dataa on ollut pakko jakaa muille osapuolille, jos tällaista pakkoa siis ylipäättään on ollut olemassa.

Tutkimuskysymyksen tarkoituksena on taustoittaa sitä, miten data ja sen jakaminen sekä datan haltijan asema ymmärrettiin ennen datasäädöstä.

Toisen tutkimuskysymyksen tavoitteena on selvittää, millaisesta lähtökohdasta datasäädös on saanut alkunsa, ja minkälaiseen dataan ja ympäristöön sääntelyllä on pyritty vaikuttamaan.

Tutkielman toteuttamisen kannalta datasäädöksen taustan ja tavoitteiden tutkiminen on tärkeää, sillä teema tuottaa ymmärrystä aiemmin vallinneesta oikeustilasta sekä siitä, millaisia muutostarpeita datasääntelyssä on havaittu. Teeman tutkiminen muodostaa kuvan siitä, millainen osa datasäädöksellä on datasääntelyn kokonaiskuvassa.

Kolmantena päätutkimuskysymyksenä selvitetään EU:n datasäädöksen sisältöä erityisesti datan käsitteen ja säädöksen soveltamisalan osalta. Tämän tutkimuskysymyksen osalta syvennyttään erityisesti kartoittamaan sitä, mitä datalla tarkoitetaan säädöksen kontekstissa. Tutkimus kohdistuu kirjallisuudessa sekä säädöstekstissä esiintyvään raw data- käsitteeseen (suom. raakadata) sekä sen määritelmään. Samalla pyritään selvittämään, mikä on datasäädöksen aineellinen soveltamisala, eli millaisen datan jakamiseen säädöstä sovelletaan. Käsitteen määritelmän selvittäminen on tärkeää ensinnäkin siksi, että se vaikuttaa suoraan datasäädöksen soveltamisalan tulkintaan. Jos käsite on epäselvä, myös aineellinen soveltamisala jää epäselväksi. Soveltamisalan tarkkarajaisuus on tärkeää myös käytännön toiminnan näkökulmasta.

Viimeisen tutkimuskysymyksen tarkoituksena on selvittää, missä tilanteissa datan haltijan tulee jakaa dataa, ja mitkä tilanteet muodostavat poikkeuksen pääsääntöön. Tämän jälkeen tarkoituksena on selvittää, millaisilla menetelmillä datan haltija voisi minimoida tai kokonaan välttää datan jakamisen. Kyseessä on uusi säädös, joten siitä ei vielä ole saatavilla runsaasti käytännön soveltamiseen liittyvää tietoa. Säädöksessä on erikseen listattu poikkeustilanteet datan jakamisvelvoitteeseen, jolloin ainakin osaan tilanteista löytyy vastaus. Viimeisen tutkimuskysymyksen tietotarpeena on selvittää, onko säädöksen tulkinnassa mahdollista aukkoa, jonka perusteella yritys vapautuu datan jakamisvelvoitteesta muutoin kuin säädöksessä luetelluissa tilanteissa.

Datasäädöksen soveltamisala kattaa sekä henkilötietoja sisältävän datan että muun kuin henkilötietoja sisältävän datan artiklan 1 kohdassa 2 eritellyn mukaisesti. Tämän tutkielman

tiedonintressi on muu kuin henkilötietoja sisältävä data, ja näin ollen tutkielma keskittyy pääasiassa ei-henkilötietoja sisältävään dataan. Henkilötietoja sisältävään dataan liittyy paljon sääntelyä, ja sen huomioiminen laajasti tässä tutkielmassa ei ole rajallisen sivumäärän vuoksi mahdollista. Tästä syystä tutkielman päätiedonintressi kohdistuu ei-henkilötietoja sisältävään dataan.

Datasäädös sääntelee sekä yritysten välistä, että yritysten ja luonnollisten henkilöiden välistä datan jakamista. Tutkimuskysymykset sekä tutkimuksen kohde on rajattu niin, että tutkielmassa keskitytään yritysten väliseen datan jakamiseen, eikä yritysten ja luonnollisten henkilöiden välistä datan jakamista käsitellä enempää, kuin se on tarpeen esimerkiksi datan haltijan ja kolmannen osapuolen välisen suhteen selvittämiseksi.

1.3.2 Tutkielman rakenne

Tutkielman toisessa luvussa käsitellään datan määritelmää yleisesti, jonka jälkeen tarkastellaan sitä, millaista suojaa lainsäädäntö on tarjonnut datalle ja toisaalta millaisella sääntelyllä datan haltijaa on määrätty jakamaan dataa myös muille. Tutkielman kolmas luku käsittelee datasäädöksen lähtöpistettä: datan haltijoiden tosiasiallista hallintaa datasta sekä niitä lähtökohtia, joista datasäädös on syntynyt. Luvussa keskitytään myös siihen, millaisen datan sääntelyä EU tavoitteli datasäädöksellä, ja millä tavalla dataa haluttiin saada pois laitteiden valmistajien hallinnasta. Neljäs luku keskittyy datan käsitteeseen datasäädöksessä. Luvussa käsitellään datasäädöksen soveltamisalaa, sekä säädöksen kattamia eri datan käsitteitä: helposti saatavilla olevaa dataa, metadataa, raakadataa ja esikäsiteltyä dataa. Tutkielman viidennessä luvussa keskitytään siihen, millä tavalla datan haltijan tulee jakaa dataa käyttäjän ja kolmannen osapuolen kanssa, mihin dataa saa käyttää, ja mitä poikkeuksia datan jakamisvelvoitteeseen datasäädös sisältää. Kuudennessa luvussa käsitellään kolmea eri strategiaa, joilla datan haltija voi pyrkiä minimoimaan jaettavan datan. Nämä strategiat ovat henkilötietostrategia, tekninen strategia, sekä oikeudellinen strategia. Tutkielman viimeisessä, seitsemännessä luvussa käsitellään työn johtopäätökset.

2 Miten dataa ja sen jakamista säänneltiin ennen datasäädöksen voimaantuloa?

2.1 Datan määritelmä

Kun puhutaan datasta, on usein epäselvää, mitä datalla oikeasti tarkoitetaan. Datalla tarkoitetaan tieto-opissa yksittäisiä numeroita, merkkejä tai symboleita, ja silloin kun datalla on jokin merkitys, puhutaan informaatiosta.²² Samaa erottelua käytetään, kun puhutaan datasta syntaktisella sekä semanttisella tasolla: syntaktisella datalla tarkoitetaan esimerkiksi digitaalista tekstiä tai videota pelkästään bitteinä ja tavuina, ennen sitä on käsitelty tai analysoitu, kun taas semanttinen taso viittaa siihen, että datan sisältämällä informaatiolla on jo merkitys.²³ Informaatioteknologian näkökulmasta digitaalisessa muodossa olevalla datalla on kolme eri ulottuvuutta, ja samalla kolme eri määritelmää. Data voidaan ensinnäkin nähdä semanttisesti, eli data tarkoittaisi sananmukaisesti informaatiota. Toiseksi data voidaan nähdä informaation esitystapana, kuten numeroina ja kirjaimina, ja tällöin datan käsitteellä viitataan esimerkiksi erilaisiin sarjoihin tai kuvioihin, joita numeroista ja merkeistä muodostuu. Kolmantena datalla voidaan viitata tiettyyn sarjaan informaatiota, joka on olemassa tietyssä sijainnissa.²⁴ Usein datasta puhutaan tietona, mutta huomionarvoista on, että data on monimuotoista, ja sitä voidaan saada eri tavoin eri lähteistä ja erilaisin menetelmin, ja data voi olla kontekstista riippuen harhaanjohtavaa tai virheellistäkin.²⁵ Datasta voidaan saada tietoa, kun sitä käsitellään ja analysoidaan, ja datan prosessointi onkin kriittinen vaatimus sille, että raakadatasta, eli numeroista ja symboleista saadaan käyttökelpoista ja luotettavaa tietoa.²⁶

Data nähdään yleisesti ottaen hyödykkeenä, jonka määrä tai laatu ei vähene siitä, että monet eri käyttäjät hyödyntävät dataa omiin tarkoituksiinsa.²⁷ Tätä seikkaa on myös pidetty datan tärkeimpänä ominaisuutena.²⁸ Oikeuskirjallisuudessa vallitsee laaja yksimielisyys siitä, että datan käsitettä on varsin hankala määritellä tarkasti. Siitä, mitä datan käsite oikeudellisesta näkökulmasta tarkoittaa, ei ole kirjallisuudessa yksimielistä näkemystä.²⁹

²² Datatalousosaamisen perusteita perusopetukseen ja toiselle asteelle.

²³ Mylly 2024, s.371.

²⁴ Ks. datan määritelmistä Geiregat 2022 s.4.

²⁵ Alastalo ym 2025, s.17-19.

²⁶ Alastalo ym. 2025, s.18-19.

²⁷ Martens ym. 2020, s.4.

²⁸ Geiregat 2022, s.9.

²⁹ ks. Geiregat 2022, s.4; Drexler 2020, s.222; Farkas 2017, s.12.

Datan käsitteen määrittely on noussut ajankohtaiseksi, kun on pohdittu yhtäältä datan suojaamista sekä toisaalta kysymyksenasettelua datan omistusoikeudesta. Yleisesti on katsottu, että data on itsessään käsitteenä liian laaja suojan kohde, ja se tulisi määritellä tarkkarajaisemmin, jotta sen voitaisiin ajatella kuuluvan suojan piiriin.³⁰ Omistusoikeuden osalta on katsottu, että dataa semanttisessa merkityksessä ei voida asettaa omistusoikeuden piiriin.³¹ Tämä tarkoittaa käytännössä sitä, että kukaan ei voi saada yksinomaista omistusoikeutta informaatioon. Oikeuskirjallisuudessa on katsottu, että data käsitteenä on liian laaja, jotta se voisi saada sellaisenaan suojaa esimerkiksi immateriaalioikeuksista. Jotta data voisi saada suojaa, määritelmä tulisi olla vain semanttisella tasolla, taikka suojan tulisi kohdistua raakadataan, vaikkakin tämä ratkaisu rajaisi pääsyä dataan.³²

Ennen datasäädöksen voimaantuloa dataa on määritelty myös Yleisessä tietosuojasetuksessa³³ (GDPR), jossa asetetaan vaatimuksia yrityksille ja organisaatioille siitä, kuinka nämä tahot keräävät, säilyttävät ja hallinnoivat henkilötietoja.³⁴ Asetusta sovelletaan kaikkiin sellaisiin tietoihin, jotka koskevat tunnistettua tai tunnistettavissa oleva luonnollista henkilöä, ja sen määrittämiseksi, onko luonnollinen henkilö tunnistettavissa, on huomioitava kaikki keinot, joita voidaan käyttää tunnistamiseen suoraan tai välillisesti, esimerkiksi kyseisen henkilön erottaminen muista.³⁵ GDPR 4 artiklan 1 kohdassa on määritelty, mitä henkilötiedoilla tarkoitetaan. Henkilötiedoilla tarkoitetaan asetuksessa kaikkia tunnistettuun taikka tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Samassa kohdassa täsmennetään sitä, millä tunnistetiedoilla luonnollinen henkilö voidaan tunnistaa. Näitä keinoja ovat esimerkiksi nimi, henkilötunnus, sijaintitieto, verkkotunnistetieto taikka henkilön tunnusomainen fyysinen, geneettinen, psyykkinen, taloudellinen tai sosiaalinen tekijä. Näin ollen voidaan todeta, että henkilötieto on sellaista tietoa, jonka perusteella jokin henkilö voidaan tunnistaa suoraan, taikka näitä tunnistetietoja voidaan yhdistää, jolloin henkilö on mahdollista tunnistaa.³⁶

³⁰ Farkas 2017, s.12.

³¹ Geiregat 2022, s.5.

³² Drexl 2020, s.222.

³³ Euroopan parlamentin ja neuvoston asetusta (EU) 2016/679, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta. Annettu 27.4.2016.

³⁴ Yleinen tietosuojasetus.

³⁵ Yleinen tietosuojasetus, resitaali 26.

³⁶ Mikä on henkilötieto.

Edellä esitetyn perusteella voidaan vetää johtopäätös, että tieto on jotain, millä jokin asia voidaan tunnistaa, taikka tietoja yhdistämällä jokin asia voidaan tunnistaa tai liittää kuuluvaksi toiseen asiaan. Koska henkilötietojen on katsottu olevan dataa, ainakin jossain merkityksessä, voidaan päätellä, että data on jotain, millä voidaan määrittää, millainen jokin asia on tai mihin kyseinen asia liittyy.

Tämän työn kontekstissa datalla tarkoitetaan digitaalisessa muodossa olevaa tietoa. Seuraavaksi keskitytään siihen, millaista dataa koskevaa sääntelyä on ollut olemassa ennen EU:n datastrategiaa ja datasäädöksen voimaantuloa. Tämän tarkastelun kohteena ei ole EU:n datastrategian myötä ennen datasäädöstä voimaan tulleet, muut dataa koskevat säädökset vaan tarkoituksena on tutkia, millainen sääntelykenttä on ollut voimassa ennen nimenomaista datasääntelyä. Voidaan jo alkuun todeta, että dataa koskevaa sääntelyä on ollut kahdenlaista: sääntelyllä on annettu suojaa datan haltijalle, ja toisaalta on ollut sääntelyä, jolla on pyritty vaikuttamaan siihen, millä edellytyksillä datan haltijoiden tulisi jakaa dataa tai myöntää pääsy hallitsemaansa dataan.

2.2 Millaista suojaa datan haltija on saanut datalle?

Tässä alaluvussa tullaan keskittymään siihen, millaista dataa koskevaa sääntelyä on ollut olemassa ennen datasäädöstä. Alaluvussa käydään läpi sitä, miten immateriaalioikeudellinen sääntely, sui generis -oikeus sekä liikesalaisuuksien suoja ovat vaikuttaneet dataan, ja kuinka laajaa suojaa ne ovat tarjonneet.

2.2.1 Immateriaalioikeudet

Immateriaalioikeudet ovat aineettomia oikeuksia, ja ne tuottavat haltijalleen yksinoikeuden hyödyntää suojan kohdetta.³⁷ Immateriaalioikeudet voivat suojata joko ilmaisun muotoa tai keksintöä.³⁸ Immateriaalioikeudet suojaavat tekijöiden taloudellisia investointeja, sillä luovan työn tulokset edellyttävät usein suuriakin investointeja.³⁹ Tämän tutkielman aiheen kannalta relevanteimmat immateriaalioikeudet ovat tekijänoikeussuoja sekä patentti.

Tekijänoikeus syntyy kohteeseen heti, kun teos on luotu, eikä se näin ollen vaadi rekisteröintiä.⁴⁰ Jotta teos voi saada suojaa, teoskynnyksen tulee ylittyä eli teoksen tulee olla

³⁷ Villa ym. s.950.

³⁸ Villa ym. s.949.

³⁹ Villa ym. s.952.

⁴⁰ Villa ym. s.975.

omaperäinen.⁴¹ Tekijänoikeus antaa tekijälle oikeuden teoksen valmistamiseen, oikeuden saattaa teos yleisön saataville sekä oikeuden jälleenmyyntikorvaukseen.⁴² Tekijänoikeus ei tarjoa suojaa pelkälle tiedolle vaan ilmaisun muodolle, ja näin ollen se pikemminkin kannustaa investoimaan liiketoimintamalleihin, jotka on suunniteltu tarjoamaan tietoa.⁴³ Toisaalta varsinkin Yhdysvalloissa sovellusrajapinnat voivat nauttia tekijänoikeussuojaa, joka mahdollistaa datan yhteentoimivuuden, ja samanaikaisesti se rajoittaa muiden tahojen pääsyä dataan.⁴⁴ Tästä huolimatta voidaan katsoa, että tekijänoikeus ei suojaa dataa sinänsä, sillä sitä ei ensinnäkään ole määritelty suojattavaksi kohteeksi tekijänoikeuslainsäädännössä, ja toisaalta mikäli data voidaan rinnastaa tietoon, tekijänoikeuslainsäädäntö ei anna sille suojaa. Lisäksi Farkas katsoo, että tekijänoikeusdirektiivi ei sovellu teknologisen laitteen tekemisiin teoksiin, koska laite ei voi olla säädöksen tarkoittama ”tekijä”.⁴⁵ Voidaankin pohtia, soveltuisiko tekijänoikeutta koskeva sääntely digitaaliseen dataan, sillä se on usein automaattisesti laitteessa syntynyttä materiaalia.

Patenttioikeus voidaan myöntää tuotteeseen tai menetelmään, ja se antaa keksinnöille määräämällisen suojan, jonka tavoitteena on edistää teknistä kehitystä.⁴⁶ Patenttilain 1.1 §:n mukaan patentti voidaan myöntää mihin tekniikan alaan tahansa liittyvään keksintöön, jota voidaan käyttää teollisesti. Patentti tuottaa siis yksinoikeuden siihen, että keksintöä voidaan hyödyntää ammattimaisesti.⁴⁷ Euroopan patenttioviraston ratkaisukäytännössä on muodostunut kanta, jonka mukaan tietokoneohjelmalle voidaan myöntää patentti mikäli se käsittää uuden ratkaisun luonteeltaan tekniseen ongelmaan ja keksinnöllä on ”tekninen vaikutus yli tietokoneohjelmalla toimimisen”.⁴⁸ Kun tietokoneohjelmalle myönnetään patentti, se voi samalla vaikuttaa rajoittavasti datan saatavuuteen esimerkiksi tilanteissa, joissa menetelmäpatentin soveltamisen tuloksena syntynyttä dataa pidetään tuotteena, joka nauttii johdannaistuotteen suojaa.⁴⁹ Toisaalta patenttilainsäädännön soveltumista tietokoneohjelmiin ja sitä myötä myös dataan on myös kritisoitu. Kriittisen näkökulman mukaan patentin tarvetta

⁴¹ Villa ym. s.976.

⁴² Villa ym. s.980.

⁴³ Drex1 2018, s.3.

⁴⁴ Drex1 2018, s.10.

⁴⁵ Farkas 2017, s.8.

⁴⁶ Villa ym. s.1015.

⁴⁷ Villa ym. s.1025.

⁴⁸ Villa ym. s.1023.

⁴⁹ Drex1 2018, s.10.

ei voida perustella sillä, että investointitoimenpiteet jäisivät ilman patentin antamaa suojaa vajaiksi, sillä datan tuottamiseen investoidaan nykytaloudessa muutenkin.⁵⁰

Tässä tapauksessa patentoitava kohde ei olisi data itsessään, vaan tietokoneohjelma, ja poikkeustilanteessa tämän patentoidun ohjelman tuloksena syntynyttä dataa voitaisiin pitää johdannaistuotteena, joka samalla nauttii patenttisuoja. Tällöin voidaan ajatella, että data voi johdannaistuotetilanteessa saada patenttisuoja. Avoimeksi kysymykseksi kuitenkin jää, mitkä ovat ne edellytykset, jolloin dataa voidaan pitää johdannaistuotteena

2.2.2 Sui generis -oikeus/ Tietokantadirektiivi

Oikeuskirjallisuuden perusteella ennen datasäädöksen julistamista oli olemassa yksi sääntelykokonaisuus, joka antoi tietyin edellytyksin datalle suojaa immateriaalioikeutena.⁵¹ Kyseinen sääntelykokonaisuus on Euroopan parlamentin ja neuvoston direktiivi 96/9/EY⁵² eli tietokantadirektiivi. Tietokantadirektiivi on säädetty tietokantojen väärinkäytön suojaamiseksi erityisesti niissä tilanteissa, joissa tietokannan valmistajat ovat tehneet taloudellisia investointeja tietokannan laatimiseksi.⁵³ Tätä tietokantojen suojaamista kutsutaan direktiivissä sui generis -oikeudeksi eli tietokantojen erityiseksi omistusoikeudeksi.⁵⁴ Tietokantadirektiivi on implementoitu suomalaisessa lainsäädännössä tekijänoikeuslakiin.

Sui generis -oikeus on määritelty tietokantadirektiivin 3 luvun 7 artiklassa. Sen mukaan *”jäsenvaltioiden on säädettävä tietokannan valmistajalle oikeus kieltää sellaisen tietokannan, jonka sisällön kerääminen, varmistaminen tai esittäminen merkitsee määrällisesti ja/tai laadullisesti huomattavaa investointia, koko sisällön tai laadullisesti ja/tai määrällisesti arvioituna olennaisen osan kopiointi ja/tai uudelleenkäyttö.”* Iot-laitteiden tuottaman datan osalta rajanveto datan luomisen, hankkimisen ja todentamisen välillä voi olla haastavaa, ja IoT-laitteiden tuottaman datan osalta erottelu tietojen luomisen ja hankkimisen välillä sulkee pois laitteiden kehittämiseen ja tekniseen suunnitteluun tehtyjen investointien arvioinnin.⁵⁵

Sekä oikeuskirjallisuudessa että oikeuskäytännössä on katsottu, että tietokantadirektiivi ei soveltuisi sensoreiden tai IoT-laitteiden tuottamiin tietokantoihin, ja näin ollen ne eivät nauti

⁵⁰ Drexl 2018, s.3.

⁵¹ Drexl 2018, s.9.

⁵² Euroopan parlamentin ja neuvoston direktiivi 96/9/EY tietokantojen oikeudellisesta suojasta. Annettu 11.3.1996.

⁵³ Tietokantadirektiivi, resitaali 39.

⁵⁴ EU:n tekijänoikeuslainsäädäntö – tietokantojen suoja.

⁵⁵ Drexl 2018, s.71.

sui generis -oikeuden antamaa suojaa.⁵⁶ Ensinnäkin on katsottu, että sui generis -oikeuden soveltaminen tosiasiallisesti lisääisi laitteen valmistajan ja muiden osapuolien välistä epätasapainoa. Mikäli sui generis -oikeus soveltuisi IoT-laitteiden tuottamaan dataan, sen tuottama suoja vahvistaisi laitteen valmistajan monopoliasemaa, ja näin ollen antaisi valmistajalle mahdollisuuden evätä data muilta osapuolilta.⁵⁷ Toinen huomio liittyy tietokantadirektiivin soveltamisalaan ja tietokannan määritelmään. Tietokantadirektiivin 1 artiklan mukaan tietokannalla tarkoitetaan ”teosten, tietojen tai muiden itsenäisten aineistojen kokoelmaa, jotka on järjestetty järjestelmällisellä tai menetelmällisellä tavalla ja johon elektronisesti tai muulla tavoin on mahdollistettu yksilöllinen pääsy.” Jotta data kuuluisi tietokantadirektiivin soveltamisalaan, sen tulisi siis täyttää edellä mainitut kriteerit, eli datan tulisi olla järjestelty menetelmällisesti taikka järjestelmällisesti kokoelmaksi, ja tähän kokoelmaan tulisi olla yksilöllinen pääsy. Peilataan tätä kriteeristöä edellä käytyyn pohdintaan datan määritelmästä: data on tietoa, numeroita tai merkkisarjoja, joista analysoimalla ja käsittelemällä saadaan informaatiota. Näin ollen voidaan todeta, kuten oikeuskirjallisuudessa on huomautettu, että raakadata itsessään ei täytä näitä kriteerejä, ja sen takia sui generis -oikeus ei soveltuisi IoT-laitteista saatavaan dataan.⁵⁸ Tätä näkemystä vahvistaa edelleen se, että kun tietokantadirektiiviä implementoitiin, tietokannan sisältämä yksittäinen data jätettiin sui generis -oikeuden tuottaman suojan ulkopuolelle.⁵⁹ Näin ollen voidaan vetää johtopäätös siitä, että sui generis -oikeus suojaa tietokantaa, joka sisältää dataa, mutta se ei suojaa yksittäistä datan tietuetta.

2.2.3 Liikesalaisuuden suoja

Liikesalaisuus ei tuota yksinoikeutta salaisuuden haltijalle, mutta se estää sen, että toinen taho voisi oikeudettomasti hankkia, siirtää, käyttää taikka ilmaista tällaista liikesalaisuudeksi luokiteltavaa tietoa.⁶⁰ Mikäli liikesalaisuutta loukataan, siitä voi vakavimmillaan seurata rikosoikeudellinen rangaistus.⁶¹ Liikesalaisuuden piiriin voi kuulua minkälainen tieto tahansa⁶². Liikesalaisuuden suoja ei kuitenkaan tuota sen haltijalle yksinoikeutta tietoon, vaan

⁵⁶ Drexl 2018, s.70.

⁵⁷ Drexl 2018, s.85.

⁵⁸ Farkas 2017, s.9.

⁵⁹ Farkas 2017, s.9.

⁶⁰ Vapaavuori 2020, s.37.

⁶¹ Vapaavuori 2020, s.153.

⁶² Vapaavuori 2020, s.38.

mikäli toinen taho saa laillisesti hankittua saman liikesalaisuudeksi katsotun tiedon itsellensä, sen hyödyntäminen ei ole kiellettyä.⁶³

Drexl on katsonut, että liikesalaisuuksien suojalla voidaan parantaa datatalouden toimintaa varsinkin IoT-laitteiden tuottaman datan osalta, sillä sen avulla voidaan ottaa markkinoiden osapuolten edut huomioon. Hän huomauttaa kuitenkin, että liikesalaisuuksien suojaaminen suojaa vain niiltä laittomilta menettelytavoilta, joilla liikesalaisuuksia voisi saada haltuun, mutta se ei suojaa dataa kokonaisuudessaan esimerkiksi luvattomalta käytöltä.⁶⁴ Näin ollen liikesalaisuuden suoja voi soveltua dataan, mutta se velvoittaisi ainoastaan tiedon salassapitoon. Liikesalaisuuksien suoja on käytännössä ikuinen, mutta se ei tarjoa riittävää suojaa rinnakkaisinnovaatioita vastaan.⁶⁵ Liikesalaisuuden määritelmä voi tuottaa hankaluuksia suojan soveltamiseen tietyn tyyppiseen dataan: esimerkiksi yksittäisestä lähteestä tulevaa dataa, johon usealla taholla voi olla pääsy saattaa olla hankala määritellä liikesalaisuudeksi, jolloin suoja ei välttämättä sovellu laitteiden tuottamaan dataan.⁶⁶

2.3 Millä perusteella dataa on täytynyt jakaa?

2.3.1 Kilpailuoikeudelliset säännökset

Kilpailuoikeudellisten säännösten tarkoituksena on puuttua markkinoilla syntyviin kilpailunrajoituksiin, eli säädellä sitä, kuinka laajasti yritykset voivat omilla toimillaan rajoittaa kilpailua.⁶⁷ Kilpailuoikeuden keskiössä on yrityksen markkinavoiman kontrollointi, sillä markkinavoiman avulla yritys voi muun muassa vaikuttaa tuotteen hintatasoon tai kilpailuolosuhteisiin esimerkiksi korottamalla hintoja tai sulkemalla kilpailijoita pois markkinoilta.⁶⁸

Euroopan unionissa yksi merkittävimmistä kilpailuoikeudellisista säännöksistä on määräävän markkina-aseman väärinkäytön kielto. Määräävä markkina-asema ei ole kiellettyä, mutta tällaisen aseman omaava yritys ei saa toimia niin, että kilpailu markkinoilla vääristyy.⁶⁹ Määräävän markkina-aseman väärinkäytön kiellosta säädetään Euroopan unionin toiminnasta

⁶³ Vapaavuori 2020, s.37.

⁶⁴ Drexl 2018, s.11.

⁶⁵ Drexl 2018, s.31.

⁶⁶ Farkas 2017, s.10.

⁶⁷ Raitio – Tuominen 2025, s.771.

⁶⁸ Raitio – Tuominen 2025, s.772.

⁶⁹ Raitio – Tuominen 2025, s.802.

tehdyn sopimuksen⁷⁰ (SEUT) 102 artiklassa. Kyseinen artikla kieltää ”*yhden tai useamman yrityksen määräävän aseman väärinkäyttö sisämarkkinoilla tai niiden merkittävällä osalla, jos se on omiaan vaikuttamaan jäsenvaltioiden väliseen kauppaan.*” Määräävän markkina-aseman väärinkäyttönä SEUT 102 artiklassa pidetään muun muassa kohtuuttomia osto- tai myyntihintoja, kohtuuttomia kauppaehtoja taikka tuotannon, markkinoiden tai teknisen kehityksen rajoittamista kuluttajien vahingoksi. Myös toimituksista tai liikesuhteista kieltäytyminen ilman perusteltua syytä voidaan katsoa määräävän markkina-aseman väärinkäytöksi, sillä se voi olla kilpailijoille tai kuluttajille vahingollista.⁷¹

Kun ajatellaan dataa hyödykkeenä ja datan haltijaa määräävässä markkina-asemassa toimivana yrityksenä, voidaan huomata, että kilpailuoikeudelliset säännökset eivät anna suojaa datalle tai datan haltijalle vaan niiden avulla pyritään puuttumaan datan haltijan tosiasialliseen hallintaan ja yksinoikeuteen datasta sekä varmistamaan dataan pääsy ja tietojen jakaminen. Kilpailuoikeudellisten säännösten nojalla kiellettyjä toimia voivat olla esimerkiksi datan hinnoittelu, datasopimusten ehdot, datan pitäminen käyttäjien tai kolmansien osapuolien ulottumattomissa taikka datanjakosopimuksen solmimisesta kieltäytyminen. Tämä kuitenkin edellyttää sitä, että datan haltija on määräävässä markkina-asemassa ja käyttää tätä asemaa väärin SEUT 102 artiklassa esitetyllä tavalla. Drexl näkee kilpailuoikeudellisten säännösten soveltumisessa dataan kaksi haastetta. Ensinnäkin määräävän markkina-aseman todentaminen on käytännössä haastavaa, varsinkin kun otetaan huomioon datan luonne. Toisena ongelmana Drexl näkee sen, että kilpailulainsäädäntö ei ole tarpeeksi tehokasta takaamaan kilpailullisia markkinoita taikka estämään tilanteita, joissa datan haltijat pitävät datan yksinoikeudellisesti itsellään.⁷²

2.3.2 Yleinen tietosuoja-asetus

Yleinen tietosuoja-asetus (GDPR) on Euroopan unionin asetus, joka sisältää yrityksiä velvoittavaa sääntelyä henkilötietojen keräämisestä, säilytyksestä ja hallinnoinnista, ja sitä on sovellettu toukokuusta 2018 lähtien.⁷³ Yleisen tietosuoja-asetuksen tavoitteena on asettaa velvoitteita ja datan hallinnalle ja käytölle, sekä taata datan turvallinen käyttö.⁷⁴ Tavoitteena

⁷⁰ Euroopan unionista tehdyn sopimuksen ja Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoidut toisinnot (2016/C 202/1). Annettu 7.6.2016.

⁷¹ Raitio – Tuominen 2025, s.822.

⁷² Drexl 2018, s.4.

⁷³ Yleinen tietosuoja-asetus.

⁷⁴ Butzow ym. 2025, s.25.

on myös varmistaa, että henkilöt saavat ymmärrettävässä muodossa olevaa tietoa siitä, mitä henkilötietoja heistä kerätään ja miten yritykset käsittelevät tätä tietoa.⁷⁵ GDPR luo henkilöille oikeuden päästä käsiksi omiin henkilötietoihinsa, jotka ovat yritysten hallinnassa, sekä se antaa henkilöille oikeuden siirtää henkilötietojaan järjestelmästä toiseen.⁷⁶ GDPR velvoittaa myös yrityksiä antamaan henkilöille kopion niistä henkilötiedoista, joita yritys käsittelee.⁷⁷

Tämän perusteella voidaan sanoa, että datan jakamista koskevaa sääntelyä on ollut olemassa. GDPR kohdistuu kuitenkin ainoastaan henkilötietoja sisältävään dataan, ja näin ollen sen soveltamisalan ulkopuolelle jää kaikki data, joka ei sisällä henkilötietoja. GDPR sisältää edellä mainitun oikeuden henkilöille saada heidän henkilötietojansa sisältävää dataa yrityksiltä. Näin ollen GDPR ei sovellu siihen tarkoitukseen, että sen perusteella toinen yritys voisi vaatia datan haltijayritystä jakamaan dataa.

2.4 Hajanainen sääntely vallitsevana oikeustilana

Kuten edellä olevasta analyysistä voidaan huomata, aiemman lainsäädännön tarjoama suoja datalle ei ole ollut yksiselitteinen tai ongelmaton. Immateriaalioikeuksien osalta suurin kompastuskivi on, että tietoa itsessään ei siis suojata tekijänoikeudellisilla säännöillä. Näin ollen data yksinkertaisimmassa muodossaan raakadatana ei saa suojaa tekijänoikeudellisista säännöksistä, mutta mikäli dataa käsitellään taikka analysoidaan ja sitä tuotetaan eri muotoon, jolloin se voitaisiin katsoa pelkän tiedon sijasta ilmaisumuodoksi, tilanne voi olla toinen. Patenttisuojan osalta ongelma on, että patenttioikeus voidaan myöntää lain sanamuodon mukaisesti vain tuotteeseen tai menetelmään. Tässä ongelmaksi tulee sama määrittelyongelma kuin tekijänoikeuden kanssa: puhdas data, eli tieto, ei ainakaan sanamuodon mukaisen tulkinnan perusteella ole tuote tai menetelmä. Dataa voidaan pitää joissain tapauksissa patentilla suojatun ohjelman johdannaistuotteena, mutta tämä soveltuisi vain rajatuissa tilanteissa.

Sui generis -oikeus ei myöskään sovellu täysin ongelmattomasti juuri IoT-laitteiden tuottamaan dataan. Laitteiden tuottama data ei täytä direktiivin vaatimuksia, koska sitä ei välttämättä voida katsoa tietokannaksi.⁷⁸ Tämä johtuu edellä mainitun mukaisesti siitä, että

⁷⁵ Questions and Answers – Data protection reform.

⁷⁶ Yleinen tietosuojasetus.

⁷⁷ Yleinen tietosuojasetus.

⁷⁸ Drexl 2018, s.73.

useimmin laitteista kerättyä raakadataa ei ole järjestetty systemaattisesti, mikä sisältyy tietokantadirektiivin vaatimuksiin.⁷⁹ Liikesalaisuuksien suoja ei ole tehokas rinnakkaisinnovaatioita vastaan, jolloin se antaa suojaa ainoastaan tiedon laitonta hyödyntämistä vastaan.

Datan jakamista on pyritty edistämään pääasiassa kahdella tavalla: kilpailuoikeudellisilla säännöillä sekä yleisellä tietosuojasetuksella. Kilpailuoikeudelliset säännöt soveltuvat dataan, mutta ongelmakohta löytyy määräävän markkina-aseman määrittelystä. Yleisen tietosuojasetuksen velvoitteet soveltuvat dataan, sen hallinnointiin ja jakamiseen, mutta niiden soveltamisala rajoittuu vain henkilötietoja sisältävään dataan.

Voidaan siis todeta, että henkilötietoja sisältävää dataa on säännelty kohtuullisen kattavasti yleisessä tietosuojasetuksessa. Ei-henkilötietoja sisältävälle datalle ei puolestaan löytynyt yksiselitteistä säädöstä, joka tarjoaisi datalle, sen haltijalle tai IoT-laitteen käyttäjälle laajaa suojaa taikka määrittelisi dataan pääsyä tai osapuolien oikeuksia ja velvollisuuksia kyseiseen dataan liittyen. Vaikka hajanaista sääntelyä oli olemassa, yhteenvetona voidaan todeta, että lainsäädäntö ennen datasäädöksen voimaantuloa ei tarjonnut kovinkaan laajaa tai yhteneväistä sääntelyä IoT-laitteiden tuottaman datan omistus- tai käyttöoikeudesta taikka näiden oikeuksien suojaamisesta.⁸⁰ Data on kuitenkin katsottu hyödykkeeksi taloudellisessa luokittelussa, ja sen sääntelystä, sääntelyn tarpeesta ja oikeudellisesta luokittelusta on käyty runsaasti keskustelua.⁸¹ Tämän takia IoT-laitteiden valmistajat ovat päätyneet suojaamaan dataa suunnittelemalla laitteet niin, että data jää laitteeseen eivätkä laitteiden käyttäjät tai muut tahot voi hyödyntää dataa omiin tarkoituksiinsa.⁸²

⁷⁹ Drexl 2018, s.74.

⁸⁰ Farkas 2017, s.11.

⁸¹ Ducuing 2022, s.4.

⁸² Eckardt – Kerber 2024, s.4.

3 Datasäädöksen lähtöpiste: Lock-in tilanne

3.1 Tosiasiallisen hallinnan strategia

Kuten edellä on todettu, EU:n lainsäädännössä ei ole ollut mitään yleistä säädöstä siitä, miten tai millaisilla ehdoilla dataa tai tietoja tulisi jakaa muille osapuolille.⁸³ Ennen datasäädöksen voimaantuloa yleisenä käytäntönä oli, että yritykset ovat pitäneet datan sekä sen tosiasiallisen hallinnan tiukasti itsellään, eikä muilla osapuolilla ole ollut mahdollisuutta hyötyä siitä.⁸⁴ Koska lainsäädännössä ei ole ollut sääntelyä datan omistusoikeudesta tai datan jakamisesta muiden osapuolien kanssa, laitteiden valmistajat ovat voineet suojata dataa teknisesti ja näin ollen varmistaa sen, että heillä on tosiasiallinen hallinta laitteiden tuottamasta datasta.⁸⁵ Tätä ilmiötä kutsutaan lukkiutumisvaikutukseksi (lock-in effect). Lukkiutumisvaikutus syntyy, kun sekä laitteen käyttäjällä että laitteen valmistajalla molemmilla on taloudellinen intressi laitteen tuottamaan dataan, ja laitteen valmistaja estää muiden tahojen pääsyn kyseiseen dataan esimerkiksi suunnittelemalla laitteen niin, että muut tahot eivät voi tarjota palveluita, jotka tarvitsevat laitteen dataa.⁸⁶

Käytännössä tämä on tarkoittanut sitä, että laitteiden valmistajat ovat saaneet tosiasiallisen hallinnan dataan suunnittelemalla tekniset laitteet niin, että laitteiden tuottama data on jäänyt valmistajan servereille taikka muutoin paikallisesti laitteeseen, johon vain laitteen valmistajalla on pääsy.⁸⁷ Näin ollen valmistajalla on ollut kontrolli myös käyttäjän toiminnan tuloksena syntyneeseen dataan, ja tästä on seurannut muun muassa se, että laitteiden käyttäjät eivät ole saaneet pääsyä dataansa, ja toisaalta kolmannet osapuolet, kuten huoltopalveluiden tarjoajat eivät ole voineet tarjota palveluitaan, sillä niillä ei ole ollut pääsyä tarpeelliseen dataan.⁸⁸ Kun laitteet on suunniteltu niin, että niiden tuottama data jää vain valmistajan haltuun, laitteiden valmistajat ovat saaneet itselleen monopoliaseman, jossa he voivat estää laitteiden käyttäjiltä sekä muilta tahoilta pääsyn laitteiden tuottamaan dataan.⁸⁹ Tämä monopoliasema ja datan tosiasiallinen hallinta on oikeuskirjallisuudessa rinnastettu immateriaalioikeuksien kaltaiseen yksinoikeuteen laitteiden tuottamasta datasta, vaikka datan haltijalle ei ole ollut immateriaalioikeutta eikä omistusoikeutta dataan, vaan teknologisilla

⁸³ Geiregat 2022, s.12.

⁸⁴ Eckardt – Kerber 2024, s.4.

⁸⁵ Martens 2020, s.73.

⁸⁶ Drexl 2018, s.34.

⁸⁷ Eckardt – Kerber 2024, s.4.

⁸⁸ Kerber 2023, s.4.

⁸⁹ Eckardt – Kerber 2024, s.4.

suunnittelutoimilla on saatu näitä oikeuksia muistuttava, tosiasiallinen hallinta laitteen tuottamaan dataan.⁹⁰

Koska data on suurelta osin ollut vain laitteen valmistajan käytettävissä, datan jakamisesta yritysten välillä on käytännössä sovittu erilaisin datanjakosopimuksin. Laitteen valmistaja on voinut saada tuloja datasta, kun se on tehnyt kaupallisia datanjako- tai datankäyttösopimuksia käyttäjien tai kolmansien osapuolien kanssa.⁹¹ Tämä tarkoittaa käytännössä sitä, että datan haltija eli käytännössä laitteen valmistaja on sopimusperusteisesti myöntänyt muille osapuolille oikeuden datan käyttöön tai pääsyn dataan. Datanjakosopimukseen on usein liittynyt myös taloudellinen näkökulma, eli datan haltijalla on ollut mahdollisuus hinnoitella jakamansa data oman näkemyksensä mukaan.⁹²

Datan jakamisen sopimusperusteisuus yhdistettynä laitteen valmistajan monopoliasemaan on aiheuttanut markkinoilla muun muassa korkeita datan hintoja sekä tiukkoja ehtoja datan käytölle.⁹³ Ekonomisesta näkökulmasta katsottuna datamarkkinat eivät toimi ilman tietynlaista ”monopoliasemaa”, sillä mikäli kaikilla olisi yhtäläinen pääsy dataan, kilpailu madaltaisi datan hinnoittelua niin, että datan tuottaminen ja investointi datan keräämiseen ja sen käsittelyyn ei enää olisi liiketoiminnallisesti kannattavaa.⁹⁴ Yhden toimijan monopoliasema ei kuitenkaan ole yhteiskunnallisessa taloudessa hyvä asia, vaan se lisää datan haltijan varallisuutta laitteiden käyttäjien kustannuksella, ja tämän vuoksi datamarkkinoilla tulisi olla tasapaino monopoliaseman ja täysin avoimen datan saatavuuden välillä.⁹⁵

Ennen datasäädöksen voimaantuloa datan jakamiseen pyrittiin vaikuttamaan edellä todetusti kahdella eri sääntelykokonaisuudella: kilpailulainsäädännöllä, sekä yleisellä tietosuojasetuksella. Kilpailulainsäädännön näkökulmasta SEUT 102 artiklan määräävän markkina-aseman väärinkäyttämisen kielto on saattanut asettaa rajoitteita datan epäämiselle tietyissä tilanteissa. Pääsyn estämisen tai jakamisen epäämisen on voitu katsoa olevan määräävän markkina-aseman väärinkäyttöä kaupan estämisenä, mutta tämä on edellyttänyt sitä, että datan haltija olisi määräävässä markkina-asemassa toisiin toimijoihin nähden, sekä datan

⁹⁰ Kerber 2023, s.16 sekä Eckard – Kerber 2024, s.4.

⁹¹ Martens 2020, s.73.

⁹² Drexl 2018, s.29.

⁹³ Eckardt – Kerber 2024, s.4.

⁹⁴ Martens 2020, s.74.

⁹⁵ Martens 2020, s.74.

luovuttamisen tulisi olla kaupan epäämisen näkökulmasta määrävän markkina-aseman väärinkäyttöä.⁹⁶

Euroopan unionin yleinen tuomioistuin on käsitellyt datan jakamista SEUT 102 artiklan määrävän markkina-aseman väärinkäytön näkökulmasta ratkaisussa T-201/04 Microsoft Corp. v Euroopan yhteisöjen komissio. Ratkaisussa oli kyse siitä, että Microsoft oli kieltäytynyt toimittamasta kilpailijoille ”yhteentoimivuutta koskevia tietoja” ja Microsoft ei ollut antanut lupaa käyttää tietoja sen omien tuotteiden kanssa kilpailevien tuotteiden kehittämiseen ja jakeluun työryhmäpalvelimille tarkoitettujen käyttöjärjestelmien markkinoilla. Tuomioistuin totesi ratkaisussaan, että osapuolten tulee osoittaa, että määrävässä markkina-asemassa olevan datan haltijan data on sellaista, jota muilla osapuolilla ei ole mahdollisuutta saada millään muulla tavalla, datan jakamisesta kieltäytyminen vaarantaa toiminnan tai uusien tuotteiden kehityksen tai estää kilpailijan pääsyn markkinoille, taikka datan jakamisesta kieltäytymiselle ei ole objektiivisia syitä.⁹⁷

Yksi suurimmista datan jakamista koskevista sääntelykokonaisuuksista on yleinen tietosuoja-asetus (GDPR). Asetuksen 15 artiklan mukaan ”luonnollisella henkilöllä on oikeus saada pääsy kaikkiin tietoihin, joita rekisterinpitäjä käsittelee ja joiden avulla heidät voidaan tunnistaa”.⁹⁸ Huomionarvoista kuitenkin on, että GDPR soveltuu ainoastaan henkilötietoja sisältävään dataan. Vaikka säädöksellä on suuri käytännön merkitys siihen, miten yritykset käsittelevät ja jakavat dataa, asetus ei kata ollenkaan ei-henkilötietoja sisältävää dataa, eikä se tämän vuoksi sovellu kaikkeen käsiteltävään dataan, sillä suuri osa esimerkiksi teollisesta datasta jää tietosuoja-asetuksen soveltamisalan ulkopuolelle.

3.2 EU:n datastrategia

Ennen datasäädöstä IoT-laitteiden valmistajat ovat siis pitäneet laitteiden tuottaman datan tiukasti itsellään tosiasiallisen hallinnan avulla. Datasäädöksen syntymisen taustalla on vaikuttanut ilmiö, jossa IoT-laitteiden valmistajat ovat saavuttaneet eräänlaisen monopoliaseman laitteiden tuottamaan dataan, ja valmistajat ovat pystyneet estämään pääsyn dataan muilta toimijoilta ja palveluntuottajilta.⁹⁹ Tämän aiemmin käsitellyn lukkiutumisvaikutuksen sekä laitteiden valmistajien monopoliaseman dataan on katsottu EU:n

⁹⁶ Drexl 2018, s.36.

⁹⁷ Jain, 2025, s.71.

⁹⁸ Geiregat 2022, s.10–11.

⁹⁹ Kerber 2024, s.235.

tasolla vaikuttavan negatiivisesti muun muassa kilpailuun ja tuotekehitykseen.¹⁰⁰ Aiemmin dataa koskevaa sääntelyä ei juurikaan ollut, mutta EU:n datastrategian myötä EU on pyrkinyt luomaan dataa koskevaa sääntelyä, jolla suojataan kansalaisten oikeuksia ja etuja ja toisaalta edistetään teknologista kehitystä.¹⁰¹ Datasäädös on vain yksi asetus Euroopan isommassa datastrategiassa, jonka tavoitteena on parantaa Euroopan talousalueen dataomavaraisuutta ja kilpailukykyä datamarkkinoilla, ja tähän tavoitteeseen pyritään luomalla datan sisämarkkinat, joiden tavoitteena on yhtäältä varmistaa, että yhteiskunnan käytettävissä on enemmän dataa, ja toisaalta lisätä dataa koskevaa tehokasta sääntelyä.¹⁰²

Yksi Euroopan datastrategian tavoitteista on lainsäädännöllisin keinoin helpottaa datan saatavuutta sekä vapauttaa yksityisten toimijoiden hallinnoimaa dataa yhteiseen käyttöön.¹⁰³ Tätä datan vapauttamista on perusteltu sillä, että yksityisten toimijoiden datan laaja avoin saatavuus samoin kuin kyseisen datan uudelleenkäyttö olisi omiaan parantamaan julkisten palveluiden laatua, varmistamaan kilpailua sekä mahdollistaa uusien liiketoimintojen syntymistä EU:n alueella.¹⁰⁴ Datasäädöksen yksi sääntelyn päätavoitteista on pyrkiä hyödyntämään teollista dataa niin, että siitä olisi hyötyä Euroopan taloudelle ja yhteiskunnalle.¹⁰⁵ Erityisesti ei-henkilötietoja sisältävän datan osalta sääntelyllä pyritään siihen, että data olisi osapuolien saatavilla riippumatta sen alkuperästä, ja erityisesti sääntelyn tarkoituksena oli parantaa datan saatavuutta ja edesauttaa siihen perustuvaa päätöksentekoa.¹⁰⁶

Datasäädöksen taustalla vaikutti Euroopan datastrategian ajatus eurooppalaisesta data-avaruudesta. Data-avaruutta on kuvattu niin, että Euroopassa vallitsisi datan sisämarkkinat, joiden puitteissa yrityksillä olisi avoin pääsy suureen määrään teollista dataa, mutta sisämarkkinoilla arkaluontoiset ja muutoin suojattavat tiedot, kuten henkilötiedot tai liikesalaisuudet, olisivat turvattuja.¹⁰⁷ On arvioitu, että yksi suurimmista datan avoimen saatavuuden vaikutuksista voisi näkyä valmistusteollisuuden alalla, jossa datan tuottamisella ja hyödyntämisellä arvioidaan olevan suuri vaikutus kilpailukykyyn.¹⁰⁸ Laaja pääsyoikeus teolliseen dataan edesauttaisi talouden kasvua ja loisi mahdollisuuden eri toimijoille

¹⁰⁰ Kerber 2024, s.235.

¹⁰¹ Eurooppalainen datastrategia.

¹⁰² Eurooppalainen datastrategia.

¹⁰³ Euroopan digitaalista tulevaisuutta rakentamassa – kysymyksiä ja vastauksia.

¹⁰⁴ Euroopan digitaalista tulevaisuutta rakentamassa – kysymyksiä ja vastauksia.

¹⁰⁵ Eurooppalainen datastrategia.

¹⁰⁶ Euroopan digitaalista tulevaisuutta rakentamassa – kysymyksiä ja vastauksia.

¹⁰⁷ COM (2020) 66 final.

¹⁰⁸ COM (2020) 66 final.

suunnitella ja kehittää uusia tuotteita ja palveluita.¹⁰⁹ Samalla dataan pääsyn ja datan jakamisen tulisi olla helppoa ja toteutua ilman suuria taloudellisia investointeja tai muita haittavaikutuksia, jotta datan jakamisesta olisi hyötyä tuotteiden jälkimarkkinoille.¹¹⁰ Näin ollen voidaan todeta, että datasäädöksen kohteena on erityisesti yksityisten toimijoiden hallussa oleva teollinen data.

Kantavana ajatuksena datasäädöksen taustalla vaikuttaa käsitys datan luonteesta ja se, että se eroaa hyödykkeenä muista perinteisistä hyödykkeistä. Data ei vähene tai kärsi siitä, että useampi eri taho käyttää sitä, kun taas fyysiset resurssit, esimerkiksi öljy, eivät ole samalla tavalla useamman toimijan käytettävissä.¹¹¹ Näin ollen useampi eri taho voisi käyttää samaa dataa ilman, että sillä olisi vähentäviä tai negatiivisia vaikutuksia dataan hyödykkeenä. EU:n näkemyksen mukaan tätä datan ominaisuutta tulisi hyödyntää siten, että se loisi lisäarvoa taloudelle.¹¹²

3.3 Ratkaisu lock in -tilanteen murtamiseen

Euroopan komission tausta-ajatuksena oli puuttua IoT-laitteiden valmistajien monopolioikeuteen. Komissioin tarkoituksena oli varmistaa terveen kilpailun toteutuminen, kuluttajien ja asiakkaiden vapaan valinnan toteutuminen sekä tuotekehityksen ja innovaatioiden takaaminen EU:n sisämarkkinoilla.¹¹³ Tästä lähtökohdasta komissio katsoi, että Euroopan unionin alueella tulee määritellä, kenellä on oikeus käyttää tuotteen tai siihen liittyvän palvelun dataa, ja mitkä ovat tällaisen datan käytön edellytykset.¹¹⁴ Sääntelyn tavoitteena on antaa toimijoille avaimia parantaa tehokkuutta ja optimoida toimintaansa, kun niillä on pääsy esimerkiksi laitteiden suorituskykyä koskeviin tietoihin.¹¹⁵

Datasäädöksen tavoitteena onkin tarjota IoT-laitteiden käyttäjille ja mahdollisille kolmansille osapuolille oikeus saada laitteiden käytön tuottamaa dataa, sekä asettaa velvollisuus datan haltijoille asettaa tällainen data saataville.¹¹⁶ Sääntelyn lähtökohtana on, että mahdollisimman moni toimija, joilla on liittynyt IoT-laitteen tuottamaan dataan, voisivat saada pääsyn dataan ja näin ollen hyötyä datasta. Datasäädöksen tavoitteena on antaa IoT-laitteiden käyttäjille

¹⁰⁹ COM (2020) 66 final.

¹¹⁰ Wong-Toropainen 2025 s.46.

¹¹¹ Keller 2025, s.198.

¹¹² COM (2020) 66 final.

¹¹³ Drexl 2018, s.36.

¹¹⁴ Datasäädös, resitaalikappale 4.

¹¹⁵ Dataäädös.

¹¹⁶ Butzow ym. 2025, s.14.

mahdollisuus määrätä tuottamastaan datasta.¹¹⁷ Tämä tavoite ilmenee muun muassa sääntelynä, jolla pyritään määrittelemään reilut ja syrjimättömät sopimusehdot datan jakamiselle.¹¹⁸ Uudella sääntelyllä annetaan myös laitteiden käyttäjille oikeus tietysin edellytyksin saada pääsy laitteiden tuottamaan dataan.¹¹⁹ Pakottava sääntely datan jakamisesta sekä sopimusehdoista on eduksi varsinkin pienille ja keskisuurille yrityksille, joiden on voinut olla hankalaa saada pääsyä dataan.¹²⁰

Suurin datasäädöksen tuoma muutos liittyy ei-henkilötietoja sisältävän datan jakamiseen sekä datan jakamista koskeviin sopimuksiin. Kuten edellä on jo todettu, ennen datasäädöstä teollisen datan jakaminen perustui yritysten välisiin sopimuksiin, eikä sitä koskevaa pakottavaa lainsäädäntöä juurikaan ollut. Datasäädöksen myötä ei-henkilötietoja sisältävän datan hyödyntämistä, dataan pääsyä sekä tällaista dataa koskevia sopimuksia säännellään jatkossa pakottavilla säännöillä.¹²¹ Tämä on suuri periaatteellinen muutos, sillä aiemmin yritykset ovat voineet vapaasti sopia datan jakamisesta ilman suurempia rajoituksia, mutta jatkossa yritykset ovat pakottavan lainsäädännön velvoittamia datasäädöksen osalta.

Datasäädöksen voimaantulo ei syrjäytä tai rajoita aiempia dataa koskevia säädöksiä, kuten tietokantadirektiiviä tai immateriaalioikeuksien antamaa suojaa. Datan haltijoiden ja käyttäjien tulee toiminnassaan ottaa huomioon immateriaalioikeudet sekä liikesalaisuudet ja suojattava niitä samoin kuin ennen datasäädöstä.¹²² Esimerkiksi datan haltija voi olla velvoitettu hankkimaan erityisen lisenssin datan käyttöön taikka sopimaan siitä datan omistajan kanssa, sillä datasäädös ei anna oikeuksia käyttää immateriaalioikeuksilla suojattua dataa ilman oikeuden haltijan lupaa.¹²³ Tämä tarkoittaa myös sitä, että datan haltijat tai laitteiden käyttäjät eivät saa datasäädöksessä minkäänlaisia uusia oikeuksia käyttää IoT-laitteiden tuottamaa dataa, vaan säädöksen tavoitteena ja kohteena on ainoastaan edistää datan jakamista ja käyttöä.¹²⁴

Datan luonteen vuoksi datan käsitteen oikeudellisen määritelmän ja dataa koskevan sääntelyn tulisi kattaa laaja-alaisesti eri tilanteita, koska datan hallinnan ongelmat ovat usein

¹¹⁷ Datasäädös selitettynä.

¹¹⁸ Keller 2025, s.196.

¹¹⁹ Kerber 2023, s.2.

¹²⁰ Butzow ym. 2025, s. 11.

¹²¹ Hynönen – Leino – Butzow 2023, s. 468.

¹²² Butzow ym. 2025, s.41.

¹²³ Butzow ym. 2025, s.41.

¹²⁴ Butzow ym. 2025, s.41.

monimutkaisia.¹²⁵ Datasäädöksen soveltamisala onkin erittäin laaja, sillä se kattaa sekä teollisuuden laitteen että yksityisten käyttäjien laitteet ja säännöksiä sovelletaan yritysten ja kuluttajien sekä yritysten välisiin sopimuksiin ja datan jakamiseen.¹²⁶

¹²⁵ Eckardt – Kerber 2024, s.3.

¹²⁶ Leistner – Antoine 2022, s.344.

4 Data datasäädöksessä

4.1 Datasäädöksen soveltamisala: verkkoon liitetty tuote sekä liitännäispalvelu

Datasäädöksen keskiössä on säädöksen nimen mukaisesti data, ja näin ollen myös tämän tutkielman intressi kohdistuu säädöksen soveltamisalaan kuuluvaan dataan ja sen käsitteen määrittelyyn. Tässä pääluvussa käsitellään ensin datasäädöksen soveltamisalaa, toisena käsitellään helposti saatavilla olevan datan sekä siihen liittyvän metadatan käsitettä, kolmantena datan käsitettä ja raakadataa ja viimeisenä esikäsitellyn datan käsitettä.

Datasäädöksen 2 artiklan 5 kohdan mukaan verkkoon liitetyllä tuotteella tarkoitetaan ”esinettä, joka saa, tuottaa tai kerää käytöstään ja ympäristöstään dataa, joka pystyy välittämään tuotteen dataa sähköisen viestintäpalvelun, fyysisen yhteyden tai laiteyhteyden kautta ja jonka pääasiallinen toiminto ei ole datan tallennus, käsittely tai siirto muun osapuolen kuin käyttäjän puolesta”. Tällaisen tuotteen datalla taas tarkoitetaan datasäädöksen 2 artiklan 15 kohdan mukaan ”verkkoon liitetyn tuotteen käytön tuloksena tuotettua dataa, jonka valmistaja on suunnitellut olevan käyttäjän, datan haltijan tai kolmannen osapuolen, tarvittaessa myös valmistajan, haettavissa verkkoon liitetystä tuotteesta”.

Kun katsotaan tarkemmin verkkoon liitetyn tuotteen määritelmää, vaatimuksena on, että laite pystyy tuottamaan, keräämään tai vastaanottamaan dataa ja lisäksi laitteen tulee pystyä jakamaan kyseinen data ulos laitteesta.¹²⁷ Käytännössä tämä tarkoittaa sitä, että laitteessa tulee olla anturit, joilla laite kerää dataa, taikka laitteessa tulee olla sellainen ohjelmisto, mikä voi tuottaa dataa esimerkiksi seuraamalla käyttäjän toimintaa.¹²⁸ Mikäli laite ei pysty jakamaan tuottamaansa tai keräämäänsä dataa, vaan käyttää sitä ainoastaan omaan toimintaansa (esimerkiksi perinteinen digitaalinen kuumemittari tai vaaka), kyseessä ei ole säädöksen soveltamisalaan kuuluva verkkoon liitetty tuote.¹²⁹ Verkkoon liitettyjä tuotteita ovat esimerkiksi älypesukoneet, älysähköautot, sekä automatisoidut tuotantolinjat.¹³⁰ Määritelmän osalta olennaista on, että verkkoon liitetty tuote on nimenomaan fyysinen esine, ja tämän vuoksi esimerkiksi ohjelmistot eivät kuulu määritelmän piiriin.¹³¹

¹²⁷ Butzow ym. 2025, s.54.

¹²⁸ Koolen 2025, s.31.

¹²⁹ Butzow ym. 2025, s.54.

¹³⁰ Esimerkit ks. Butzow ym. 2025, s.55.

¹³¹ Butzow ym. 2025, s.52.

Tuotteeseen liittyvä palvelu on määritelty datasäädöksen 2 artiklan 6 kohdassa. Sillä tarkoitetaan ”muuta digitaalista palvelua kuin sähköistä viestintäpalvelua, mukaan lukien ohjelmistot, jotka ovat osto-, vuokraus- tai liisaushetkellä liitetty tuotteeseen siten, että verkkoon liitetty tuote ei pystyisi ilman sitä suorittamaan jotain sen toiminnoista, tai jotka valmistaja tai kolmas osapuoli myöhemmin liittää tuotteeseen lisätäkseen, päivittääkseen tai mukauttaakseen verkkoon liitetyn tuotteen toimintoja”. Tuotteeseen liittyvän palvelun datalla eli liitännäispalveludatalla tarkoitetaan datasäädöksen 2 artiklan 16 kohdan mukaan dataa, ”joka edustaa verkkoon liitettyyn tuotteeseen liittyvien käyttäjän toimien tai tapahtumien digitointia, jonka käyttäjä on tallentanut tarkoituksella tai joka on tallentunut käyttäjän toiminnan sivutuotteena ja joka tuotetaan palveluntarjoajan tarjotessa tuotteeseen liittyvää palvelua”. Toisin sanoen palvelun tulee vaikuttaa verkkoon liitetyn tuotteen toimintaan ja palveluun tulee liittyä palveluntarjoajan tekemää datansiirtoa verkkoon liitettyyn tuotteeseen.¹³² Tuotteeseen liittyviä palveluita ovat esimerkiksi erilaiset hallintaohjelmistot, joilla seurataan ja ohjataan tuotteen toimintaa, ja tuotteeseen liittymättömiä palveluita ovat esimerkiksi, konsultointi, analytiikka tai säännölliset korjaus- ja huoltopalvelut.¹³³

Datasäädös ei siis sovellu kaikkeen olemassa olevaan dataan, vaan sen soveltamisalaan kuuluvat ainoastaan IoT-laitteiden ja niiden liitännäispalveluiden käytöstä ja toiminnasta syntyvä data. IoT-laitteet ja liitännäispalvelut ovat siis säädöksen soveltamisalaan kuuluvan datan lähteitä. Seuraavaksi tarkastellaan, millaista dataa datan haltijoiden tulee säädöksen perusteella jakaa.

4.2 Helposti saatavilla oleva data sekä metadata

Datasäädöksen datanjakovelvoite kohdistuu verkkoon liitettyjen tuotteiden ja näihin tuotteisiin liittyvien palvelujen tuottamaan helposti saatavilla olevaan dataan.¹³⁴ Tämän helposti saatavilla olevan datan lisäksi datan haltijan tulee asettaa saataville metadata, joka on tarpeen helposti saatavilla olevan datan käyttämiseksi.¹³⁵

Datasäädöksen 2 artiklan 17 kohdan mukaan helposti saatavilla olevalla datalla tarkoitetaan ”tuote- ja liitännäispalveludataa, jonka datan haltija laillisesti saa tai voi saada verkkoon liitetystä tuotteesta tai siihen liittyvästä palvelusta ilman kohtuutonta vaivaa ja jota ei voida

¹³² Butzow ym. 2025, s.56.

¹³³ Butzow ym. 2025, s.56.

¹³⁴ Butzow ym. 2025, s.65.

¹³⁵ Butzow ym. 2025, s. 94.

toteuttaa yksinkertaisin toimenpitein.” Datan haltija voi saada helposti saatavilla olevaa dataa IoT-laitteesta tai liitännäispalvelusta esimerkiksi tuotesuunnittelun, datan haltijan ja käyttäjän välisen sopimuksen taikka teknisten keinojen avulla, edellytyksenä tietysti, että datan saaminen tapahtuu laillisesti ja ilman kohtuutonta vaivaa.¹³⁶

Saataville asetettavaan dataan olisi sisällytettävä myös asiaankuuluva metadata.¹³⁷ Tämä on yksi keskeisimmistä datasäädöksen määritelmistä, sillä sen vuoksi datan haltijan tulee aina pystyä jakamaan vähintään IoT-laitteen tuottama helposti saatavilla oleva data sekä asiaankuuluva metadata.¹³⁸ Datasäädöksen 2 artiklan 2 kohdan mukaan metadatatalla tarkoitetaan ”muun datan jäsenneiltyä sisällön tai käytön kuvausta, joka helpottaa kyseisen muun datan hakemista tai käyttämistä”. Metadataa ovat muun muassa datan peruskonteksti ja aikaleima, ja näiden avulla laitteen dataa voidaan käyttää yhdistettynä muuhun lajiteltuun ja luokiteltuun tai uudelleenmuotoiltuun dataan.¹³⁹ Metadata tukee innovointia ja tuotteiden kehittämistä sekä helpottaa verkkoon liitettyjen tuotteiden huoltoa ja korjaamista, ja se on tämän vuoksi usein käyttäjälle arvokasta.¹⁴⁰ Jotta metadata voisi olla sisällytettynä IoT-laitteen tuottamaan dataan ja jotta ne olisivat IoT-laitteen käyttäjän saatavilla, metadata tulee sijoittaa esimerkiksi samaan kansioon tuotetiedon kanssa joko itse tuotteessa, taikka laitteen ulkopuolella, esimerkiksi serverillä.¹⁴¹

Kim ja Kwok esittävät artikkelissaan ”*Data Usability as a Parameter of Rights and Obligations under the EU Data Act*”, että helposti saatavilla olevan datan tulisi täyttää seuraavat kriteerit: datan hankkimisen tulisi olla laillista ja datan hankkimiseen ei saisi liittyä liiallista vaivannäköä.¹⁴² Kirjoittajat huomauttavat, että näistä kriteereistä laillisuus on objektiivinen kriteeri, mutta liiallista vaivannäköä on hankalaa määritellä objektiivisesti. Sama pätee helposti saatavilla olevan datan määritelmässä mainittuun kohtuuttoman vaivan vaatimukseen. Mikäli tätä kriteeriä tulkitaan liian tapauskohtaisesti, se voi vaarantaa oikeusvarmuuden.¹⁴³

¹³⁶ Datasäädös resitaali 20.

¹³⁷ Datasäädös, resitaali 15.

¹³⁸ Butzow ym. 2025, s. 67.

¹³⁹ Butzow ym. 2025, s.69.

¹⁴⁰ Datasäädös, resitaali 15.

¹⁴¹ Kim – Wai 2024, s.149.

¹⁴² Kim – Wai 2024, s.147.

¹⁴³ Kim – Wai 2024, s.147.

Verkkoon liitetystä tuotteesta helposti saatavilla oleva data sekä asiaankuuluva metadata ovat vasta yläkäsitteitä jaettavalle datalle. Helposti saatavilla olevan datan määritelmä kertoo, millä tavalla datan tulisi olla tallennettuna laitteelle, taikka kuinka vaativilla toimenpiteillä voidaan edellyttää, että dataa asetetaan käyttäjän tai kolmannen osapuolen haltuun. Metadata taas on datan käytön helpottamiseksi jaettavaa tietoa, eikä sekään kerro jaettavan datan laadusta juuri mitään. Seuraavaksi keskitytään siihen, millaista datasäädöksen perusteella jaettavan datan tulee laadultaan olla.

4.3 Raakadata

Datasäädös sisältää määritelmän siitä, mitä säädöksessä tarkoitetaan datan käsitteellä. Datasäädöksen 2 artiklan 1 kohdan mukaan datalla tarkoitetaan ”kaikkea toimenpiteiden, toiseikkojen tai tietojen digitaalista esittämistä sekä kaikkia tällaisten toimenpiteiden, toiseikkojen tai tietojen koosteita, myös ääni- tai kuvatallenteena tai audiovisuaalisena tallenteena”. Datasäädöksen 4 artiklassa määritelty datanjakovelvoite kohdistuu edellä todetusti ainoastaan verkkoon liitetystä tuotteesta tai liitännäispalvelusta helposti saatavilla olevaan dataan.¹⁴⁴ Tuotteista ja niiden liitännäispalveluista saadaan paljon erilaista dataa, ja datasäädöksen soveltamisalaan kuuluvat seuraavat tuotteista ja liitännäispalveluista saatavat datatyypit:

”verkkoon liitettyjen tuotteiden ja niihin liittyvien palvelujen suorituskykyä, käyttöä ja ympäristöä koskeva data, yksityisen sektorin data, jota koskevat lakisääteiset datan jakamista koskevat velvoitteet, yritysten välinen data, johon päästään ja jota käytetään yritysten välisten sopimusten perusteella, sekä yksityisen sektorin data, jossa painotetaan muita kuin henkilötietoja”.¹⁴⁵

Näiden lisäksi datasäädöksen soveltamisala kattaa datankäsittelypalvelujen tarjoajien käsittelemän datan ja palvelut sekä datankäsittelypalvelujen tarjoajien hallussa unionissa olevat muut kuin henkilötiedot.¹⁴⁶

Datasäädöksen velvoitteet kohdistuvat vain digitaalisessa muodossa olevaan dataan.¹⁴⁷

Datasäädöksen soveltamisalaan ei sisälly online-servereiden tai alustojen käytön tuottama data, sillä datasäädös soveltuu vain IoT-laitteiden tuottamaan dataan.¹⁴⁸ Datasäädöstä

¹⁴⁴ Butzow ym. 2025, s.93.

¹⁴⁵ Butzow ym. 2025, s.11.

¹⁴⁶ Butzow ym. 2025, s.11.

¹⁴⁷ Mylly 2024, s.372.

¹⁴⁸ Leistner – Antoine 2022, s.346.

sovelletaan sekä henkilötietoja sisältävään dataan että muuhun kuin henkilötietoja sisältävään dataan.¹⁴⁹

Kun ajatellaan datasäädöksen piiriin kuuluvaa, IoT-laitteiden sensoreiden tuottamaa dataa, datan on määritelty olevan raakadataa (*raw data*). Raakadata tarkoittaa käsittelemätöntä ja jalostamatonta materiaalia.¹⁵⁰ Tämä on looginen määritelmä, sillä näkökulma sensorien tuottamasta datasta raakadatana on ollut olemassa oikeuskirjallisuudessa jo ennen datasäädöstä.¹⁵¹ Pureudutaan seuraavaksi siihen, mitä raakadata oikeastaan on.

Datasäädöksen mukaan velvollisuus jakaa dataa koskee ensisijaisesti ”dataa, jota ei ole olennaisesti muutettu”. Tällä tarkoitetaan siis raaka- lähde- tai primaaridataa, jotka ovat IoT-laitteen tai liitännäispalvelun automaattisesti tuottamia tietopisteitä, joita ei ole lisäkäsitelty.¹⁵² Raakadatan lisäksi datanjakovelvollisuus kohdistuu ”dataan, joka on esikäsitelty sen ymmärrettävyyden ja käytön mahdollistamiseksi ennen jatkokäsittelyä ja analysointia”. Tällaisia, antureista kerättyjä tietoja voidaan käyttää määrittämään fyysinen määrä tai muutos muun muassa lämpötilassa, paineessa, äänessä tai nopeudessa, ja sitä kutsutaan esikäsitellyksi dataksi.¹⁵³ Anturin tuottama raakadata on dataa, joka syntyy, kun analoginen signaali muunnetaan digitaaliseen muotoon, eli dataksi. Se ei siis kerro fyysisiä arvoja tai suureita, vaan data tulee kalibroida, jotta se saadaan käyttökelpoiseen muotoon.¹⁵⁴ Kim ja Kwok ovat artikkelissaan katsoneet, että juuri tähän kalibrointitoimeen viitataan datasäädöksen resitaalikappaleessa 15.¹⁵⁵ Tiivistettynä voidaan sanoa, että säädös velvoittaa jakamaan sellaista raakadataa ja esikäsiteltyä dataa, joka on valmistajan teknisen suunnitteluratkaisun vuoksi helposti saatavilla.¹⁵⁶ Kirjallisuudessa on väitetty, että raakadataa ei koskaan voida täysin erottaa sen sisältämästä informaatiosta.¹⁵⁷ Tämä tarkoittaa sitä, että data sisältää aina sen kontekstiin liittyvää tietoa.

Data, jota on jalostettu taikka analysoitu tavalla, joka on edellyttänyt lisäinvestointeja, ei kuulu datasäädöksen soveltamisalaan, elleivät datan haltija ja käyttäjä ole sopineet asiasta.¹⁵⁸

¹⁴⁹ Butzow ym. 2025, s.11.

¹⁵⁰ Tieteen termipankki.

¹⁵¹ Farkas 2017, s.9.

¹⁵² Butzow ym. 2025, s.68.

¹⁵³ Datasäädös, resitaali 15.

¹⁵⁴ Kim – Wai 2024, s.144.

¹⁵⁵ Kim – Wai 2024, s.144.

¹⁵⁶ Euroopan komissio 2026, s.6.

¹⁵⁷ Drexl 2018, s.44.

¹⁵⁸ Hynönen – Leino – Butzow 2023, s.473.

Raakadatan ja jatkojalostetun datan erottelulla datasäädöksessä on pyritty suojaamaan datan haltijaa, sillä datan jatkojalostaminen voi vaatia taloudellisia lisäpanostuksia ja investointeja, ja se voi olla raakadataa huomattavasti arvokkaampaa.¹⁵⁹ Jalostetun datan käsitettä käsitellään myöhemmin luvussa 5.4.1.

Tästä voidaan päätellä, että datanjakovelvollisuus ei tarkoita sitä, että yritykset voisivat täyttää datanjakovelvoitteen jakamalla käyttäjille ja muille tahoille vain sensorien tietopisteitä, pelkkiä ykkösiä ja nollia. Tällainen täysi raakadata olisi käyttökeltvotonta. Datasäädöksen velvoitteilla asetetaan valmistajille velvollisuus tarjota raakadatan ohessa sellaista metadataa, joka on tarpeen raakadatan ymmärtämiseksi. Toisaalta asetuksella varjellaan sitä, ettei yritysten tarvitse tehdä lisäpanostuksia tai investointeja dataan vain sen jakamiseksi muille tahoille. Herää siis kysymys, milloin tämä datan laadun parantaminen kuuluu datasäädöksen soveltamisalaan ja milloin se on katsottava lisäinvestoinneiksi?

4.4 Esikäsitelty data

IoT-laitteiden antureiden tuottaman datan käyttökelpoisuus riippuu siitä, kuinka sopivaa se on kuhunkin käyttötarkoitukseensa, kuten datan jakamiseen, tallentamiseen taikka päätöksentekoon.¹⁶⁰ Anturit tuottavat suuria datamääriä, mutta nämä datajoukot eivät ole käyttökelpoisia, sillä ne sisältävät paljon harha-arvoja, poikkeamia, häiriöitä sekä kohinaa, ja tällaisen raakadatan analysointi johtaisi helposti vääristyneisiin tuloksiin.¹⁶¹ Tämän vuoksi laitteen antureiden tuottama raakadata esikäsitellään, jotta datan laatua saadaan parannettua ja siitä saadaan hyödyllistä informaatiota eri käyttötarkoituksiin.¹⁶² Tämän seurauksena datan käyttökelpoisuutta voidaan parantaa, kun raakadataa muutetaan käsittelytoimenpiteillä tavoiteltuun muotoon.¹⁶³

Rajalakshmi Krishnamurthi ym. ovat esittäneet tutkimuksessaan ”*An Overview of IoT Sensor Data Processing, Fusion, and Analysis Techniques*” mallin, jonka mukaan IoT-laitteen tuottaman datan käsittelyprosessi voidaan nähdä kerrosteisena. Alimmalla tasolla on IoT-laite, joka sisältää erilaisia antureita, jotka voivat mitata muun muassa lämpötilanvaihtelua, painetta, tai kosteutta.¹⁶⁴ Tämän jälkeinen kerros sisältää laitteen antureiden keräämää dataa,

¹⁵⁹ Butzow ym. 2025, s.94.

¹⁶⁰ Kim – Wai 2024, s.141-142.

¹⁶¹ Jane – Arockiam 2021, s.238.

¹⁶² Jane – Arockiam 2021, s.238.

¹⁶³ Kim – Wai 2024, s.141-142.

¹⁶⁴ Krishnamurthi ym. 2020, s.3.

jota voivat olla esimerkiksi arvot edellä mainituista lämpötilanvaihteluista, paineesta tai kosteudesta. Nämä arvot eivät vielä kerro suureita, kuten celsiusasteita tai kosteusprosentteja, vaan antureiden tuottamat arvot ovat edellä selostettua raakadataa. Tämän jälkeen raakadataa esikäsitellään, esimerkiksi poistamalla datasta kohinaa, tunnistamalla poikkeavia arvoja ja yhdistämällä dataa.¹⁶⁵ Tämän vaiheen jälkeen esikäsitelty data yhdistetään, ja tämän vaiheen tavoitteena on integroida Iot-laitteiden antureiden antamat tiedot toisiinsa, jonka jälkeen viimeisenä kerroksena on datan analysointi, jossa kerätyn, esikäsitellyn ja yhdistetyn datan perusteella saadaan tietoa ja muodostetaan erilaisia päätelmiä.¹⁶⁶

Tutkielman kannalta relevantein datan käsittelyn vaihe on datan esikäsitely, sillä esikäsitelty data kuuluu datasäädöksen jakovelvoitteiden soveltamisalaan, mutta pidemmälle käsitelty johdettu data ei. Datan esikäsitelyllä tarkoitetaan prosessia, jossa raakadatasta muodostetaan erilaisilla menetelmillä jäsennelty aineisto, jota voidaan sittemmin tarkastella erilaisin analysointimenetelmin.¹⁶⁷ Dataa voidaan esikäsitellä monilla erilaisilla menetelmillä, ja esikäsitelyssä voidaan käyttää useita eri esikäsitelymenetelmiä. Dataa voidaan integroida, eli eri lähteistä saatua dataa voidaan yhdistää, dataa voidaan puhdistaa, jolloin siitä poistetaan kohinaa ja virheellisiä tietoja. Datan formaattia eli muotoa voidaan myös muuttaa erilaisin tekniikoin.¹⁶⁸ Dataa voidaan myös tiivistää tai vähentää, jolloin datasta saadaan tilavuudeltaan pienempi, mutta samat tulokset sisältävä yksikkö.¹⁶⁹ Esimerkkinä esikäsitelystä datasta on kirjallisuudessa käytetty tilannetta, jossa data on automaattisesti kategorisoitu ennalta-annettujen parametrien mukaan, ja tämä voisi käytännön tasolla tarkoittaa esimerkiksi tietoa siitä, onko anturin mittausarvo normaaliarvojen piirissä.¹⁷⁰

4.4.1 Esikäsitellyn datan käsite datasäädöksessä

Yksi rajanvetokysymyksistä koskee esikäsitellyn datan käsitettä ja sen sisällön määrittelyä. Millaisia toimenpiteitä voidaan katsoa esikäsitelyksi, ja mitkä toimenpiteet taas ovat sellaisia, jotka ovat edellyttäneet niin suuria investointeja, että ne jäävät soveltamisalan ulkopuolelle? Tämän käsitteen määrittely on tärkeää, sillä datalle tehtävät toimenpiteet määrittävät toisaalta sen, millaisia oikeuksia ja velvollisuuksia datan haltijalle asetetaan datasäädöksessä, ja

¹⁶⁵ Krishnamurthi ym. 2020, s.2.

¹⁶⁶ Krishnamurthi ym. 2020, s.4.

¹⁶⁷ Why and what do we need to know about data preprocessing?

¹⁶⁸ Jane – Arockiam 2021, s.240.

¹⁶⁹ Why and what do we need to know about data preprocessing?

¹⁷⁰ Butzow ym. 2025, s.69.

toisaalta esikäsittelytoimenpiteet vaikuttavat siihen, kuinka ymmärrettävää ja käyttökelpoista datasta tulee.¹⁷¹

Datasäädöksessä viitataan esikäsittelyn datan jakamiseen resitaalikappaleessa 15, jonka mukaan

”data, joka on esikäsitelty sen ymmärrettävyyden ja käytön mahdollistamiseksi ennen jatkokäsittelyä ja analysointia, kuuluu tämän asetuksen soveltamisalaan. Tällaisiin tietoihin kuuluvat tiedot, jotka on kerätty yksittäisestä anturista tai yhteenliitetystä anturiryhmästä, jotta kerätyt tiedot olisivat ymmärrettäviä laajemmissa käyttötapauksissa, määrittämällä fyysinen määrä tai laatu tai muutos fyysisessä määrässä, kuten lämpötilassa, paineessa, virtausnopeudessa, äänessä, pH-arvossa, nestetasossa, asennossa, kiihtyvyydessä tai nopeudessa. Termiä ’esikäsitelty data’ ei pitäisi tulkita siten, että datan haltija velvoitetaan tekemään merkittäviä investointeja datan puhdistamiseen ja muuntamiseen.”¹⁷²

Kun mietitään esikäsittelyn datan määritelmää datasäädöksessä, se sisältää ensinnäkin oletuksen siitä, että datan käsittelyllä on parannettu datan ymmärrettävyyttä ja mahdollistettu käyttöä, mutta kyseistä dataa ei ole vielä jatkokäsitelty tai analysoitu. Esikäsiteltyyn dataan sisältyy antureiden tuottama data, joka on käsitelty esimerkiksi määrittämällä fyysinen määrä tai laatu taikka muutos fyysisessä määrässä. Resitaalikappaleessa annetaan esimerkkeinä muun muassa määrä, laatu tai muutos lämpötilassa taikka paineessa. Mikäli datan analysointi tai jalostus on edellyttänyt sellaisia toimenpiteitä, joista on aiheutunut merkittäviä lisäinvestointeja, data ei lähtökohtaisesti kuulu säädöksen soveltamisalaan, elleivät datanhaltija ja käyttäjä ole nimenomaisesti sopineet tällaisen datan jakamisesta.¹⁷³

Kim ja Kwok käyttävät artikkelissaan esimerkkinä lämpötila-anturia: anturi tuottaa signaaleja, jotka saadaan anturista raakadatana, ei lämpötilan arvoina. Raakadatan tulosta kuvataan kvantitatiivisella mitalla raakadatapisteen ja niiden todellisten arvojen välisestä erosta, jolloin datasta voidaan tuottaa datan ja celsiusasteiden välinen yhteys.¹⁷⁴ Raakadataa voidaan jalostaa eri tavoin, ja nämä toimenpiteet vaikuttavat datan käyttökelpoisuuteen. Kim ja Kwok tuovat ilmi, että erityisesti datan kalibrointi sekä kohinanpoisto (*de-noising*) ovat merkittäviä toimenpiteitä, joilla raakadatasta saadaan käyttökelpoista. Kalibrointi ja kohinanpoisto

¹⁷¹ Kim – Wai 2024, s.144.

¹⁷² Datasäädös, resitaali 15.

¹⁷³ Hynönen – Leino – Butzow 2023, s.473.

¹⁷⁴ Kim – Wai 2024, s.142.

suoritetaan usein datan käsittelyn alkuvaiheessa, ja näitä toimenpiteitä voidaan pitää datan esikäsittelynä.¹⁷⁵

4.4.2 Millaista on datan käsittely, joka ei edellytä merkittäviä investointeja?

Voidaan siis todeta, että laitteen antureiden tuottamaa dataa täytyy lähes aina käsitellä jotenkin, jotta siitä saadaan ymmärrettävää ja käyttökelpoista. Koska raakadatan muuttaminen ymmärrettävään muotoon edellyttää siis vähintään datan esikäsittelyä, tulee seuraavaksi pohtia, milloin nämä toimenpiteet muuttuvat lisäinvestointeja edellyttäviksi toimenpiteiksi. Datan ominaisuudet sekä datan haltijan tekemät investoinnit datan käsittelyyn ja analysointiin voivat vaihdella tapauskohtaisesti, eikä niille ole asetettu tiettyä standardia. Tämän lisäksi datan ymmärrettävyys tai käytettävyys on suhteellista, sillä se riippuu monesta eri tekijästä ja näkökulmasta.¹⁷⁶ Näin ollen sovellettava kynnyks esikäsittelyn ja johdetun datan välillä on epäselvä, ja sitä tulisi tarkentaa, jotta datan esikäsittelyn ja jalostetun datan välinen raja olisi selkeämpi ja vaatisi vähemmän tapauskohtaista harkintaa.

Mikäli edellä todetun mukaisesti datan saattaminen ymmärrettävään muotoon vaatii aina käsittelytoimenpiteitä ja näin ollen myös investointeja, Kim ja Kwok näkevät, että datan haltijoilla on mahdollisuus tuottaa esikäsiteltyä dataa ilman, että siitä aiheutuu merkittäviä lisäkustannuksia datan haltijalle.¹⁷⁷ Kirjoittajat kuitenkin huomauttavat, että datan esikäsittelyn laatu voi vaihdella suuresti, mikä vaikuttaa sekä datan käyttökelpoisuuteen että esikäsittelyn kustannuksiin.¹⁷⁸ Datasäädöksen mukaisesti datan haltijan tulee jakaa käyttäjälle helposti saatavilla olevan datan lisäksi asianmukainen metadata, joka siis sisältää datan analysointiin tarpeellisia tietoja. Tällä perusteella datan vastaanottaja voisi itse tehdä datalle käsittelytoimenpiteitä, kuten kalibroida dataa tai suorittaa datalle kohinanpoistotoimenpiteitä, mikäli datan haltija ei ole niitä riittävällä tai tarpeellisella tavalla tehnyt.¹⁷⁹ Näin ollen datan haltija voisi vähentää datan käsittelystä aiheutuvia kustannuksia.

Datasäädös ei erittele sitä, millaisia ominaisuuksia helposti saatavilla olevalla datalla on. Määritelmä ei tuo ilmi sitä, onko helposti saatavilla olevassa datassa kyse raakadatasta vai esikäsittelystä datasta, ja tämän seikan määrittely vaikuttaa siihen, kuinka laaja velvollisuus

¹⁷⁵ Kim – Wai 2024, s.142.

¹⁷⁶ Kim – Wai 2024, s.145.

¹⁷⁷ Kim – Wai 2024, s.145.

¹⁷⁸ Kim – Wai 2024, s.145.

¹⁷⁹ Kim – Wai 2024, s.146.

datan haltijalla on jakaa helposti saatavilla olevaa dataa.¹⁸⁰ Datasäädöksen resitaalikappaleen 47 sisällöstä Kim ja Kwok päättelivät artikkelissaan, että helposti saatavilla olevan datan jakovelvollisuus voisi sisältää myös velvollisuuden datan esikäsittelyyn.¹⁸¹ Resitaalikappale 47 käsittelee kohtuullista korvausta datan saataville asettamisesta, ja resitaalikappaleessa mainitaan, että kohtuullinen korvaus datan saataville asettamisesta voi sisältää teknisiä kustannuksia, joita ovat muun muassa ”*tietojen saataville asettamisen edellyttämät käsittelykustannukset, kuten tietojen formatointiin liittyvät kustannukset*”.¹⁸²

¹⁸⁰ Kim – Wai 2024, s.146.

¹⁸¹ Kim – Wai 2024, s.146.

¹⁸² Datasäädös resitaali 47.

5 Datan jakamisvelvoite

5.1 Datan haltijan velvollisuus jakaa dataa datasäädöksen nojalla

Ensinnäkin datasäädös antaa IoT-laitteiden käyttäjille pääsyn siihen dataan, jota syntyy, kun käyttäjä käyttää laitetta, sekä oikeuden jakaa tätä dataa kolmannelle osapuolelle joko suoraan, taikka pyytämällä datan haltijaa jakamaan dataa kolmannelle osapuolelle. Toiseksi datasäädös sääntelee sitä, millä edellytyksillä datan haltijayrityksillä on lakiin perustuva velvollisuus jakaa dataa toisen yrityksen kanssa. Kolmantena datasäädös sisältää sääntelyä datan haltijayritysten ja viranomaisten välisestä datan jakamisesta.¹⁸³ Datasäädöksen II luku sääntelee sekä yritysten välistä (B2B) että yritysten ja kuluttajien välistä (B2C) datan jakamista, ja sääntelyn keskeisin sisältö on siinä, kuinka IoT-laitteiden käyttäjät voivat saada, käyttää ja siirtää sellaista dataa, joka syntyy IoT-laitteen käyttämisestä, säädöksen III luku keskittyy yritysten väliseen datan yhteiskäyttöön ja erityisesti niihin ehtoihin, joita sovelletaan, kun datan haltijayritys on lain mukaan velvollinen jakamaan dataa kolmannen osapuolen, eli toisen yrityksen kanssa, ja säädöksen V luku koskee datan jakamista B2G osapuolten välillä.¹⁸⁴ Tässä tutkielmassa keskitytään ensimmäisenä mainittuun tilanteeseen ja datasäädöksen II luvun sääntelyyn.

5.1.1 Datan jakamiseen liittyvät osapuolet

Datasäädöksen II luvun säännökset lähtevät siitä, että laitteen käyttäjällä on oikeus saada pääsy IoT-laitteen tuottamaan dataan, joka on syntynyt siitä, kun käyttäjä on käyttänyt laitetta, ja käyttäjällä on myös oikeus halutessaan jakaa laitteen käyttämisestä syntyntä dataa kolmannen osapuolen kanssa esimerkiksi korjauspalveluiden toteuttamiseksi.¹⁸⁵

Datasäädöksessä on määritelty datan jakamisen eri osapuolet: datan haltija, käyttäjä sekä datan vastaanottaja. Tämän tutkielman kannalta relevantit osapuolet ovat datan haltija sekä datan vastaanottaja, josta käytetään myös nimitystä kolmas osapuoli.

Datan haltija on määritelty datasäädöksen 2 artiklan 13 kohdassa. Määritelmän mukaan datan haltija voi olla luonnollinen henkilö taikka oikeushenkilö, jolla on ”*tämän asetuksen, sovellettavan unionin oikeuden tai unionin oikeuden mukaisesti annetun kansallisen lainsäädännön mukaisesti oikeus tai velvollisuus käyttää ja asettaa saataville dataa, myös*

¹⁸³ Datasäädös selitettynä.

¹⁸⁴ Datasäädös selitettynä.

¹⁸⁵ Datasäädös.

tuotteen dataa tai siihen liittyvän palvelun dataa, jonka datan haltija on hankkinut tai tuottanut tuotteeseen liittyvän palvelun tarjoamisen aikana, kun tästä on sovittu sopimuksella”. Datan haltijalla tulee siis olla tosiasiallinen hallintavalta IoT-laitteen tuottamaan tuote- tai liitännäispalveludataan sekä kyky asettaa sitä saataville säädöksen velvoitteiden mukaisesti.¹⁸⁶ Tässä yhteydessä tulee huomata, että datan haltijalla ei välttämättä tarkoiteta laitteen valmistajaa. Valmistaja on voinut myydä tai vuokrata IoT-laitteen niin, ettei valmistajalla ole tosiasiallisesti pääsyä laitteen tuottamaan dataan, ja tällöin valmistaja ei enää ole säädöksessä tarkoitettu datan haltija, paitsi jos dataa jää osittainkin valmistajan haltuun, niin tällöin valmistaja katsotaan tältä osin datan haltijaksi.¹⁸⁷

Datasäädöksessä on määritelty myös IoT-laitteen käyttäjän käsite. Datasäädöksessä tarkoitettu käyttäjä voi olla luonnollinen henkilö tai oikeushenkilö, joka omistaa tai jolle on siirretty tilapäinen käyttöoikeus IoT-laitteeseen, taikka luonnollinen henkilö tai oikeushenkilö, joka vastaanottaa laitteeseen liittyviä palveluja. Datasäädöksen sisältämä käyttäjän oikeus dataan ja toisaalta datan jakovelvoite datan haltijalle on sama riippumatta siitä, onko laitteen käyttäjänä luonnollinen henkilö vai oikeushenkilö.¹⁸⁸ Tässä kohtaa on hyvä huomata, että myös toinen yritys voi olla datasäädöksen tarkoittama laitteen käyttäjä ja näin ollen oikeutettu saamaan dataa säädöksen velvoitteiden mukaisesti. Näin ollen datasäädöksen II luvun oikeudet ja velvoitteet soveltuvat sekä yritysten ja kuluttajien että yritysten välisiin suhteisiin.¹⁸⁹

Viimeisenä osapuolena datan jakamiseen liittyen datasäädöksessä määritellään datan vastaanottaja. Datasäädöksessä datan vastaanottajalla tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka ei ole IoT-laitteen käyttäjä, ja joka toimii omaan elinkeino-, liike- tai ammattitoimintaansa liittyvässä tarkoituksessa ja jolle käyttäjän pyynnöstä taikka unionin oikeuden tai unionin oikeuden mukaisesti annetun kansallisen lainsäädännön sisältämän velvoitteen perusteella datan haltijan on asetettava dataa saataville.¹⁹⁰ Datasäädöksessä datanjakovelvoitteiden yhteydessä datan vastaanottajasta käytetään termiä ”kolmas osapuoli”, joka muuttuu datan vastaanottajaksi kun datan haltijalle esitetään pyyntö jakaa dataa

¹⁸⁶ Butzow ym. 2025, s.58.

¹⁸⁷ Butzow ym. 2025, s.76.

¹⁸⁸ Kerber 2023, s.6.

¹⁸⁹ Butzow ym. 2025, s.60.

¹⁹⁰ Butzow ym. 2025, s.65.

kolmannelle osapuolelle.¹⁹¹ Tämän vuoksi myös tässä tutkielmassa datan vastaanottajaan viitataan kolmantena osapuolena.

Kolmannella osapuolella on oikeus saada pääsy dataan kahdella tavalla, ja näitä tapoja käsitellään seuraavassa alaluvussa 5.2. Datasäädöksen II luvun määräysten teknisestä luonteesta johtuen laitteen käyttäjän ja kolmannen osapuolen välisellä suhteella on vaikutus siihen, mitä oikeuksia ja velvollisuuksia datan vastaanottajalla on ja tämän vuoksi käsitellään ensin relevanteilta osin datan haltijan ja laitteen käyttäjän välistä datan jakamista.

5.1.2 Datasäädöksen sisältämät velvoitteet datan jakamiselle

Datasäädöksen 2 luvun 3 artikla asettaa datan haltijoille velvoitteen saattaa tuotteen data ja siihen liittyvän palvelun data käyttäjän saataville. 3 artiklan 1 kohdan mukaan ”Verkkoon liitetyt tuotteet on suunniteltava ja valmistettava ja niihin liittyvät palvelut on suunniteltava ja tarjottava siten, että tuotteen data ja siihen liittyvän palvelun data, myös asiaankuuluva metadata, joka on tarpeen kyseisen datan tulkitsemiseksi ja käyttämiseksi, on oletusarvoisesti ja – tapauksen mukaan ja silloin, kun se on teknisesti mahdollista suoraan käyttäjän saatavilla helposti, turvallisesti ja maksutta kattavassa, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa.”¹⁹² Kyseisellä artiklalla on käytännön merkitys uusien IoT-laitteiden suunnitteluun, sillä verkkoon liitettyjä tuotteita ei ole ennen datasäädöksen voimaantuloa suunniteltu niin, että niiden data olisi käyttäjän saatavilla.¹⁹³ Artiklan asettama velvoite ei kuitenkaan ole ehdoton, sillä, sanamuoto ”tarpeen mukaan ja silloin, kun se on teknisesti mahdollista” antaa liikkumavaraa tilanteissa, joissa vaatimus olisi hankala toteuttaa.¹⁹⁴ Mikäli laitteen tuottamaan dataan ei ole suoraa pääsyä, käyttäjä voi pyytää datasäädöksen 4 artiklassa määrätyllä tavalla pääsyä dataan.¹⁹⁵

Datasäädöksen 2 luvun 4 artiklassa säädetään käyttäjien ja datan haltijoiden oikeuksista ja velvollisuuksista tuotteen dataan pääsyn, käytön ja saataville asettamisen osalta.

Datasäädöksen 4 artiklan 1 kohdan mukaan ”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 ja asiaankuuluva metadata, joka on tarpeen

¹⁹¹ Butzow ym. 2025, s.65.

¹⁹² Datasäädös 3 artikla 1 kohta

¹⁹³ Butzow ym. 2025, s.78.

¹⁹⁴ Butzow ym. 2025, s.77.

¹⁹⁵ Butzow ym. 2025, s.77.

kyseisen datan tulkitsemiseksi ja käyttämiseksi, ilman aiheetonta viivytystä samanlaatuiseina kuin datan haltijan käytettävissä oleva data, helposti, turvallisesti ja käyttäjälle maksutta kattavassa, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa sekä tarvittaessa ja kun se on teknisesti mahdollista, jatkuvasti ja reaaliaikaisesti. Tämä on tehtävä pelkän pyynnön perusteella, joka esitetään sähköisesti, jos se on teknisesti mahdollista”.¹⁹⁶

Datan haltijalla ja laitteen käyttäjällä tulee olla sopimus, jonka perusteella määräytyvät muun muassa pääsy laitteen tuottamaan dataan, datan jakamisen ehdot sekä se, saako datan haltija käyttää ei-henkilötietoja sisältävää dataa omiin tarkoituksiinsa.¹⁹⁷ Voidaan huomata, että samalla kun datasäädös antaa laitteen käyttäjälle oikeuden hyödyntää dataa sekä pääsyn dataan, se asettaa myös rajoituksia sille, mitä osapuolet voivat tehdä välittömästi saatavilla olevalle ei-henkilötietoja sisältävälle datalle.¹⁹⁸ Näistä rajoituksista säädetään datasäädöksen 4 artiklassa ja niitä käsitellään tarkemmin myöhemmin tässä luvussa.

5.2 Millä perusteella kolmannella osapuolella on oikeus saada dataa?

Datasäädös sisältää kaksi eri tilannetta, joissa kolmannesta osapuolesta voi tulla datan vastaanottaja. Ensinnäkin kolmas osapuoli voi saada dataa datasäädöksen 5 artiklan perusteella, eli kun IoT-laitteen käyttäjä pyytää datan haltijaa jakamaan dataa kolmannen osapuolen kanssa. Toisaalta datasäädöksen 4 artikla sisältää säännöksen tilanteeseen, jossa kolmas osapuoli voi saada dataa myös suoraan datan haltijan ja kolmannen osapuolen välisen sopimuksen perusteella, mutta tämä jakotapa sisältää käyttäjään liittyviä lisäedellytyksiä, joiden tulee täyttyä.

5.2.1 Käyttäjän pyynnön perusteella tapahtuva datan jakaminen

Datasäädöksen 5 artikla sisältää velvoitteen, jonka perusteella datan haltija on käyttäjän pyynnöstä velvollinen jakamaan IoT-laitteen tai siihen liittyvän palvelun dataa käyttäjän nimeämille kolmansille osapuolille.¹⁹⁹ Jakovelvoitteen piirissä oleva data on määritelty samalla tavalla kuin haltijan ja käyttäjän välisessä suhteessa jaettava data,²⁰⁰ eli toisin sanoen

¹⁹⁶ Datasäädös 4 artikla 1 kohta.

¹⁹⁷ Datasäädös selitettynä.

¹⁹⁸ Hynönen – Leino – Butzow 2023, s.474.

¹⁹⁹ Butzow ym. 2025, s.102.

²⁰⁰ Butzow ym. 2025, s.104.

datan haltija on velvollinen jakamaan samanlaista dataa sekä käyttäjälle että käyttäjän pyynnöstä kolmannelle taholle.

Butzow ym. esittelevät teoksessaan seuraavanlaisen esimerkin: Käyttäjä on älyajoneuvon omistaja, ja hän haluaa viedä autonsa valmistajan (=datan haltija) tarjoaman huoltopalvelun sijaan kolmannelle osapuolelle huollettavaksi. Kolmas osapuoli tarvitsee auton dataa, jotta huoltotoimenpiteen voidaan tehdä.²⁰¹ Näin ollen käyttäjä voi pyytää datan haltijaa jakamaan tälle kolmannelle osapuolelle auton datan, ja haltija on velvollinen toimimaan käyttäjän pyytämällä tavalla. Yksi datasäädöksen päätavoitteista oli edistää uusien dataa hyödyntävien liiketoimintojen syntymistä, ja kirjallisuudessa on katsottu, että datanjakamisvelvoite edistää tätä tavoitetta.²⁰²

Jotta kolmas osapuoli voisi saada IoT-laitteen tuottamaa dataa, vaaditaan aina käyttäjän taikka käyttäjän puolesta toimivan tahon pyyntö, ja näin ollen kolmas osapuoli ei voi vaatia laitteen dataa datan haltijalta oma-aloitteisesti.²⁰³ Mikäli käyttäjä ei itse esitä pyyntöä datan jakamisesta kolmannelle, pyynnön esittäjän tulee olla käyttäjän valtuuttama kolmas osapuoli, esimerkiksi datan välityspalvelun tarjoaja.²⁰⁴ Siitä, kuinka kyseinen valtuutus tulee toteuttaa, ei ole säädetty datasäädöksessä.²⁰⁵

Jotta kolmas osapuoli voi saada dataa datan haltijalta käyttäjän pyynnön perusteella, datan haltijan ja kolmannen osapuolen välille tulee solmia datanjakosopimus, jossa sovitaan ehdoista, joilla dataa luovutetaan, sekä mahdollisten liikesalaisuuksien salassapidosta ja mahdollisesta datan jakamisesta perittävästä maksusta.²⁰⁶ Näin ollen kolmannella osapuolella on kaksi sopimussuhdetta, joita sen on noudatettava: käyttäjän kanssa tehty sopimus, sekä datan haltijan kanssa tehty sopimus esimerkiksi liikesalaisuuksia sisältävän datan suojaamisesta taikka kohtuullisen korvauksen maksamisesta.²⁰⁷ Datan haltijat eivät kuitenkaan voi asettaa datanjakosopimukselle minkälaisia ehtoja tahansa, vaan datasäädöksessä säädetään siitä, että sopimusehtojen on noudatettava FRAND-ehtoja, eli niiden tulee olla oikeudenmukaisia, kohtuullisia ja syrjimättömiä.²⁰⁸

²⁰¹ Butzow ym. 2025, s.102.

²⁰² Butzow ym. 2025, s.102.

²⁰³ Butzow ym. 2025, s.104.

²⁰⁴ Butzow ym. 2025, s.104.

²⁰⁵ Butzow ym. 2025, s.104.

²⁰⁶ Kerber 2023, s.6.

²⁰⁷ Noyette – Stähler – Margoni 2025, s.991.

²⁰⁸ Kerber 2023, s.7.

5.2.2 Datan jakaminen datan haltijan ja kolmannen osapuolen välisen sopimuksen perusteella

Kolmas osapuoli voi saada IoT-laitteen tuottamaa ei henkilötietoja sisältämää dataa myös suoraan datan haltijalta haltijan ja vastaanottajan välisen sopimuksen nojalla. Datan jakamista on kuitenkin rajoitettu, ja datasäädöksen 4 artiklan 14 kohdan mukaan datan haltija ei kuitenkaan saa jakaa dataa kolmannen osapuolen kanssa muutoin kuin täyttääkseen käyttäjän kanssa tehdyn sopimuksen. Tämä tarkoittaa siis sitä, että datan haltijan tulee olla sopinut käyttäjän kanssa siitä, että käyttäjän ei-henkilötietoja sisältävää dataa luovutetaan eteenpäin kolmannelle.²⁰⁹ Butzow ym. on kiinnittänyt huomiota säännöksen sanamuotoon, sillä säännöksen sanamuodon mukaisen tulkinnan perusteella dataa saa luovuttaa kolmannelle ainoastaan ”käyttäjän kanssa tehdyn sopimuksen täyttämiseksi”. Tämä tarkoittaa sitä, että luovutuksen peruste tulee löytyä datan haltijan ja käyttäjän välisestä sopimuksesta, esimerkiksi sillä tavoin, että käyttäjälle tarjotun palvelun toteuttaminen vaatii datan luovuttamista kolmannelle osapuolelle.²¹⁰ Tästä voidaan vetää johtopäätös, että pelkkä yleisluontoinen varaus luovuttaa dataa missä tahansa tarkoituksessa kolmannelle osapuolelle ei täytä säännöksen vaatimusta siitä, että dataa luovutettaisiin haltijan ja käyttäjän välisen sopimuksen täyttämiseksi.²¹¹

5.3 Mihin IoT-laitteen tuottamaa dataa saa käyttää?

Datasäädös ei anna IoT-laitteiden käyttäjille oikeutta päästä käsiksi kaikkeen laitteiden ja niihin liittyvien palveluiden tuottamaan dataan, vaan käyttäjien oikeus rajoittuu dataan, joka on syntynyt nimenomaisen käyttäjän käyttäessä tuotetta tai siihen liittyvää palvelua.²¹² Dataan pääsyä ja käyttöä rajaa myös se, ettei sitä saa käyttää dataa tuottaneen IoT-laitteen kanssa kilpaileviin käyttötarkoituksiin.²¹³ Näin ollen esimerkiksi toinen valmistaja ei saa käyttää dataa samankaltaisen IoT-laitteen valmistamiseen tai tuotekehitykseen.

Datasäädös rajoittaa datan haltijoiden oikeutta käyttää IoT-laitteiden ja niihin liittyvien palveluiden tuottamaa dataa. Datasäädöksen 4 artiklan 13 kohdan mukaan datan haltija saa käyttää helposti saatavilla olevaa muuta dataa kuin henkilötietoja vain käyttäjän kanssa

²⁰⁹ Butzow ym. 2025, s.90-91.

²¹⁰ Butzow ym. 2025, s.90-91.

²¹¹ Butzow ym. 2025, s.90-91.

²¹² Geiregat 2022, s.20.

²¹³ Leistner – Antoine 2022, s.344.

tehdyn sopimuksen perusteella. Tämä tarkoittaa sitä, että tuotteen valmistajan tulee sopia datan käyttötarkoituksesta nimenomaisesti laitteen käyttäjien kanssa, koska muutoin datan haltija ei lähtökohtaisesti voi käyttää muuta kuin henkilötietoluonteista helposti saatavilla olevaa dataa esimerkiksi tuotekehityksessä.²¹⁴

Myös kolmannelle osapuolelle, eli datan vastaanottajalle on asetettu rajoituksia sille, mihin se voi käyttää vastaanottamaansa dataa. Datasäädöksen 6 artiklan mukaan ”kolmas osapuoli saa käsitellä sen saataville 5 artiklan mukaisesti asetettua dataa vain käyttäjän kanssa sovittuihin tarkoituksiin ja käyttäjän kanssa sovituin ehdoin”. Datan vastaanottajan käyttöoikeudet dataan määräytyvät siis vastaanottajan ja laitteen käyttäjän välisen sopimuksen perusteella, eikä datan haltijalla ole vaikutusvaltaa kuin poikkeustilanteissa siihen, miten datan vastaanottaja käyttää dataa.²¹⁵ Käytännössä tämä tarkoittaa esimerkiksi huolto- tai korjauspalvelun toteuttamista.²¹⁶

Kolmas osapuoli ei kuitenkaan saa käyttää vastaanottamaansa dataa IoT-laitteen kanssa kilpaileviin käyttötarkoituksiin.²¹⁷ Näin ollen esimerkiksi toinen valmistaja ei saa käyttää dataa samankaltaisen IoT-laitteen valmistamiseen tai tuotekehitykseen. Huomionarvoista kiellon osalta on se, että se kohdistuu ainoastaan kilpailevan tuotteen kehittämiseen, mutta kilpailevan palvelun kehittäminen on sallittua.²¹⁸ Kilpailevan tuotteen kehittämisen kiellon lisäksi datasäädöksen 6 artikla sisältää kolmannelle osapuolelle muitakin rajoituksia. Sen mukaan kolmas osapuoli ei saa muun muassa ”käyttää saamaansa dataa tietosuoja-asetuksessa tarkoitettuun profilointiin, paitsi jos se on tarpeen käyttäjän pyytämän palvelun tarjoamiseksi, tai jakaa dataa muun kolmannen osapuolen kanssa kilpailevan tuotteen kehitystä varten, käyttää sen saataville asetettua tuotteen tai siihen liittyvän palvelun ei-henkilötietoluonteista dataa saadakseen tietoa datan haltijan taloudellisesta tilanteesta, varoista ja tuotantomenetelmistä tai siitä, miten datan haltija käyttää dataa, käyttää vastaanottamaansa dataa tavalla, joka vaikuttaa haitallisesti verkkoon liitetyn tuotteen tai siihen liittyvän palvelun suojaukseen taikka estää käyttäjää, joka on kuluttaja, asettamasta vastaanottamaansa dataa muiden osapuolten saataville, myöskään sopimuksen perusteella”.²¹⁹

²¹⁴ Butzow ym. 2025, s.88.

²¹⁵ Butzow ym. 2025, s.107.

²¹⁶ Butzow ym. 2025, s.107.

²¹⁷ Leistner – Antoine 2022, s.344.

²¹⁸ Butzow ym. 2025, s.108.

²¹⁹ Butzow ym. 2025, s.109.

Yhteenvedona voidaan todeta, että laitteen käyttäjällä on oikeus käyttää dataa laillisiin tarkoituksiin, kun taas kolmas osapuoli voi käyttää dataa ainoastaan käyttäjän kanssa tehdyn sopimuksen perusteella.²²⁰

5.4 Poikkeukset datan jakamisvelvoitteeseen

Datasäädöksessä on määritelty myös rajoitteita datan jakamiselle. Nämä rajoitteet voidaan jakaa kahteen kategoriaan: datatyypit, jotka eivät ole jakovelvoitteen piirissä sekä olosuhteet, joissa dataa ei tarvitse jakaa tai jakamiselle on asetettu lisäkrityerejä. Datan tyyppiä koskeva rajoitus on esimerkiksi datasäädöksen resitaalikappaleessa 16 luetellut immateriaalioikeuksien piiriin kuuluvat ohjelmistot ja sisällöt, jotka on tuotettu esimerkiksi jonkin verkkopalvelun suorittamaa käyttöä varten, taikka sellainen data, joka on siirretty verkkoon liitetyle tuotteelle tallentamista tai muuta käsittelyä varten muiden osapuolten kuin käyttäjän puolesta.²²¹

Datasäädöksen soveltamisalan ulkopuolelle on myös rajattu johdettu data, joka tarkoittaa dataa, jonka analysointiin on käytetty lisäinvestointeja.²²² Lisäksi säädöksessä on poikkeussäännöksiä datan jakamisvelvoitteeseen silloin, kun jaettava data sisältää liikesalaisuuksia, datan haltijana on mikro- tai pienyritys tai kun kyseessä on turvallisuutta uhkaava tilanne. Tämän tutkielman kannalta relevantit poikkeukset datan jakovelvoitteeseen ovat johdetun datan käsite sekä liikesalaisuudet. Näin ollen seuraavaksi käsitellään ensin johdetun datan määritelmää, sitten liikesalaisuuksia ja lopulta muita datan jakamisvelvoitteeseen vaikuttavia poikkeustilanteita.

5.4.1 Johdettu data

Datasäädöksen perusteluiden mukaan saataville asetetusta datasta taikka sen metadatasta päätelty tai johdettu tieto ei kuulu jakovelvoitteen piiriin, jos kyseisen datan tuottamiseen on käytetty lisäinvestointeja.²²³ Tällaista dataa kutsutaan *jalostetuksi tai johdetuksi dataksi*. Rajoitus koskee erityisesti tietoa, joka on johdettu saataville asetettavasta datasta monimutkaisilla ja yksinoikeuksien piiriin kuuluvilla algoritmeilla tai ohjelmistoilla. Dataa voidaan jalostaa esimerkiksi sellaisilla algoritmeilla ja ohjelmistoilla, jotka ovat jonkin yksinoikeuden piiriin kuuluvia sekä monimutkaisia, esimerkiksi anturifuusiotekniikalla datan

²²⁰ Kerber 2023, s.6.

²²¹ Butzow ym. 2025, s.11.

²²² Hynönen – Leino – Butzow 2023, s.473.

²²³ Datasäädös, resitaali 15.

johtaminen.²²⁴ Rajausta on perusteltu, sillä jalostettu data on usein arvokkaampaa kuin raakadata ja se saattaa sisältää tietoa datan haltijan tuotekehityksestä tai liikesalaisuuksista.²²⁵ Raakadatan ja johdetun datan erottelulla datasäädöksessä on pyritty myös suojaamaan datan haltijaa ja kannustamaan liiketoiminnan kehittämiseen, sillä datan jatkojalostaminen voi vaatia taloudellisia lisäpanostuksia ja investointeja.²²⁶ Tämän vuoksi jalostetun datan pakollinen jakaminen muille voisi johtaa siihen, että datan haltijat eivät haluaisi panostaa taloudellisesti datan käsittelyyn. Datasäädös ei siis aseta velvollisuutta edellä mainitun datan jakamiseen, mutta datan haltija ja datan käyttäjä voivat silti sopia datan jakamisesta säädöksen estämättä.²²⁷

5.4.2 Muut mahdolliset poikkeustilanteet

Datasäädöksessä on käsitelty myös muutamia muita poikkeustilanteita, joissa muutoin datasäädöksen soveltamisalaan kuuluvaa dataa ei tarvitse jakaa säädöksen velvoittamalla tavalla. Ensimmäinen poikkeus koskee mikro- ja pienyrityksiä. Datasäädöksen 2 luvun määräyksiä ei sovelleta mikroyritysten tai sellaisten pienten yritysten, jotka on eritelty 2 luvun 7 artiklassa, verkkoon liitettyjen laitteiden dataan. Tämä tarkoittaa käytännössä sitä, että mikroyrityksiksi katsotaan sellaiset yritykset, joissa on alle 10 työntekijää ja joiden vuosiliikevaihto on enintään 2 miljoonaa euroa. Pieniä yrityksiä taas ovat sellaiset yritykset, joissa on alle 50 työntekijää ja joiden vuosiliikevaihto on alle 10 miljoonaa euroa. Lisäksi mikro- tai pienyrityksellä ei saa olla yhteyttä sellaiseen yritykseen, joka ei ole mikro- tai pienyritys ja joka suunnittelee IoT-laitteita taikka tarjoaa liitännäispalveluita. Tällä pyritään varmistamaan se, että suuri konserniyritys ei voi kiertää datasäädöksen asettamia velvoitteita sillä, että verkkoon liitettyjen laitteiden valmistus tai datan hallinta siirrettäisiin konsernin pieneen tytäryhtiöön.²²⁸

Datasäädös sisältää myös poikkeussäännöksen tilanteeseen, jossa datan haltija ja käyttäjä voivat sopia dataan pääsyn tai sen käytön rajoittamisesta tai kieltämisestä tilanteissa, joissa kyseinen toiminta voisi heikentää EU:n tai kansallisessa lainsäädännössä säädettyjä

²²⁴ Butzow ym. 2025, s.69.

²²⁵ Butzow ym. 2025, s.72.

²²⁶ Butzow ym. 2025, s.94.

²²⁷ Butzow ym. 2025, s.72.

²²⁸ Butzow ym. 2025, s.74.

turvallisuusvaatimuksia ja aiheuttaa vakavia haittavaikutuksia luonnollisten henkilöiden terveydelle tai turvallisuudelle.²²⁹

²²⁹ Butzow ym. 2025, s. 97.

6 Datan jakamisen minimoinnin strategiat

6.1 Tekninen strategia: johdetun datan tallentaminen

Johdettu data on raakadatasta taikka metadatasta pääteltyä tai johdettua tietoa, jonka tuottamiseen on käytetty lisäinvestointeja taikka datasta omisteisia monimutkaisia algoritmeja, jotka voivat olla osa omisteista ohjelmistoa. Johdettu data voi sisältää erityisesti tietoa, joka on johdettu anturifuusiolla eli keräämällä useista IoT-laitteen sensoreista dataa ja johtamalla siitä tietoa käyttäen monimutkaisia algoritmeja.²³⁰ Kuten edellä on jo todettu, johdettu data ei kuulu datasäädöksen soveltamisalaan ja näin ollen johdettua dataa ei tarvitse jakaa. Mikäli laitteesta olisi saatavilla vain johdetuksi dataksi luokiteltavaa dataa, eikä ollenkaan helposti saatavilla olevaa raaka-, meta- tai esikäsiteltyä dataa, datan haltijalla ei olisi velvollisuutta jakaa laitteen dataa käyttäjän taikka kolmansien osapuolien kanssa.

Datasäädös sisältää velvoitteen laitteen valmistajille suunnitella IoT-laitteet ja niihin liittyvät palvelut teknisesti siten, että data olisi käyttäjän saatavilla helposti, turvallisesti ja maksutta.²³¹ Tämä tarkoittaa sitä, että laitteen valmistajan tulisi ottaa laitteen teknisessä suunnittelussa huomioon datan jakaminen käyttäjän ja kolmannen osapuolen kanssa. Laitteet voidaan suunnitella niin, että niistä on mahdollista saada dataa fyysisesti, esimerkiksi USB-portin kautta, taikka data voidaan asettaa saataville laitteen datantallennustilan tai pilvipalvelun kautta langattomien lähiverkkojen avulla.²³² Mikäli laite on tekniseltä luonteeltaan sellainen, että sen suunnittelu ei mahdollista laitteen käytön tuottaman datan tallentamista tai siirtämistä laitteen ulkopuolelle, laitteen tuottama data ei kuulu datasäädöksen soveltamisalaan.²³³ Datasäädöksen resitaalikappaleen 20 mukaan suunnitteluvaikeus ei tarkoita sitä, että laitteiden valmistajille asetettaisiin velvoite suunnitella IoT-laitteet ja niihin liittyvät palvelut siten, että laitteen tuottamaa dataa henkilötietoja sisältävää tallennetaan tai muuten käsitellään, mikäli tällaisen datan tallentaminen tai käsittely ei ole tarpeen niiden tarkoitusten täyttämiseksi, joita varten tietoja käsitellään.²³⁴

Mikäli laitteen valmistaja/datan haltija haluaa välttää datasäädöksestä johtuvan datanjakovelvollisuuden, vaihtoehdot ovat seuraavat:

²³⁰ Datasäädös resitaali 15.

²³¹ Datasäädös resitaali 20.

²³² Datasäädös, resitaali 22.

²³³ Datasäädös resitaali 20.

²³⁴ Datasäädös resitaali 20.

1. Laitteen tekninen suunnittelu ei mahdollista datan tallentamista tai siirtämistä laitteen ulkopuolelle, jolloin data ei kuulu datasäädöksen soveltamisalaan.
2. Laitteen tekninen suunnittelu mahdollistaa datan tallentamisen tai siirtämisen laitteen ulkopuolelle, mutta laitteeseen tallennettu tai ulkopuolelle siirretty data on johdetussa muodossa, jolloin data ei kuulu datasäädöksen soveltamisalaan.

Seuraavaksi keskitytään siihen, millä toimenpiteillä datan haltija voisi saavuttaa tilanteen, jossa laitteeseen tallennettu tai laitteen ulkopuolelle siirretty data olisi johdettua dataa, jota ei tarvitse jakaa säädöksen velvoittamalla tavalla laitteen käyttäjälle tai kolmannelle osapuolelle. Mikäli datan haltija haluaa minimoida jaettavan datan tai välttyä datan jakamiselta kokonaan, datan haltijan tulee tehdä joko teknisiä toimenpiteitä taikka tuotesuunnitteluratkaisuja.

Tuotesuunnittelun näkökulmasta laitteen valmistaja voisi suunnitella laitteen niin, että laitteesta ei ole mahdollista saada dataa ulos (fyysisesti tai esimerkiksi palvelimelle tai pilvipalveluun), vaan sitä käytettäisiin ainoastaan paikallisesti laitteessa. Datasäädöksen resitaalikappale 20 mukaan helposti saatavilla olevaksi dataksi ei katsota sellaista dataa, jota ei IoT-laitteen suunnittelun vuoksi pystytä tallentamaan tai siirtämään laitteen ulkopuolelle. Näin ollen tällaista dataa ei tarvitse jakaa säädöksen tarkoittamalla tavalla. Tämän strategian näkökulmasta tulee kuitenkin huomata, että mikäli dataa ei voida tallentaa laitteeseen tai siirtää sieltä pois, myöskään datan haltija ei voi hyödyntää tällaista dataa.

6.1.1 Reunalaskenta

Tekninen ratkaisu tarkoittaa käytännössä sitä, että dataa käsitellään laitteessa niin, että sitä ei tallenneta laitteeseen taikka palvelimelle raakadatana taikka esikäsitellyssä muodossa. Datasäädöksen datan jakamista koskevien säännösten lähtökohtana on ollut datankäsittelyn perinteinen tapa, jossa dataa käsitellään keskitetysti, esimerkiksi siirtämällä laitteen antureiden tuottamaa raakadataa IoT-laitteesta pilvipalveluun.²³⁵ Näin ollen laite tallentaa joko sisäisesti tai ulkoiseen tallennustilaan raakadataa, jota jatkokäsitellään ja analysoidaan laitteen ulkopuolella. Tämän ”perinteisen” käsittelytavan lisäksi dataa voidaan käsitellä myös IoT-laitteessa itsessään siirtämättä dataa pois laitteesta, jolloin datan käsittelyä kutsutaan termillä ”edge computing” (suom. reunalaskenta). Se tarkoittaa käytännössä sitä, että laitteen tuottamaa dataa käsitellään lähellä datan lähdettä, eikä dataa siirretä pois laitteesta esimerkiksi

²³⁵ Mitä on edge computing eli reunalaskenta?

pilvipalveluun tai muuhun ulkoiseen tallennustilaan datan käsittelyä varten.²³⁶ Dataa voidaan käsitellä tällä tavoin esimerkiksi IoT-laitteissa, taikka itseohjautuvissa autoissa.²³⁷ Kun dataa käsitellään reunalaskennan avulla, laitteesta pois siirrettävän raakadatan määrää voidaan pienentää, sekä laitteen tuottaman datan antamaa informaatiota voidaan hyödyntää nopeammin suoraan laitteessa, joka puolestaan tehostaa toimintaa sekä vähentää tietojenkäsittelyn viivettä.²³⁸

Edge computing toimii siis sillä tavoin, että laitteen tuottamaa raakadataa ei lähetetä keskitetysti käsiteltäväksi, vaan dataa prosessoidaan, valikoidaan ja analysoidaan paikallisesti laitteessa, ja vasta tämän jälkeen lähetetään eteenpäin esimerkiksi pilvipalveluun tai se tallennetaan.²³⁹ Käytännössä IoT-laitteen sensorit tuottavat raakadataa, jonka jälkeen data kerätään paikallisesti prosessoitavaksi laitteeseen rakennettujen teknisten ratkaisujen ja toimintojen avulla, ja tämän jälkeen prosessoitu data voidaan lähettää keskitettyyn palveluun, jossa sitä voidaan varastoida tai edelleen jatkojalostaa.²⁴⁰ Edge computing ei kuitenkaan ole yksinkertainen ratkaisu, sillä datan käsittelyn tekninen toteutus suoraan laitteeseen vaatii laitteesta fyysistä tilaa, ja riippuen laitteesta tai laitteen käyttöolosuhteista tällaista tilaa voi olla hankala toteuttaa.²⁴¹

6.1.2 Reunalaskentamenetelmän soveltaminen datasäädöksen soveltamisalaan kuuluvaan dataan

Euroopan komissio on ottanut FAQ-muistiossa kantaa datasäännöksen velvoitteiden soveltumiseen edge computing-tilanteissa. Ensinnäkin komissio toteaa, että resitaalikappaleen 20 mukaisesti datan haltijoiden tulee jakaa kaikki helposti saatavilla oleva data, ja tätä määritelmää täsmennetään ”*raaka- tai esikäsitelty data, joka on tallennettu, haettavissa tai jota siirretään ulos IoT-tuotteesta taikka siihen liittyvästä palvelusta*”. Komissio toteaa, että resitaalikappaleen 20 mukaisesti datan ei katsota olevan ”helposti saatavilla”, mikäli tuotteen tekninen ratkaisu tai toteutus estää datan ulkoisen tallennuksen tai siirron. Datasäädöksellä pyritään varmistamaan se, että IoT-laitteiden käyttäjät sekä kolmannet osapuolet saavat

²³⁶ ks. edge processing- käsitteen määrittelystä Mitä on edge computing eli reunalaskenta? sekä What is Edge Computing? Hazelcast.

²³⁷ Mitä on edge computing eli reunalaskenta?

²³⁸ What is Edge Computing? Hazelcast.

²³⁹ What is Edge Computing? HPE.

²⁴⁰ What is Edge Computing? HPE.

²⁴¹ What is Edge Computing? Hazelcast.

pääsyn dataan, ja datasäädöksen tavoitteena on välttää niitä tilanteita, joissa datan haltijat voisivat saada hyötyä datasta, joka on johdettu käyttäjän antamista tiedoista.²⁴²

Komissio toteaa, että datasäädöksen sisältävät velvoitteet soveltuvat dataan, jos siihen on edes jossain vaiheessa ollut pääsy, taikka se on ollut siirrettävissä pois laitteesta. Mikäli IoT-laite käsittelee dataa vain paikallisesti eikä siirrä tietoja ulos, datasäädöksen II luvun velvoitteet eivät siinä tapauksessa soveltuisi laitteen tuottamaan dataan.²⁴³ Mikäli IoT-laitteessa kuitenkin on tekninen mahdollisuus tietojen tallentamiselle tai siirrolle, laitteen valmistajan/datan haltijan tulee harkita, onko olemassa sellaisia ”oikeasuhteisia, teknisesti toteutettavissa olevia ja kustannustehokkaita” menetelmiä, joilla käyttäjä tai kolmas osapuoli voisi saada pääsyn raakadataan tai esikäsiteltyyn dataan.²⁴⁴ Tämän voi ymmärtää viittaukseksi datasäädöksen 2 luvun 3 artiklaan, joka sisältää velvollisuuden suunnitella laitteet siten, että data on - silloin kuin se on teknisesti mahdollista – käyttäjän saatavilla. Nämä kriteerit, oikeasuhtainen, teknisesti toteutettavissa oleva sekä kustannustehokas, ovat kohtuullisen tulkinnanvaraisia, ja ne voivat olla riippuvaisia monesta eri tekijästä, kuten laitteen ominaisuuksista tai datan määrästä. Mikäli datan haltija voi osoittaa, että kriteeristöä täyttävää keinoa datan asettamiseen käyttäjän saataville ei ole olemassa, dataa ei sanamuodon perusteella tarvitsisi asettaa laitteen käyttäjän saataville.

Yksi reunalaskennan soveltumiseen liittyvä muuttuja koskee jo edellä käsiteltyä esikäsiteltyä ja johdetun datan käsitteiden rajanvetoa. Reunalaskenta on yläkäsite, joka tarkoittaa erilaisia datan käsittelytoimenpiteitä, jotka tehdään IoT-laitteessa. Reunalaskennan käsite ei itsessään määrittele sitä, onko reunakäsitelty data johdettua dataa, vaan reunalaskennassa tehdyt käsittelytoimenpiteet määräävät sen, katsotaanko data datasäädöksen kontekstissa esikäsitellyksi vai johdetuksi dataksi. Toisin sanoen näiden reunalaskennassa tehtyjen käsittelytoimenpiteiden tulee olla sellaisia, että datan arvojen tai sisältämän informaation määrittäminen on edellyttänyt lisäinvestointeja. Mikäli reunalaskennassa tehtävät datan käsittelytoimenpiteet voidaan katsoa sellaisiksi toimiksi, jotka ovat edellyttäneet merkittäviä lisäinvestointeja, reunalaskennan tuloksena tallennettu data ei datasäädöksen sanamuodon sekä komission kannanoton perusteella kuulu datasäädöksen soveltamisalaan.

²⁴² Euroopan komissio 2026, s.8.

²⁴³ Euroopan komissio 2026, s.8.

²⁴⁴ Euroopan komissio 2026, s.8.

Mikäli laite ei tallenna raakadataa, myöskään datan haltija ei voi saada raakadataa ja käyttää sitä laitteen suunnittelussa.

6.2 Privacy by design -järjestelmäsuunnittelu

Privacy by design tarkoittaa järjestelmäsuunnittelun muotoa, jonka lähtökohtana on, että tietosuoja on sisäänrakennettuna järjestelmään ja sen perusrakenteeseen, eikä sitä lisätä jälkikäteen ominaisuutena siinä vaiheessa, kun järjestelmä on jo valmis.²⁴⁵ Erilaisia suunnittelumalleja on olemassa useita erilaisia, ja yksi ohjelmistosuunnittelumalleista on esimerkiksi ”Model-View-Controller”, jonka avulla data erotetaan siitä näkymästä, joka esitetään käyttäjälle ja jossa käyttäjä voi muokata dataa.²⁴⁶ Hoepman esittelee artikkelissaan ”*Privacy Design Strategies*” erilaisia Privacy by design -strategioita, joilla tallennettavan datan määrää voidaan vähentää ilman, että se vaikuttaa datan käytettävyyteen.²⁴⁷ Artikkeliki käsittelee strategioita ja dataa henkilötietoja sisältävän datan suojaamisen ja yksityisyyden näkökulmasta. Yksi strategioista on datan minimointi, jolloin yksinkertaisesti käsiteltävän datan määrä rajoitetaan mahdollisimman vähäiseksi, esimerkiksi käyttämällä anonymisointia ja salausta.²⁴⁸ Dataa voidaan myös koostaa, jolloin dataa tallennetaan käsiteltyssä muodossa niin, että siinä on mahdollisimman vähän yksityiskohtia ja tiedot ovat tällöin vähemmän arkaluontoisia.²⁴⁹

Myös datasäädöksen resitaalikappaleessa 8 on otettu kantaa tietojen minimointiin sekä privacy by design -järjestelmäsuunnitteluun ja näiden strategioiden soveltumiseen datasäädöksen näkökulmasta. Resitaalikappale 8 mukaan nämä periaatteet ovat keskeisiä silloin, kun käsitellään dataa, johon kohdistuu yksilöiden perusoikeuksiin kohdistuvia merkittäviä riskejä, ja näin ollen datasäädöksessä määriteltyjen osapuolien olisi toteutettava erilaisia teknisiä toimenpiteitä, kuten tiedon salausta ja anonymisointia, jotta datasta voidaan saada tarpeellinen tieto ilman, että dataa siirretään osapuolten välillä taikka sitä joudutaan kopioimaan.²⁵⁰

Euroopan komissio on ottanut FAQ-muistiossa kantaa siihen, miten datan prosessointia tulisi arvioida siinä tilanteessa, kun dataa anonymisoidaan eri menetelmillä. Komission

²⁴⁵ Hoepman 2014, s.446.

²⁴⁶ Hoepman 2014, s.448.

²⁴⁷ Hoepman 2014, s.449.

²⁴⁸ Hoepman 2014, s.452-453.

²⁴⁹ Hoepman 2014, s.455.

²⁵⁰ Datasäädös resitaali 8.

näkemyksen mukaan datan suojaaminen esimerkiksi yksityisyyttä suojaavilla tekniikoilla ei tarkoita sitä, että näiden tekniikoiden käytöstä syntyvää dataa tulisi pitää johdettuna datana vain siksi, että datan saamiseen on käytetty suojaamistekniikoita.²⁵¹ Komissio viittaa resitaalikappaleeseen 15, jonka mukaan johdettua data ei kuulu jakovelvoitteen piiriin, sillä tarkoituksena on suojata datan haltijoiden tekemiä lisäinvestointeja, joilla datasta pyritään saamaan arvoja tai informaatiota. Komissio on kuitenkin katsonut, että toimenpiteet, jotka tehdään vain siksi, että dataa voidaan käsitellä suojatusti, eivät ole sellaisia datasäädöksessä tarkoitettuja toimenpiteitä, jotka määrittäisivät arvoja tai tuottaisivat informaatiota.²⁵² Tästä voidaan päätellä, että vaikka dataa käsiteltäisiinkin sellaisilla toimenpiteillä, jotka ovat vaatineet investointeja, dataa ei välttämättä katsota johdetuksi dataksi, sillä investointien luonne ei ole sellainen, että sillä olisi kaupallista arvoa. Mikäli datan haltija haluaisi hyödyntää Privacy by design -järjestelmäsuunnittelua ja välttää datan jakamisen, järjestelmäsuunnittelussa käytetyt tekniset ratkaisut tulisi olla luonteeltaan sellaisia, että ne määrittävät datan arvoja, tuottavat informaatiota ja datan haltija on tehnyt kyseisten teknisten ratkaisujen vuoksi taloudellisia investointeja, jotka lisäävät datan kaupallista arvoa.

Samassa komissio on ottanut kantaa siihen, että vaikka datan haltija hyödyntäisi anonymisointi- tai salaustekniikoita datan käsittelyssä, datan haltija ei voi automaattisesti vapautua velvollisuudestaan jakaa dataa käyttäjän tai kolmannen osapuolen kanssa.²⁵³ Komissio nostaa esiin, että kun tietoja siirretään laitteen ulkopuolelle, käyttäjille ja kolmansille osapuolille tulee tässä vaiheessa jakaa dataa, ennen kuin sille tehdään salaustoimenpiteitä tai muita käsittelytoimenpiteitä niin, että data anonymisoidaan. Toinen komission esiin nostama seikka koskee datan yhdistettävyyttä sen alkuperään: mikäli salattu data saadaan helposti yhdistettyä siihen laitteeseen, josta se on peräisin, data kuuluu säädöksen jakovelvoitteiden piiriin.²⁵⁴

Koska tutkielman pääpaino on ei-henkilötietoja sisältävässä datassa, tätä henkilötietostrategiaa ei tutkielman rajallisuuden vuoksi käsitellä enempää. Tarkoituksena on tuoda ilmi, että myös henkilötietoja sisältävän datan osalta yrityksellä voi olla strategioita, joilla dataa pyritään muokkaamaan niin, ettei sitä tarvitsisi jakaa datasäädöksen velvoittamalla tavalla. Toisaalta IoT-laitteet voivat tuottaa sekä henkilötietoja, että ei-henkilötietoja

²⁵¹ Euroopan komissio 2026, s.12.

²⁵² Euroopan komissio 2026, s.12.

²⁵³ Euroopan komissio 2026, s.12.

²⁵⁴ Euroopan komissio 2026, s.12.

sisältävää dataa, jolloin datan haltija voi hyödyntää useampaa datastrategiaa, ja tämän vuoksi on tärkeää nostaa esille, että myös henkilötietoja sisältävän datan osalta on olemassa erilaisia käsittelystrategioita.

6.3 Oikeudellinen strategia: liikesalaisuuksien suoja

Butzow ym. esittivät teoksessaan hypoteettisen tilanne-esimerkin, jossa datan haltija luovuttaa datasäädöksen velvoittamana liikesalaisuuksia sisältävää dataa kolmannelle osapuolelle, kuten huolto- tai korjauspalveluntarjoajalle, joka on datan haltijan suora kilpailija. Vaikka luovutettava data sisältäisi datan haltijan liikesalaisuuksia esimerkkitalanteen mukaisesti, se ei lähtökohtaisesti anna datan haltijalle perustetta kieltäytyä datan jakamisesta.²⁵⁵ Jotta liikesalaisuuksia voitaisiin suojata asianmukaisesti, datasäädökseen on sisällytetty sääntelyä liikesalaisuuksia sisältävän datan luovuttamisesta, ja tällä pyritään suojaamaan datan sisältämiä liikesalaisuuksia tilanteissa, joissa dataa jaetaan kolmansille osapuolille, jotka saattavat olla datan haltijan kilpailijoita.²⁵⁶

Datasäädöksessä säädetään liikesalaisuuksien suojasta 4 ja 5 artikloissa, joiden perusteella datan haltijalla on mahdollisuus vaatia sekä käyttäjää että käyttäjän pyynnöstä dataa vastaanottavaa kolmatta osapuolta tekemään riittävät toimenpiteet, joilla liikesalaisuutta suojellaan.²⁵⁷ Datasäädöksen 4 artiklan 6 kohdan mukaan datan haltijan on yksilöitävä liikesalaisuuksia sisältävä data sekä asiaankuuluva metadata, ja datan haltijan ja käyttäjän on ensin sovittava ja tämän jälkeen toteutettava kaikki tarvittavat tekniset ja organisatoriset toimenpiteet liikesalaisuuksien suojaamiseksi, ennen kuin niitä sisältävää dataa jaetaan. Datasäädöksen 5 artiklan 9 kohdan mukaisesti liikesalaisuudet on säilytettävä myös silloin, kun dataa jaetaan kolmansille osapuolille. Datasäädöksen 5 artiklan 9 kohdan mukaan kolmannelle osapuolelle saa ilmaista liikesalaisuuksia vain sellaisessa tilanteessa, kun niiden ilmaiseminen on ”ehdottoman välttämätöntä käyttäjän ja kolmannen osapuolen välillä sovitun käyttötarkoituksen täyttämiseksi”. Tässäkin tapauksessa datan haltijan on yksilöitävä liikesalaisuutena suojattava data sekä metadata ja sovittava kolmannen osapuolen kanssa tarvittavista toimenpiteistä, joilla liikesalaisuuksia voidaan suojata. Edellä mainitut kohdat eivät siis anna datan haltijalle oikeutta olla jakamatta liikesalaisuuksia sisältävää dataa, vaan

²⁵⁵ Butzow ym. 2025, s.110.

²⁵⁶ Butzow ym. 2025, s.110.

²⁵⁷ Butzow ym. 2025, s.152.

niillä säännellään tarpeellisia ja oikeasuhtaisia suoja-toimia, jotta liikesalaisuudet voidaan säilyttää.

6.3.1 Datan jakamisesta kieltäytyminen liikesalaisuusperusteella

Datasäädös tarjoaa datan haltijalle mahdollisuuden poikkeustapauksissa keskeyttää liikesalaisuuksia sisältävän datan jakamisen taikka pidättäytyä tällaisen datan jakamisesta. Tämä koskee tilanteita, joissa käyttäjä tai datan vastaanottaja ei ole ryhtynyt sovittuihin tarpeellisiin toimenpiteisiin datan suojaamiseksi taikka niistä ei ole päästy sopimukseen. Tätä mahdollisuutta säännellään datan haltijan ja käyttäjän välisen datan jakamisen osalta datasäädöksen 4 artiklan 7 kohdassa, ja datan haltijan sekä kolmannen osapuolen välisen datan jakamisen osalta 5 artiklan 10 kohdassa. Säännösten sisällöllinen merkitys on sama, ja niillä annetaan datan haltijalle oikeus pidättäytyä liikesalaisuuksiksi määritellyn datan jakamisesta taikka keskeyttää datan jakaminen, mikäli käyttäjä taikka kolmas osapuoli ei toteuta sovittuja toimenpiteitä liikesalaisuuksien suojaamiseksi tai muuten heikentää liikesalaisuuksien luottamuksellisuutta, taikka suojaavista toimenpiteistä ei päästy sopimukseen osapuolten välillä. Lisäksi säännöksissä asetetaan datan haltijalle velvollisuus perustella keskeytys- tai pidättäytymispäätös, sekä toimittaa se käyttäjälle tai kolmannelle osapuolelle tiedoksi. Datan haltijan on ilmoitettava datasäädöksen 37 artiklan mukaisesti nimetyille toimivaltaiselle viranomaiselle pidättäytymisestä sekä yksilöitävä, mitä toimenpiteitä ei ole sovittu tai pantu täytäntöön ja mikä liikesalaisuus on vaarantunut.²⁵⁸ Tätä pidättäytymisoikeutta ei siis voi käyttää ensisijaisena keinona liikesalaisuuksien suojaamiselle, vaan ensin datan haltijan tulee pyrkiä sopimaan liikesalaisuuksien suojaamisesta datan jakamistilanteissa.²⁵⁹

Datasäädös sisältää poikkeussäännöksen tilanteeseen, jossa datan haltija katsoo, että tarpeellisista toimenpiteistä huolimatta liikesalaisuuksia sisältävän datan jakamisesta kolmannelle osapuolelle aiheutuisi erittäin todennäköisesti taloudellista vahinkoa. Tällaisessa tilanteessa datan haltija voi kieltäytyä datan jakamisesta kokonaan. Datan haltijan oikeudesta evätä pääsyyntö dataan säädetään datasäädöksen 5 artiklan 11 kohdassa, jonka mukaan

”jos datan haltija, joka on liikesalaisuuden haltija, voi osoittaa, että sille aiheutuu erittäin todennäköisesti vakavaa taloudellista vahinkoa liikesalaisuuksien ilmaisemisesta kolmannen osapuolen tämän artiklan 9 kohdan mukaisesti

²⁵⁸ Ks. datasäädös art. 4 kohta 7 sekä art. 5 kohta 10.

²⁵⁹ Butzow ym. 2025, s.159.

toteuttamista teknisistä ja organisatorisista toimenpiteistä huolimatta, se datan haltija voi tapauskohtaisesti ja poikkeuksellisesti evätä pääsypyynnön kyseiseen dataan. Kyseinen osoittaminen on perusteltava asianmukaisesti objektiivisilla seikoilla, joita ovat erityisesti liikesalaisuuksien suojan täytäntöönpanokelpoisuus kolmansissa maissa, pyydetyn datan luonne ja luottamuksellisuuden taso sekä verkkoon liitetyn tuotteen ainutlaatuisuus ja uutuus.”

Kuten datan jakamisen keskeytys- ja pidättäytymistilanteissa, myös pääsypyynnön eväämisestä tulee ilmoittaa kirjallisesti kolmannelle osapuolelle, ja datan haltijan tulee ilmoittaa kieltäytymisestä myös 37 artiklan mukaiselle toimivaltaiselle viranomaiselle.²⁶⁰ Datasäädöksen resitaalikappaleessa 31 on täsmennetty pääsypyynnön eväämistä. Pyyntö evääminen olisi mahdollista vain poikkeuksellisissa olosuhteissa ja tapauskohtaisesti, ja vakavan taloudellisen vahingon, kuten vakavien ja korjaamattomien taloudellisten menetysten aiheutuminen tulisi olla erittäin todennäköistä.²⁶¹

Jotta datan haltija voisi kieltäytyä liikesalaisuuksia sisältävän datan jakamisesta, tulee kahden edellytyksen täytyä: ensinnäkin jaettavan datan tulee sisältää liikesalaisuus, ja 5 artiklan 11 kohdassa mainittujen kriteereiden tulee täytyä. Käsittelykappaleet etenevät niin, että ensin käsitellään liikesalaisuuden käsitettä ja sen soveltumista dataan, ja tämän jälkeen käsitellään sitä, missä tilanteissa datan haltija voi vedota 5 artiklan 11 kohtaan kieltäytyessään datan jakamisesta.

6.3.2 Millainen data voidaan katsoa liikesalaisuudeksi?

Datasäädöksen resitaalikappaleessa 31 viitataan liikesalaisuusdirektiiviin²⁶², kun puhutaan datasäädöksessä suojatuista liikesalaisuuksista. Datasäädöksen 2 artiklan 18 kohdassa on määritely, että liikesalaisuudella tarkoitetaan liikesalaisuusdirektiivin 2 artiklan 1 alakohdassa määriteltyä liikesalaisuutta, eli direktiivin liikesalaisuuden määritelmä soveltuu myös datasäädöksessä tarkoitettuun liikesalaisuuteen.

Jotta data voitaisiin katsoa liikesalaisuudeksi, tulee kaikkien kolmen liikesalaisuusdirektiivin 2 artiklan 1 alakohdassa määritellyn kriteerin täytyä samanaikaisesti. Kyseisen 2 artiklan 1 alakohdan mukaan liikesalaisuus on tietoa, joka on salaista niin, ettei se ole yleisesti tiedossa

²⁶⁰ Ks. datasäädös 5 artikla 11 kohta

²⁶¹ Datasäädös resitaali 31.

²⁶² Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943, julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta. Annettu 8.6.2016.

tai helposti saatavilla, tiedolla on salaisen luonteensa vuoksi taloudellista arvoa ja salaisuuden suojaamiseksi sen haltija on ryhtynyt kohtuullisiin toimenpiteisiin, jotta tieto pysyisi salassa. Tiedon tulee siis olla vain rajatun henkilöpiirin tiedossa tai saatavissa, tiedolla tulee olla taloudellista arvoa ja tiedon haltijan on suojattava tietoa kohtuullisin toimenpitein, jotta se voidaan katsoa liikesalaisuudeksi. Mikäli kaikki kriteerit eivät täyty, tieto ei täytä liikesalaisuuslaissa määriteltyjä kriteereitä, eikä sitä näin ollen katsota liikesalaisuudeksi.

Kuten liikesalaisuuden määritelmästä voidaan päätellä, liikesalaisuuksia eivät ole sellaiset tiedot, jotka ovat yleisessä tiedossa ja helposti saatavilla taikka sellaiset tiedot, joilla ei ole taloudellista arvoa. Kun tätä sovelletaan dataan, voidaan katsoa, että datasta ilmenevät tavanomaiset, tuotteen toiminnasta tai datan käsittelystä yleisesti pääteltävissä olevat tiedot, jotka eivät paljasta laitteen valmistajan tai datan haltijan omaperäisiä, taloudellista arvoa sisältäviä toimenpiteitä taikka teknisiä ratkaisuja, eivät voi nauttia liikesalaisuuksien suojaa.²⁶³ Butzow ym. ovat katsoneet teoksessaan, että tavanomaisten tietojen ja taloudellista arvoa sisältävien liikesalaisuuksien välissä vallitsee harmaa alue, johon ei ole selkeää sääntelyä, oikeuskäytäntöä tai viranomaisohjeistusta.²⁶⁴

Tutkielmassa on jo selvitetty, että datasäädöksen soveltamisala koskee raakadataa sekä esikäsiteltyä dataa. Johdettu data ei kuulu säädöksen soveltamisalaan. Näin ollen datasäädöksen sisältämät liikesalaisuuden suojaa koskevia säännöksiä sovelletaan laitteiden antureiden tuottamaan raakadataan ja tällaisen datan metadataan, sekä esikäsiteltyyn dataan.

Ulla-Maija Mylly on artikkelissaan ”*Trade Secrets and the Data Act*” soveltanut liikesalaisuuden määritelmää dataan nimenomaan datasäädöksen määräysten näkökulmasta, ja Josef Drexl on teoksessaan ”*Data Access and Control in the Era of Connected Devices*” soveltanut liikesalaisuuden määritelmän kriteerejä IoT-laitteiden tuottamaan dataan. Ensimmäinen kriteeri on, että datan sisältämän tiedon tulisi olla salaista, eli se ei saa olla yleisesti tiedossa tai yleisesti saavutettavissa.²⁶⁵ Mikäli data on yleisesti tiedettyä, tai eri osapuolilla on siihen vapaa pääsy, tietoa ei voida katsoa salaiseksi.²⁶⁶ Toinen vaatimus on, että IoT-laitteen tuottamalla datalla tulee olla datan haltijalle taloudellista arvoa.²⁶⁷ Tästä voidaan päätellä, että tiedon tulee olla luonteeltaan sellaista, joka parantaa datan haltijan

²⁶³ Butzow ym.2025, s.156.

²⁶⁴ Butzow ym.2025, s.156.

²⁶⁵ Mylly 2024, s.373.

²⁶⁶ Drexl 2018, s.93.

²⁶⁷ Mylly 2024, s.373.

asemaa datamarkkinoilla.²⁶⁸ Viimeisenä vaatimuksena on, että datan haltijan on tullut ryhtyä toimiin datan suojaamiseksi ja pitääkseen tiedon salaisuutena.²⁶⁹ Datan suojaaminen ja salaisuuden vaaliminen edellyttää datan haltijalta aktiivisia toimia, kuten datan suojaamista teknisillä toimenpiteillä taikka salassapitosopimuksilla sellaisten osapuolten välillä, joilla on pääsy dataan.²⁷⁰

Yhteenvetona Drexl toteaa teoksessaan, että liikesalaisuuden suojaa nauttii ainoastaan sellainen data, jonka salassapito tuottaa datan haltijalle taloudellista hyötyä, ja tällaisen tiedon salassa pitämiseksi on tehty aktiivisia ja riittäviä toimenpiteitä.²⁷¹ Mikäli nämä kolme edellä selostettua kriteeriä täyttyvät, raakadatan sekä esikäsitellyn datan voidaan katsoa sisältävän liikesalaisuuksia.

Käytännön tasolla liikesalaisuuksien suojan soveltuminen raakadataan tai esikäsiteltyyn dataan on usein rajattua.²⁷² Tämä johtuu raakadatan luonteesta. Drexl esittämän analyysin mukaan, kun verrataan liikesalaisuuden määritelmää dataan, voidaan katsoa, että liikesalaisuuksilla pyritään suojaamaan tietoa sen semanttisella tasolla, eli suojan kohteena on tieto, jolla on jokin merkitys.²⁷³ Datasäädöksen määrittelemä raakadatasta on, että raakadata on automaattisesti tuotettuja tietopisteitä.²⁷⁴ Koska raakadataa täytyy aina käsitellä jollakin tavalla, jotta datasta voidaan saada käyttökelpoista ja ymmärrettävää, voidaan katsoa, että raakadata ei tämän vuoksi yleensä täytä liikesalaisuuden kriteerejä.²⁷⁵ Tämä johtuu siitä, että raakadata ei ole semanttista tietoa, vaan se on tietopisteitä, joista jalostamalla ja analysoimalla saadaan tietoa. Yksittäisellä datajoukolla ei myöskään ole katsottu olevan suurta taloudellista arvoa datan haltijalle, vaan taloudellinen arvo syntyy, kun yksittäisiä datajoukkoja yhdistetään, analysoidaan sekä verrataan toisiinsa.²⁷⁶ Mylly toteaaakin, että tavallisesti datasäädöksen säätelemissä datan jakamistilanteissa ei jaeta sellaista tietoa, joka täyttäisi liikesalaisuuden määritelmän kriteerit, sillä jaettava data on tyypiltään raakadataa.²⁷⁷

²⁶⁸ Drexl 2018, s.93.

²⁶⁹ Mylly 2024, s.373.

²⁷⁰ Drexl 2018, s.93.

²⁷¹ Drexl 2018, s.93.

²⁷² Noyette – Stähler – Margoni 2025 s.989.

²⁷³ Drexl 2018, s. 92.

²⁷⁴ Datasäädös, resitaali 15.

²⁷⁵ Mylly 2024, s.370.

²⁷⁶ Drexl 2018, s.94.

²⁷⁷ Mylly 2024, s. 390.

Raakadata on datan käsittelyn alkupiste, ja käsittelymenetelmillä raakadatasta voidaan erilaisin menetelmin johtaa ja analysoida erilaisia tietoja. Tämä tarkoittaa sitä, että raakadatasta voidaan erilaisin datankäsittelymenetelmin johtaa sellaista tietoa, joka voi paljastaa datan haltijan liikesalaisuuksia, vaikka raakadata yksin ei liikesalaisuuden kriteereitä täyttäisikään.²⁷⁸ Myös Drexl on esittänyt analyysissään samansuuntaisen näkökulman, ja hänen mukaansa liikesalaisuudet voidaan koodata digitaaliseen muotoon, jolloin data itsessään voi sisältää liikesalaisuuksia.²⁷⁹ Näin ollen raakadata itsessään ei näytä täyttävän liikesalaisuuden kriteerejä, jolloin sitä ja siihen liittyvää metadataa tulisi jakaa, ja tämä voi johtaa siihen, että vastaanottaja voi metadatan avulla saada raakadatasta selville datan haltijan liikesalaisuuksia. Raakadatan luonne asettaa kuitenkin haasteen datan haltijalle, sillä liikesalaisuuden yksilöinti raakadatasta voi olla hankalaa, ja se voi edellyttää laajempaa harkintaa siitä, mitä datan vastaanottaja voi saada raakadatasta selville ja voiko datan jatkokäsittely tai datan analysointi paljastaa datan haltijan liikesalaisuuksia laitteen käyttäjälle tai datan vastaanottajalle.²⁸⁰

6.3.3 Missä tilanteissa datan haltija voi rajoittaa datan jakamista liikesalaisuuksien suojaamisen perusteella?

Mikäli datan haltija haluaa vedota datasäädöksen liikesalaisuuden suojaa koskeviin artikloihin, datan haltijan on ensin täytynyt tunnistaa ja yksilöidä jakovelvoitteen piirissä olevan datan sisältämät liikesalaisuudet. Tämän tunnistamisen ja yksilöimisen jälkeen, ennen kuin dataa jaetaan käyttäjälle tai kolmannelle osapuolelle, datan haltijan tulee ensisijaisesti sopia käyttäjän tai kolmannen osapuolen kanssa siitä, millaisin toimenpitein haltijan tunnistamia liikesalaisuuksia suojataan. Nämä toimenpiteet voivat olla muun muassa pääsyoikeuden rajaaminen liikesalaisuuksia sisältävään dataan, menettelytapaohteet datan käsittelyyn, erilaisten mallisopimusehtojen käyttäminen tai salassapitosopimuksen laatiminen tai muut tekniset toimenpiteet.²⁸¹ Mikäli osapuolet eivät pääse sopimukseen tarpeellisista toimenpiteistä taikka käyttäjä tai kolmas osapuoli ei suojaa liikesalaisuuksia sovitun mukaisesti, datan haltija voi keskeyttää datan jakamisen taikka pidättäytyä jakamasta liikesalaisuuksiksi määriteltyä dataa.²⁸² Mikäli datan haltija pystyy osoittamaan, että se on

²⁷⁸ Mylly 2024, s.373.

²⁷⁹ Drexl 2018, s.92.

²⁸⁰ Butzow ym. 2025, s.157.

²⁸¹ Datasäädös resitaali 31.

²⁸² Keller 2025, s.217.

pyrkinyt sopimaan liikesalaisuuksia suojaavista toimenpiteistä mutta toinen osapuoli ei ole suostunut sovintoon tai suorittanut sovittuja toimenpiteitä, datan haltijan tulee esittää konkreettiset perustelut siitä, että kyseiset toimenpiteet ovat tarpeellisia liikesalaisuuksien suojaamiseksi.²⁸³ Mikäli datan jakamisesta on sovittu asianmukaisesti, mutta liikesalaisuuksia sisältävän datan jakaminen aiheuttaisi erittäin todennäköisesti vakavaa taloudellista vahinkoa datan haltijalle, se voi evätä kolmannen osapuolen pyynnön saada tällaista dataa. Tämä mekanismi on kuitenkin 5 artiklan 11 kohdan sanamuodon mukaisesti tapauskohtainen ja poikkeuksellinen, ja sen käyttö edellyttää objektiivisia perusteluita.

Tilanteet, joissa datan haltija voisi hyödyntää liikesalaisuuksien suojausta ja minimoida datan jakamista tai jopa kieltäytyä jakamisesta kokonaan, rajautuvat edellä esitetyn mukaisesti yhtäältä liikesalaisuuden käsitteen soveltumisella datasäädöksen velvoitteiden perusteella jaettavan datan käsitteeseen, ja toisaalta datasäädöksen 5 artiklan 9 ja 11 kohtaan.

Lähdetään oletuksesta, että datan jakamisen välttäminen tai jaettavan datan määrän minimointi on datan haltijan intressissä. Jotta datan haltija voisi minimoida datan jakamisen tai välttää sen kokonaan 5 artiklan 11 kohdan mukaisesti, laitteen tuottaman datan tulisi täyttää liikesalaisuuden määritelmän kriteerit. Tämä on kaiken alkupiste, sillä ilman, että data täyttää liikesalaisuuden kriteeristön, sitä ei katsota liikesalaisuudeksi ja liikesalaisuutta koskevia poikkeussääntöjä ei sovelleta. Raakadatan osalta kuvio on haasteellinen, sillä data ei itsessään välttämättä sovellu liikesalaisuudeksi sen luonteen vuoksi, mutta se voi sisältää liikesalaisuuksia, jotka ilmenevät, kun dataa käsitellään. Esikäsitellyn datan osalta voidaan katsoa, että data on liikesalaisuuden tarkoittamaa tietoa, jolloin se voidaan katsoa liikesalaisuudeksi, mikäli data täyttää kriteeristön, eli se on taloudellisesti arvokasta ja salaista.

Datasäädöksen 5 artiklan 9 kohdan mukaisesti käyttäjä saa ilmaista datan haltijan liikesalaisuuksia kolmannelle vain niiltä osin kuin tiedon jakaminen on käyttäjän ja kolmannen osapuolen välisen sopimuksen täyttämiseksi ehdottomasti välttämätöntä. Näin ollen datan haltija voisi vedota siihen, että liikesalaisuuksia sisältävän datan jakaminen ei ole välttämätöntä käyttäjän ja kolmannen osapuolen sopimuksen täyttämiseksi, ja näin välttyä datan jakamiselta. Datan haltijan intressissä on pyrkiä rajoittamaan jaettavaa dataa mahdollisimman tehokkaasti vetoamalla juurikin tietojen tarpeellisuuteen.²⁸⁴ Tätä on

²⁸³ Butzow ym. 2025, s.166.

²⁸⁴ Kerber 2023, s.12.

ennakoitu myös oikeuskirjallisuudessa, sillä on katsottu, että datasäädöksen sisältämä liikesalaisuutta koskeva sääntely antaa datan haltijalle mahdollisuuden yksilöidä liikesalaisuuksia sisältävä data ja näin ollen vaatia sen suojaamista, ja tämä voi johtaa siihen, että liikesalaisuuksiin vedotaan liiallisesti ja datan vapaa liikkuvuus voi häiriintyä.²⁸⁵

Edellä on siis todettu, että liikesalaisuudet tulee suojata asianmukaisilla toimenpiteillä silloin, kun dataa luovutetaan kolmansille osapuolille. Mikäli käyttäjä tai kolmas osapuoli on valmista hyväksymään nämä suojaamistoimenpiteet, voidaan katsoa, että pyyntöä saada liikesalaisuuksia sisältävää dataa ei voitaisi hylätä.²⁸⁶ Datan haltija voi kuitenkin kieltäytyä datan jakamisesta myös tällaisessa tilanteessa datasäädöksen 5 artiklan 11 kohdan mukaisesti, mutta sen tulee kyetä osoittamaan, että suojatoimenpiteistä huolimatta sille aiheutuisi erittäin todennäköisesti vakavaa taloudellista vahinkoa.

Kieltäytymisen perusteena datan haltijan tulisi siis esittää konkreettinen kuvaus siitä, millaista vakavaa taloudellista vahinkoa datan luovuttamisesta aiheutuu. Kyseessä on siis datan haltijan esittämä hypoteettinen tilanne tai ennustus tulevaisuudesta, jonka arviointiin käytetään tapauskohtaista harkintaa. Tämän seikan valossa mahdollisuus vedota tähän oikeuteen on nykyhetkellä epävarmaa, ja vaatisi objektiivisten kriteereiden lisäämistä taikka oikeuskäytäntöä arvioinnin tueksi. Taloudellisen vahingon aiheutumisen arviointiin vaikuttavat muun muassa datan luonne ja luottamuksellisuuden taso sekä verkkoon liitetyn tuotteen ainutlaatuisuus ja uutuus. Kun otetaan huomioon se, kuinka haastavaa liikesalaisuuden määritelmän soveltaminen on datasäädöksen nojalla jaettavaan dataan, voidaan ajatella, että arviointiperusteena käytetty ”datan luonne” edellyttää, että data tulisi olla ensinnäkin liikesalaisuuden kriteeristön täyttävää, ja lisäksi laadultaan sellaista, että sen paljastuminen voisi aiheuttaa datan haltijan liiketoiminnalle merkittävää vahinkoa.

Lisäksi tulee huomata, että liikesalaisuuden suoja ei anna yksinoikeutta tietoon, vaan se suojaa tiedon oikeudettomalta hyödyntämiseltä, mikä tarkoittaa, että kilpailijat voivat käytännössä saada saman tiedon esimerkiksi oman tuotekehityksensä taikka ”reverse engineering” -tekniikan perusteella.²⁸⁷ Reverse engineering tarkoittaa käänteismallinnusta, jossa tuotetta analysoidaan sen toiminnan selvittämiseksi ja sen jälkeen saatujen tietojen

²⁸⁵ Mylly 2024, s. 390.

²⁸⁶ Noyette – Stähler – Margoni 2025, s.989.

²⁸⁷ Mylly 2024, s.368.

perusteella valmistetaan analysoitua tuotetta vastaava uusi tuote.²⁸⁸ Tämänkaltaisen tuotekehitysstrategian käyttäminen on datasäädöksen valossa ongelmallista, sillä datasäädös kieltää kolmatta osapuolta käyttämästä vastaanottamaansa dataa kilpailevan tuotteen kehittämiseen.²⁸⁹ Datasäädöksen 6 artiklan 2 kohdan e -alakohta kieltää kolmatta osapuolta käyttämästä dataa sellaisen tuotteen kehittämiseen, ”*joka kilpailee sen verkkoon liitetyn tuotteen kanssa, josta sen saama data on peräisin*”. Näin ollen, mikäli kolmas osapuoli vastaanottaa datan haltijan dataa datasäädöksen perusteella, se ei saa käyttää dataa käänteismallinnukseen. Datasäädös kuitenkin sallii datan käytön laillisiin tarkoituksiin, mikä tarkoittaa, että datan vastaanottaja voi kehittää saamansa datan perusteella palvelun, joka kilpailee datan haltijan tarjoamien palveluiden kanssa.²⁹⁰

Tästä voidaan huomata, että datasäädös tuo mielenkiintoisen vivahteen siihen, kuinka paljon kilpailevat yrityksen haluavat saada dataa datan haltijalta datasäädöksen määräysten mukaisesti. Kilpailevalla yrityksellä eli datan vastaanottajalla voi olla oikeus saada dataa datasäädöksen nojalla, mutta se ei saa käyttää dataa kilpailevan tuotteen luomiseen. Mikäli datan vastaanottajan intressissä on kehittää datan haltijan tuotteen kanssa kilpailevaa tuotetta, sen ei välttämättä kannata ottaa vastaan dataa, sillä se voi vaikuttaa siihen, millaiset mahdollisuudet datan vastaanottajalla on kehittää kilpailevaa tuotetta tulevaisuudessa.²⁹¹ Tämä voi osaltaan hyödyttää datan haltijaa, sillä kilpailijan tuotekehitys on datan saamisen jälkeen suurennuslasin alla, mutta käytännössä datan haltijan voi olla hankalaa näyttää toteen, että kilpailija olisi hyödyntänyt dataa oman laitteensa tuotekehityksessä.

Kaiken kaikkiaan voidaan todeta, että liikesalaisuussuojan hyödyntäminen datan jakamisen minimoinnissa tai välttämiseksi on haastavaa, sillä pääasiassa liikesalaisuuksien suojaaminen edellyttää vain suojatoimia, eikä datasäädös anna oikeutta pidättäytyä datan jakamisesta kuin muutamassa poikkeustilanteessa. Ensinnäkin voidaan todeta, että liikesalaisuuden määritelmän kriteerit sopivat suoraan sovellettuna heikosti datasäädöksessä määriteltyyn raakadatan käsitteeseen. Mikäli raakadataa ja siihen kuuluvaa metadataa jaetaan rajoituksetta, riskinä on, että vastaanottaja voi saada raakadatasta johtamalla selville liikesalaisuuksia. Näin ollen voidaan katsoa, että liikesalaisuuksia määritellessä tulee ottaa huomioon myös se, mitä tietoja raakadata ja metadata voivat yhdessä paljastaa datan vastaanottajalle. Toisena

²⁸⁸ TEPA-termipankki.

²⁸⁹ Mylly 2024, s.373.

²⁹⁰ Mylly 2024, s. 385.

²⁹¹ Mylly 2024, s.385.

heikkoutena on se, että datan jakamisesta pidättäytyminen on säädöksen näkökulmasta hyvinkin rajallista ja poikkeuksellista. Datasäädös mahdollistaa ainoastaan poikkeustapauksissa sen, ettei datan haltijan tarvitse antaa pääsyä laitteen tuottamaan dataan. Muutoin datasäädös ainoastaan tarjoaa sääntelyä siihen, että dataa tulee suojata tarpeellisin toimenpitein, ja toisaalta siihen, että kilpaileva taho ei saa käyttää dataa kilpailevien tuotteiden kehitykseen.

7 Johtopäätökset

7.1 Mitä datasäädöksen soveltaminen tarkoittaa laitteen valmistajan tai datan haltijan näkökulmasta

Kuten edellä on todettu, ennen datasäädöksen voimaantuloa yritykset ovat hyödyntäneet ei-henkilötietoja sisältävää dataa tuotekehityksessään, ja muutoinkin kohdelleet dataa kuin omaisuutenaan, joka synnytti datamarkkinoille lock in -tilanteen.²⁹² Datasäädös ei kuitenkaan sääntele datan omistusoikeutta, vaan se keskittyy tilanteisiin, joissa eri tahoilla on oikeus käyttää ja saada pääsy IoT-laitteiden ja niihin liittyvien palveluiden tuottamaan dataan.²⁹³ Datasäädöksen lähtöpisteenä on erityisesti ei-henkilötietoja sisältävä teollinen data, jonka komissio näkee olevan avainasemassa EU:n sisämarkkinoiden kilpailun ja innovaatioiden edistämiseen. Datasäädöstä on myös kritisoitu, sillä sen on katsottu asettavan pakottavia velvoitteita myös niille osa-alueille, joissa ei ole nähtävissä minkäänlaista markkinavoiman epätasapainoa, taikka tämä epätasapaino on päinvastainen säädöksen tavoitteiden kanssa.²⁹⁴

Datasäädöksen myötä datan yksipuolinen hyödyntäminen ei enää ollut mahdollista, sillä datasäädöksen voimaantulon jälkeen ei-henkilötietoja sisältävän datan hyödyntämisestä tuotekehityksessä tai muussa tarkoituksessa on ollut sovittava etukäteen laitteen käyttäjän kanssa, eli käytännössä yritysten tulee sisällyttää tämä pyyntö oikeudesta käyttää dataa esimerkiksi sopimusehtoihin, mikäli dataa halutaan hyödyntää entiseen tapaan.²⁹⁵ Pakottavien datanjakosäännösten lisäksi yksi merkittävimmistä muutoksista oli datasäädöksen soveltuminen yritysten väliseen datan jakamiseen sekä yritysten välisiin datanjakosopimuksiin. Yleisesti ottaen tällaista yritysten välistä pakottavaa sääntelyä ei ole ollut, sillä sitä ei ole voitu perustella markkinoiden tai sopimuksen toimimattomuudella kuin poikkeustapauksissa.²⁹⁶ On katsottu, että yrityksillä on tarpeeksi tietotaitoa sopimusneuvotteluihin sekä resursseja ymmärtää tämänkaltaisten sopimusten sisältämät oikeudet ja velvoitteet, ja vain harvoin yritykset kohtaavat tilanteen, jossa toinen yritys on selvästi heikommassa asemassa toiseen osapuoleen nähden.²⁹⁷ Nämä kaksi edellä selostettua muutosta, eli pakottavat rajoitukset IoT-laitteiden valmistajien oikeuteen käyttää laitteen

²⁹² Eckardt – Kerber 2024, s.4.

²⁹³ Keller 2025, s.200.

²⁹⁴ Leistner – Antoine 2022, s.344.

²⁹⁵ Butzow ym. 2025, s.89.

²⁹⁶ Leistner – Antoine 2022, s.346.

²⁹⁷ Kerber 2024, s.237.

muodostamaa dataa sekä eli pakottava sääntely yritysten välisiin sopimusehtoihin ovat merkittäviä muutoksia aiempaan oikeustilaan.²⁹⁸

Toisaalta datasäädös asettaa myös rajoituksia datan hyödyntämiselle käyttäjien ja kolmansien osapuolten suuntaan: laitteiden käyttäjät tai kolmannet osapuolet eivät saa hyödyntää dataa kilpailevien laitteiden kehittämiseen, mutta kilpailevan palvelun kehittäminen on sallittua. Kerber on artikkelissaan katsonut tämän antavan laitteiden valmistajille suojaa innovaatiokilpailulta, joskin ilman häntä vakuuttavia perusteluja.²⁹⁹ Toisaalta tämä innovaatiokilpailun rajoittaminen on hieman nurinkurinen säädöksen tavoitteiden kanssa, sillä säädöksen yhtenä päätavoitteena oli edistää kilpailua ja innovaatioita EU:n sisämarkkinoilla. Se, että dataa ei saa hyödyntää kilpailevan laitteen valmistamiseen on herättänyt pohdintaa siitä, voivatko yritykset tosiasiallisesti hyödyntää saamaansa dataa sallittujen palveluiden tarjoamiseen ja kehittämiseen, ja onko yrityksillä säädöksen perusteella pääsy näiden toimintojen kannalta relevanttiin dataan.³⁰⁰

Yhteenvetona voidaan siis todeta, että datasäädöksen soveltaminen aiheuttaa muutoksia datan haltijoiden toimintaan monessa eri näkökulmassa. Ensinnäkin datan haltijoiden tulee tunnistaa, millaista dataa heidän tulee säädöksen velvoitteiden perusteella jakaa, ja sisältääkö jaettava data mahdollisesti liikesalaisuuksiksi luokiteltavaa tietoa, toiseksi yritysten tulee kiinnittää huomiota datan jakamisen teknisiin vaatimuksiin, ja kolmantena datan haltijoiden tulee tehdä muutoksia sopimuskäytäntöihin, sillä sopimuksissa tulee huomioida toisaalta informointivelvollisuus laitteen käyttäjiä kohtaan ja toisaalta datan suojaaminen jakotilanteissa.³⁰¹

7.2 Datan käsitteen määrittely suunnannäyttäjänä

Käsitteiden määrittely erittäin tärkeää, määrittävät sen, miten ymmärrämme asiat ja tässä tapauksessa määrittävät myös sen, mitä säädöksen soveltamispiiriin kuuluu. Kuten tutkielman edetessä on voinut huomata, datasäädös sisältää runsaasti erilaisia uusia käsitteitä ja määritelmiä. Datasäädöksen sisältämät oikeudet ja velvollisuudet rakentuvat näiden säädöksen sisältämien uusien käsitteiden varaan, ja ovat riippuvaisia toisistaan.³⁰² Datan

²⁹⁸ Hynönen – Leino – Butzow 2023, s.474.

²⁹⁹ Kerber 2024, s.239.

³⁰⁰ Kerber 2024, s.238.

³⁰¹ EU:n datasäädös – uudet säännöt datan jakamiselle.

³⁰² Butzow ym. 2025, s.50.

käsite on kaiken perusta ja lähtökohta, sillä se määrittää sen, mitä säädöksen soveltamisalaan kuuluu ja mitä säädöksen jakovelvoitteiden nojalla datan haltijan tulee jakaa. Tämän määrittelyssä varsinkin helposti saatavilla olevan datan, metadatan, raakadatan, esikäsitellyn datan ja johdetun datan käsitteet ovat keskeisiä. Kun säädöksen perusteella jaettava data on selvillä, datan käsitettä sovelletaan muun muassa niissä tilanteissa, kun pohditaan datanjakosopimuksia, datanjakostrategioita, tuotekehittelyä ja mahdollisten liikesalaisuuksien suojaamista.

Datasäädöstä on kritisoitu oikeuskirjallisuudessa, sillä se ei sisällä tarpeeksi selvää määritelmää siitä, mitä on säädöksen soveltamisalaan kuuluva data.³⁰³ Varsinkin datan tekninen määrittely jää ilman taustoitusta ja lisäperusteluja.³⁰⁴ Oikeuskirjallisuudessa on myös esitetty, että datasäädöksen kattama soveltamisala on kapea, sillä säädös rajaa pois datasta johdetut ja päätellyt tiedot sekä ohjelmistoprosesseista peräisin olevat tiedot, jotka laskevat johdettua dataa ohjelmistoprosessin datasta.³⁰⁵

Tutkimuksessa on selvitetty, että datan teknisellä määritelmällä sekä datan käsittelyn teknisellä toteutuksella on merkitystä siihen, miten data määritellään oikeudellisesti datasäädöksessä. Erityisesti datan teknisten ominaisuuksien määrittely vaikuttaa suoraan siihen, millainen vaikutus sillä on datanjakovelvoitteeseen sekä jaettavan datan laajuuteen. Erityisesti kompastuskiveksi muodostuu helposti saatavilla olevan datan kriteeri ”ilman kohtuutonta vaivaa”, raakadatan kriteeri ”data, jota ei olennaisesti muuteta” sekä käsitellyn datan kriteeri ”tieto, joka on tulosta lisäinvestoinneista datanarvojen tai tiedon määrittämiseen”, kun pohditaan datasäädöksen soveltamisalaa ja sen rajaamista.³⁰⁶

Helposti saatavilla olevan datan ja esikäsitellyn datan käsittelyä rajoittavat kriteerit on myös nähty teknisen välttämättömyyden, oikeusvarmuuden ja eturistiriitojen näkökulmasta ongelmallisina.³⁰⁷ Kriteeristöissä on oikeudellista epävarmuutta, sillä prosessit voivat vaihdella monimutkaisuuden, investointien sekä työmäärän laajuuden perusteella paljonkin.³⁰⁸ Kuten on

³⁰³ Kerber 2023, s.11.

³⁰⁴ Kim – Wai 2024, s.140.

³⁰⁵ Kerber 2023, s.11.

³⁰⁶ Kim – Wai 2024, s.154.

³⁰⁷ Kim – Wai 2024, s.141.

³⁰⁸ Kim – Wai 2024, s.149.

jo aiemmin todettu, raakadataa on haastavaa irrottaa kokonaan sen sisältämästä informaatiosta, ja lähes kaikki ymmärrettävissä oleva data on jollakin tavalla käsiteltyä.³⁰⁹

Koska datasäädöksen soveltamisala on niin laaja-alainen, sisältäen sekä henkilötietoja että ei-henkilötietoja sisältävän datan sekä B2C että B2B osapuolten välisen datan jakamisen, on tärkeää, että määritelmässä on joustavuutta, ja tähän pyritään esimerkiksi käyttämällä avoimia standardeja.³¹⁰ Toisaalta liian laaja-alaiset ja joustavat määritelmät johtavat helposti tulkintaongelmiin ja horjuttavat oikeusvarmuutta. Datasäädös on kohtuullisen tuore asetus, ja käsitteiden määritelmät ja soveltamisala tulevat todennäköisesti tarkentumaan oikeuskäytännössä.

7.3 Strategiat, joilla datan jakamista voidaan minimoida

Datasäädöksen soveltamisalaan kuuluvan datan käsitteen määrittelyn jälkeen tutkielmassa selvitettiin erilaisia toimintamalleja, joilla datan haltijat voisivat minimoida datan jakamisen. Näistä toimintamalleista henkilötietostrategia sekä tekninen strategia keskittyivät datan käsittelyyn ja siihen, miten datan käsittelyllä päästäisiin siihen lopputulokseen, ettei tallennettava tai siirrettävä data kuuluisi asetuksen soveltamisalaan. Oikeudellinen strategia taas keskittyy datan jakamisen välttämiseen ja datan sisältämän tiedon suojaamiseen oikeudellisen instrumentin, eli liikesalaisuuden suojan kautta. Datasäädöksen piiriin kuuluvan datan käsitteen määrittelyllä on kuitenkin suuri rooli myös siinä arvioinnissa, miten liikesalaisuuksien suoja soveltuu IoT-laitteiden tuottamaan dataan.

Tekninen strategia perustuu nimensä mukaisesti laitteen tekniseen suunnitteluun. Strategian tarkoituksena on hyödyntää reunalaskentaa, jolloin raakadataa ei siirretä tai tallenneta mihinkään, vaan data käsitellään laitteessa ja tämän jälkeen se tallennetaan laitteeseen tai siirretään palvelimelle.³¹¹ Strategian tavoitteena on, että reunalaskennan avulla käsitelty data ei kuuluisi datasäädöksen soveltamisalaan, jolloin sitä ei tarvitsisi jakaa. Oikeudellisesta näkökulmasta strategian keskiössä on datasäädöksen resitaalikappaleessa 15 määritelty johdetun datan käsite sekä 3 artiklan mukainen suunnitteluvaihtoehto ja 4 artiklan mukainen datanjakovaihtoehto.

³⁰⁹ Kerber 2023, s.12.

³¹⁰ Leistner – Antoine 2022, s. 345.

³¹¹ What is Edge Computing? HPE.

Privacy by design- suunnittelussa keskeistä on henkilötietojen anonymisointi laitteen tuottamaa dataa käsittelemällä. Tällä strategialla on kuitenkin rajansa: ensinnäkin, datan käsittely erilaisin anonymisointi toimenpitein ei välttämättä tee datasta johdettua dataa. Lisäksi EU:n komissio on katsonut, että anonymisointiin käytetyt investoinnit eivät ole sellaisia merkittäviä investointitoimenpiteitä, joiden takia data katsottaisiin johdetuksi dataksi.³¹² Käytännössä tämä tarkoittaa sitä, että anonymisoitu data saattaa silti kuulua datasäädöksen jakamisvelvoitteiden piiriin, mikäli se on käyttäjän toimista syntynyttä laitedataa, ja datan käsittely ei ole vaatinut muita merkittäviä investointeja.

Teknisen strategian hyödyntäminen saa tukea myös komission laatimasta oppaasta. Komissio on todennut, että reunalaskennalla tuotettu data ei ole datasäädöksen jakovelvoitteiden piirissä, mikäli laitteesta saadaan ulos vain johdettua dataa, eikä raakadataa tallenneta tai siirretä laitteen ulkopuolelle missään vaiheessa käsittelyä.³¹³ Näin ollen tällä teknisellä strategialla datan haltijat voivat välttää datan jakamisen, mikäli data käsitellään johdetuksi dataksi suoraan IoT-laitteessa. Toisaalta, jos raakadataa ei missään vaiheessa tallenneta tai siirretä laitteen ulkopuolelle, tällöin myöskään laitteen valmistaja tai datan haltija ei saa laitteen tuottamaa raakadataa. Tällä voi olla merkitystä muun muassa tuotekehityksessä.

Oikeudellisella strategialla yritys pyrkii suojaamaan liikesalaisuuksia sisältävää dataa, ja koska datasäädös ei perussäännön mukaan anna vapautusta liikesalaisuuksia sisältävän datan jakamisesta, tämän strategian perustana on datasäädöksen 5 artiklan 11 kohdan poikkeussäännös ja sen tulkinta. Tämän lisäksi keskiössä on liikesalaisuuden käsitteen kriteeristön soveltaminen jaettavaan dataan, eli sen selvittäminen, voidaanko jaettava data katsoa liikesalaisuudeksi.

Oikeudellisen strategian hyödyntäminen vaatii käsitellyistä kolmesta strategiasta eniten tulkintaa. Ensinnäkin datan haltijan tulee tunnistaa liikesalaisuuksia sisältävä data, ja datan tulee täyttää liikesalaisuuden kriteerit. Tutkielmassa huomattiin, että esimerkiksi raakadataan liikesalaisuuden kriteerit eivät välttämättä sovellu ongelmattomasti. Tämän jälkeen 5 artiklan 11 kohdan mukaisten olosuhteita koskevien vaatimusten tulee täytyä, jotta datan jakamisesta voidaan kieltäytyä. Nämä olosuhteita koskevat vaatimukset, kuten todennäköinen vakava taloudellinen vahinko, ovat tulkinnanvaraisia ja usein tapaus- ja tilannekohtaisia, jolloin voidaan pohtia, mihin soveltamisalan raja vedetään ja vaarantavatko liian laveat kriteerit

³¹² Euroopan komissio 2026, s.12.

³¹³ Euroopan komissio 2026, s.8.

oikeusvarmuuden. Mikäli kolmas osapuoli haluaa riitauttaa datan jakamisen epäämisen, kolmas osapuoli voi saattaa asian toimivaltaisen viranomaisen ratkaistavaksi datasäädöksen 5 artiklan 12a kohdan mukaisesti. Näin ollen sekä liikesalaisuutta sisältävän datan käsite, että vakavan taloudellisen vahingon todennäköisyysaste tulevat tarkentumaan ensinnäkin viranomaisen menettelyssä, että myöhemmin oikeuskäytännössä.