Datan luovutusvelvollisuus ja yleinen tietosuoja-asetus – henkilötietoja sisältävän datan luovuttaminen yrityskäyttäjälle

Lapin yliopisto
Oikeustieteiden tiedekunta
Kauppaoikeus
Pro gradu -tutkielma
Helmi Helotie
Syksy 2022

Lapin yliopisto, oikeustieteiden tiedekunta

Työn nimi: Datan luovutusvelvollisuus ja yleinen tietosuoja-asetus – henkilötietoja sisältävän datan luovuttaminen yrityskäyttäjälle
Tekijä: Helmi Helotie
Koulutusohjelma/oppiaine: Kauppaoikeus
Työn laji: Pro gradu -tutkielma
Sivumäärä, liitteiden lukumäärä: XIII + 69
Vuosi: 2022

Tiivistelmä: Viime vuosikymmenten aikana datan määrä on kasvanut huomattavasti. Datan hallinnointi on kuitenkin rajautunut ainoastaan tiettyjen toimijoiden käsiin. Näillä portinvartijoiksi kutsutuilla toimijoilla on hallussaan keinot muokata ja hyödyntää dataa siten, että siitä tulee arvokasta liiketoiminnalle. Lainsäädännöllä ei ole kyetty riittävän kattavasti puuttumaan dataa hallinnoivien portinvartijoiden toimintaan, eikä niiden pienemmillä kilpailijoilla ole ollut samanlaista pääsyä dataan taikka mahdollisuutta hyödyntää sitä omassa toiminnassaan. Euroopan unionin tasoisen uuden kilpailullisista ja oikeudenmukaisista markkinoista digitaalialalla koskevan asetuksen eli digimarkkinasäädöksen myötä portinvartijat velvoitetaan luovuttamaan niiden hallussaan olevaa dataa kilpailijoina toimiville yrityskäyttäjilleen. Euroopan unionin yleistä tietosuoja-asetusta tulee noudattaa silloin, kun luovutettava data sisältää henkilötietoja.

Tämän lainopillisen tutkielman tavoitteena oli analysoida, miten henkilötietoja voidaan yrityskäyttäjälle luovuttaa ja millaiseksi digimarkkinasäädöksen ja yleisen tietosuoja-asetuksen yhteensopivuus uuden velvollisuuden myötä muodostuu. Tutkielmassa havaittiin, että luovutusvelvollisuuden käytännön toteuttaminen voi yleisen tietosuoja-asetuksen asettamien tiukkojen edellytyksien vuoksi olla haastavaa. Yrityskäyttäjän tulisi luovutusvelvollisuuden myötä saada itselleen datasta se hyöty, jonka portinvartija saa tai ainakin mahdollisuus hyödyntää dataa haluamallaan tavalla. Jos luovutusvelvollisuus ei toteudu täysimääräisesti yleisen tietosuoja-asetuksen sääntelyn vuoksi, ei tavoite dataan pääsystä toteudu. Tutkielman tuloksena havaittiin tähän suuntautuvan tulkinnan olevan mahdollista. Tämä korostaa tulevaisuudessa muodostuvan tulkinnan ja oikeuskäytännön tärkeyttä.

Avainsanat: eurooppaoikeus, henkilötietojen suoja, digimarkkinasäädös, digitaaliset markkinat, datan jakaminen, datan luovutusvelvollisuus

SISÄLLYS

LÄHTEET

KIRJALLISUUS

Aarnio, Aulis, Laintulkinnan teoria. Yleisen oikeustieteen oppikirja. WSOY 1989.

Alén-Savikko Anette – Pitkänen, Olli, Rights and entitlements in information: proprietary perspectives and beyond. Data Protection, privacy and European regulation in the digital age. Helsinki 2016.

Bygrave, Lee A., Core principles of data protection. PrivLawPRpr 9; (2001) 7(9) Privacy Law and Policy Reporter 169, 2001.

Byström, Nomi, The Data Subject and The European Convention on Human Rights: Access to Own Data, s. 209–246.Viestintäoikeus nyt – Viestintäoikeuden vuosikirja 2014.

Geradin, Damien – Bania, Konstantina – Karanikioti, Theano, The interplay between the Digital Markets Act and the General Data Protection Regulation, 29.8.2022.

Van Gorp, Nicolai – de Bilj, Paul – Graef, Inge – Molnar, Gabor – Peeters, Roel – Regeczi, David, Exploring data sharing obligations in the technology sector. Research for the ministry of Economic Affairs and Climate Policy. Rotterdam, 30 November 2020.

Hanninen, Minna – Laine, Elli – Rantala, Kati – Rusi, Mari – Varhela, Markku, Henkilötietojen käsittely, EU-tietosuoja-asetuksen vaatimukset. Vantaa 2017.

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

Kaivola, Tuomas, Datan vapaa liikkuvuus – EU:n sisämarkkinoiden viides perusvapaus. Artikkeleita Eurooppaoikeudesta. Defensor Legis N:o 2/2020, s. 230–242.

Kerber, Wolfgang – Zolna, Karsten K., The German Facebook case: the law and economics of the relationship between competition and data protection law. European Journal of Law and Economics. Accepted 27 January 2022.

Kolehmainen, Antti, Tutkimusongelma ja metodi lainopillisessa työssä, s. 105–134 teoksessa Miettinen, Tarmo (toim.), Oikeustieteellinen opinnäyte – Artikkeleita oikeustieteellisten opinnäytteiden vaatimuksista, metodista ja arvostelusta. Helsinki 2016.

Korpisaari, Päivi, Henkilötietojen ja yksityiselämän suoja vuonna 2018 – katsaus sääntelyyn ja ratkaisukäytäntöön, s. 27–54 teoksessa Korpisaari, Päivi (toim.), Data, viestintä ja sääntely: Viestintäoikeuden vuosikirja 2018. Helsinki 2019.

Korpisaari, Päivi – Pitkänen, Olli – Warma-Lehtinen, Eija, Uusi tietosuojalainsäädäntö. Helsinki 2018.

Lehtioksa, Jere, Big Data as an Essential Facility: The Implications from the Perspective of Competition Law and Data Protection Law. Kilpailuoikeudellinen vuosikirja 2018, s. 111–132.

Lehtioksa, Jere – Ljungman, Jan – Vainio, Sonja, Tieto on valtaa – tietosuojalainsäädännön vastainen henkilötietojen käsittely määräävän markkina-aseman väärinkäyttönä. Defensor Legis N:o 6/2019, s. 865–882.

Mahkonen, Sami, Oikeus yksityisyyteen. Helsinki 1997.

Marini-Balestra, Federico – Tremolada, Riccardo, Digital markets and merger control: balancing big data and privacy against competition law – a comment on the European Commission's Decision in the Microsoft/LinkedIn Merger. European Competition Law Review, Vol. 38(7), 2017, s. 337–345.

Mäenpää, Olli, Julkisuusperiaate. Helsinki 2016.

Neuvonen, Riku, Viestintä- ja informaatio-oikeuden perusteet. Helsinki 2019.

Neuvonen, Riku, Yksityisyyden suoja Suomessa. Helsinki 2014.

Ojanen, Tuomas, EU-oikeuden perusteita. 3., uudistettu painos. Keuruu 2016.

Penttinen, Sirja-Leena – Talus, Kim, Avaimet EU-oikeuteen. Helsinki 2017.

Pitkänen, Olli – Tiilikka, Päivi – Warma, Eija, Henkilötietojen suoja. Helsinki 2013.

Raitio, Juha, Teleologia eurooppaoikeudessa. Oikeus 2005 (34);3, Referee-artikkeli, s. 276–297.

Raitio, Juha, Euroopan Unionin oikeus. Helsinki 2016.

Siltala, Raimo, Oikeustieteen tieteenteoria. Helsinki 2003.

Suomen itsenäisyyden juhlarahasto, Bräutigam, Tobias – Cunningham Francine – Aholainen Maria – Geus Marjolein, Kukorelli Floora – Toivanen Meeri, EU-sääntely rakentaa reilumpaa datataloutta – Euroopan viiden datalainsäädäntöehdotuksen tarjoamat mahdollisuudet yrityksille, yksilöille ja julkiselle sektorille. Helsinki 2022.

Talus, Anu, Tietosuojasääntelyn eurooppalaistuminen – it's an evolution, not a revolution. Artikkeleita Euroopasta – artiklar inom europarätt. Defensor Legis N:o 2/2019, s. 210–220.

Tarkela, Pekka, Digitaalinen talous, data ja varallisuusoikeuden muutostarpeet – Property Law in Flux: How to Deal with Digital Data in Digital Economy. Liikejuridiikka 2/2016, Referee-artikkeli, s. 60–114.

Vapaavuori, Tom, Liikesalaisuudet ja salassapitosopimukset. 3., uudistettu painos. Helsinki 2019.

Voutilainen, Tomi, Oikeus tietoon. Informaatio-oikeuden perusteet. Keuruu 2019.

Warma, Eija – Nieminen, Jussi, Tietosuoja ja kilpailuoikeus – määräävässä markkina-asemassa olevan yrityksen toimitusvelvollisuudesta ja tietosuojalainsäädännöstä. Defensor Legis N:o 4/2016, s. 549–569.

Wasastjerna, Maria, Blurred lines: The German Facebook case and the interlink between competition law and data protection. Kilpailuoikeudellinen vuosikirja 2018, s. 23–34.

VIRALLISLÄHTEET

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

European Data Protection Board Guidelines, Guidelines 05/2020 on consent under Regulation 2016/679. Version 1.1. European Data Protection Board, 4.5.2020.

European Data Protection Supervisor, Opinion 2/2021 on the Proposal for a Digital Markets Act, 10.2.2021.

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

HE 30/2020 vp, Hallituksen esitys Eduskunnalle yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen muuttamisesta tehdyn pöytäkirjan hyväksymiseksi ja voimaansaattamiseksi sekä laeiksi tietosuojalain ja henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annetun lain 1 ja 54 §:n muuttamisesta.

PeVL 38/2016 vp, Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laeiksi pelastuslain ja hätäkeskustoiminnasta annetun lain muuttamisesta.

PeVL 31/2017 vp, Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laiksi valtakunnallisista opinto- ja tukirekistereistä.

PeVL 2/2018 vp, Perustuslakivaliokunnan lausunto hallituksen esityksestä eduskunnalle laiksi liikenteen palveluista annetun lain muuttamiseksi ja eräiksi siihen liittyviksi laeiksi.

Liikenne- ja viestintäministeriö. Päätösperustelut; valtioneuvoston periaatepäätöksen datan hyödyntämisestä liiketoiminnassa – massadatan ja omadatan linjaukset ja toimet.

Valtioneuvoston periaatepäätös datan hyödyntämisestä liiketoiminnassa LVM/2016/45, 6.5.2016.

Valtioneuvoston selvitys- ja tutkimustoiminta, Tietosuojasäädöksen muutostarve – Pitkänen, Olli (toim.). Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisusarja 41/2017. Helsinki 2017.

WP 136, Article 29 Data Protection Working Party 136, Opinion 4/2007 on the concept of personal, Adopted on 20 June 2007.

WP 203, Article 29 Data Protection Working Party 203, Opinion 03/2013 on purpose limitation, Adopted on 2 April 2013.

WP 217, Article 29 Data Protection Working Party 217, Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC, Adopted on 9 April 2014.

WP 242, Article 29 Data Protection Working Party 242 rev.01, Guidelines on the right to data portability; Adopted on 13 December 2016, as last Revised and Adopted on 5 April 2017.

WP 259, Article 29 Data Protection Working Party 259 rev.01, Guidelines on consent under Regulation 2016/679; Adopted on 28 November 2017, as last Revised and Adopted on 10 April 2018.

OIKEUSKÄYTÄNTÖ JA MUUT RATKAISUT

Asia C-252/21 – Meta Platforms and Others

C-252/21 - Meta Platforms and Others (Conditions générales d'utilisation d'un réseau social). Ennakkoratkaisupyyntö, 22.4.2021.

Asia C-238/05 (ECLI:EU:C:2006:734) - Asnef-Equifax

C238/05, Asnef-Equifax, Servicios de Información sobre Solvencia y Crédito, SL vastaan Asociación de Usuarios de Servicios Bancarios (Ausbanc), 23.11.2006. ECLI:EU:C:2006:734.

Euroopan komission päätös 3.10.2014, COMP/M.7217 – Facebook/WhatsApp.

Euroopan komission päätös 6.12.2016, M.8124 – Microsoft/LinkedIn.

MUUT LÄHTEET

Bundeskartellamt. Bundeskartellamt prohibits Facebook from combining user data from different sources, lehdistötiedote 7.2.2019. [https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html]. (9.8.2022).

Centre for Information Policy Leadership, Bridging the DMA and the GDPR – Comments by the centre for Information Policy Leadership on the Data Protection Implications of the Draft Digital Markets Act, 6.12.2021.

Elinkeinoelämän tutkimuslaitos. Alustava lausunto Digital Markets Act -lainsäädäntöaloitteesta, 11.1.2021. [https://www.etla.fi/ajankohtaista/lausunnot/lausunto-digital-markets-act-lainsaadantoaloitteesta/] (2.8.2022).

Euroopan unionin neuvosto. Digimarkkinasäädös: neuvosto hyväksyi lopullisesti uudet säännöt reilusta kilpailusta verkossa, lehdistötiedote 18.7.2022. [https://www.consilium.europa.eu/fi/press/press-releases/2022/07/18/dma-council-gives-final-approval-to-new-rules-for-fair-competition-online/?source=techstories.org] (9.8.2022).

Euroopan komissio. EU:n digimarkkinasäädös varmistaa oikeudenmukaiset ja avoimet digitaalialan markkinat. [https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_fi] (2.11.2022).

Euroopan komissio. Datasäädös: Komissio ehdottaa toimenpiteitä oikeudenmukaisen ja innovatiivisen datatalouden edistämiseksi, lehdistötiedote 23.2.2022. [https://ec.europa.eu/commission/presscorner/detail/fi/ip_22_1113] (2.11.2022).

Eurooppa-neuvosto. Digipalvelupaketti, 26.10.2022. [https://www.consilium.europa.eu/fi/policies/digital-services-package/] (2.11.2022).

Finlex, EU:n uudet digisäädökset, digimarkkinasäädös (DMA) ja digipalvelusäädös (DSA) voimaan marraskuussa 2.11.2022. [https://finlex.fi/fi/uutiset/432/] (2.11.2022).

Information Commissioner's Office, Legal Obligation: Information Commissioner's Office, Guide to the General Data Protection Regulation. Lawful basis for processing. Legal Obligation. [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/] (16.10.2022).

Information Commissioner's Office, Legitimate interests: Information Commissioner's Office, Guide to the General Data Protection Regulation. Lawful basis for processing.

Legitimate interests. [https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/] (16.10.2022).

Joint Research Centre, Duch-Brown, N. – Martins, B. – Muller-Langer, F., JRC Technical reports, JRC Digital Economy Working Paper 2017-01. The economics of ownership, access and trade in digital data. Seville 2017.

Joint Research Centre, Cabral, L. – Haucap, J. – Parker, G. – Petropoulos, G. – Valletti, T. – Van Alstyne, M., The EU Digital Markets Act – A Report from a Panel of Economic Experts. Luxembourg 2021.

Kilpailu- ja kuluttajavirasto. Kilpailun ja kuluttajansuojan kysymyksiä datataloudessa. Kilpailu- ja kuluttajaviraston selvityksiä 1/2019.

Koenigswarter, Nathan Bigaud, Big data is hard to anonymize; here is what it means for development, 13.11.2019. [Big data is hard to anonymize; here is what it means for development. | by Nathan Bigaud Koenigswarter | The Startup | Medium] (5.8.2022)

Oberlandesgericht Düsseldorf. Facebook gegen Bundeskartellamt: Ergebnisse des Verhandlungstermins, 24.3.2021, Pressemitteilung Nr. 9/2021. [Oberlandesgericht Düsseldorf: Facebook gegen Bundeskartellamt: Ergebnisse des Verhandlungstermins (nrw.de)] (9.8.2022).

Organisation for Economic Co-operation and Development, DAF/COMP(2016)14; Big Data: Bringing Competition Policy to the Digital era – Background note by the Secretariat 29-30 November 2016.

Tietosuojavaltuutetun toimisto. Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille. Rekisteröidyn informointi. [https://tietosuoja.fi/rekisteroidyn-informointi] (26.7.2022).

Tietosuojavaltuutetun toimisto. Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille. Rekisterinpitäjän oikeutettu etu. [https://tietosuoja.fi/rekisterinpitajan-oikeutettu-etu] (22.10.2022).

Työ- ja elinkeinoministeriö. EU:n digimarkkinasäädöksestä alustava sopu, 28.3.2022. [https://tem.fi/-/eu-n-digimarkkinasaadoksesta-alustava-sopu] (9.8.2022).

Wiewiórowski, Wojciech, Sharing is caring? That depends…. European Data Protection Supervisor, Blog, 13.12.2019. [https://edps.europa.eu/press-publications/press-news/blog/sharing-caring-depends_en] (16.10.2022).

Yleisradio. Nettimainonta alaikäisille kieltoon, sääntöjen rikkomisesta miljardisakot – näin etenee EU:n historiallinen yritys suitsia digijättejä, 15.12.2021. [https://yle.fi/uutiset/3-12229936] (9.11.2022).

Zerdick, Thomas, Pseudonymous data: processing personal data while mitigating risks. European Data Protection Supervisor, Blog, 12.12.2021. [https://edps.europa.eu/press-publications/press-news/blog/pseudonymous-data-processing-personal-data-while-mitigating_en] (30.10.2022).

LYHENTEET

CIPL	Centre for Information Policy Leadership
DA	Data Act, Proposal for a Regulation on harmonised rules on fair access to and use of data (datasäädös)
DMA	Regulation (EU) 2022/1925 of the European Parliament and of the Council on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act, digimarkkinasäädös)
DSA	Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act, datapalvelusäädös)
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EIS	yleissopimus ihmisoikeuksien ja perusvapauksien suojaamiseksi SopS 18–19/1990 (Euroopan ihmisoikeussopimus)
ETLA	elinkeinoelämän tutkimuslaitos
EU	Euroopan unioni
EUT	Euroopan unionin tuomioistuin
HE	hallituksen esitys
ICO	Information Commissioner's Office
JRC	Joint Research Centre
KKV	kilpailu- ja kuluttajavirasto
OECD	Organisation for Economic Co-operation and Development
PeVL	perustuslakivaliokunta
PL	Suomen perustuslaki 731/1999
SEUT	Euroopan unionin toiminnasta tehty sopimus
Sitra	Suomen itsenäisyyden juhlarahasto
TEM	työ- ja elinkeinoministeriö
TSA	Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä

	näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus)
YLE	yleisradio

1 JOHDANTO

1.1 Tausta ja johdatus aiheeseen

Kysymys suurien teknologiayhtiöiden taloudellisesta asemasta on viime vuosikymmenien aikana herättänyt keskustelua laajasti. Aihetta on käsitelty globaalisti erityisesti digitaalisia markkinoita hallitsevien teknologiayhtiöiden kilpailullisen aseman osalta. Teknologiayhtiöiden liiketoimintamalli sisältää uudenlaisen toimintatavan, jossa yhdistyy digitaalisen datan hyödyntäminen yhtiön taloudellisena perustana. Datan hyödyntämiseen liittyy useita eri kysymyksiä alkaen aina datan itsensä käsitteestä ja ominaispiirteistä datan käsittelyn oikeudelliseen asemaan, kilpailulliseen näkökulmaan ja tietosuojaan. Tämä kaikki on laajentanut asian käsittelyä yhdeltä oikeudenalalta toiselle, jolloin oikeudenalojen rajapinnat ovat hälventyneet.

Teknologiayhtiöiden liiketoimintamallin perustana oleva digitaalinen data koostuu pitkälti näiden yhtiöiden tuottamien palveluiden käyttäjiltä kerätyistä tiedoista. Tiedot voivat olla lähtöisin niin yritys- kuin yksityiskäyttäjiltäkin. Yksityisiltä käyttäjiltä kerättyjen henkilötietojen merkitys teknologian kehittyessä on johtanut asetelmaan, jossa yritykset kerryttävät taloudellista hyötyä henkilötietojen erilaisella käsittelyllä ja sitä kautta henkilötietojen arvon jalostamisella, kun taas yksityisille henkilöille omien henkilötietojen luovutus on tällä hetkellä lähinnä ainoastaan se vastike, jolla taataan pääsy yritysten tarjoamiin palveluihin. Yksityisille henkilöille omat henkilötiedot eivät edusta samaa arvoa, minkä yritykset niistä omassa käytössään saavat.[1]

Datan hyödyntämisen lisäksi yhtiöiden toiminta on lähes poikkeuksettomasti globaalia. Sääntelyn haasteina on asettaa maailmanlaajuisesti toimiva viitekehys sille, miten toimintaa voidaan harjoittaa innovoivasti ja kehitystä turvaavasti, mutta myös voimassa olevan sääntelyn, kuten kilpailu- ja tietosuojalainsäädännön, edellytysten mukaisesti. Teknologiayhtiöt ovat saavuttaneet datan keräämisen ja käytön avulla markkinoilla vankkumattoman aseman, jossa alan suurimmilla yhtiöillä on hallinnassaan suuri määrä arvokasta dataa, johon erityisesti muilla pienemmillä kilpailijoilla ei ole samanlaista pääsyä.

[1] Lehtioksa – Ljungman – Vainio 2019, s. 865.

Datatalouden keskittyessä maantieteellisesti lähinnä Yhdysvaltojen ja Kiinan alueelle, on Euroopan unionissa (EU) ryhdytty kehittämään uusia keinoja eurooppalaisen datatalouden kehittämiseksi. Helmikuussa vuonna 2020 julkaistu Euroopan datastrategia on nostanut esiin kilpailullisia ongelmia liittyen muun muassa datan yhteiskäyttöön ja yhteentoimivuuteen yritysten välillä.[2] Datastrategiasta johdettuna markkinavoiman epätasapainoon on pyritty reagoimaan Euroopan unionin uudella digimarkkinasäädöksellä (*Digital Markets Act, DMA*)[3], jossa yhtenä sääntelykeinona asetetaan teknologiayhtiöille velvollisuus luovuttaa hallussaan olevaa dataa kilpailijoilleen tietyin edellytyksin. Tätä nimenomaista velvollisuutta voidaan lähestyä kilpailuoikeudellisen näkökulman lisäksi tietosuojaoikeudelliselta kannalta, jolloin aihepiirin keskiössä on sääntelyn yhteensopivuus etenkin unionin tietosuojaoikeudellisesti keskeisimmän säädöksen eli yleisen tietosuoja-asetuksen (*tietosuoja-asetus, TSA*)[4] kanssa.

Se, mikä muuttuu ja mikä suurten teknologiayhtiöiden asemaan liittyvässä keskustelussa on uutta, tulee näkymään voimassa olevan oikeuden muuttumisena uuden sääntelyn myötä. Tämänhetkiset – mutta toisaalta pitkään jatkuneet – teknologiayhtiöiden liiketoimintamallit ja -tavat ovat väistämättä muutoksen edessä.

Teknologiayhtiöihin liittyvien kilpailullisten ongelmien lisäksi myös datan jakamista ja erityisesti datan luovuttamista koskeva keskustelu nousi uudella tavalla esille, kun Euroopan komissio julkaisi Euroopan datastrategian. Digimarkkinasäädös on vain yksi osa tätä datastrategiaa, joka sisältää tällä hetkellä viisi uutta lainsäädäntöehdotusta[5]. Digimarkkinasäädös on tullut voimaan 1.11.2022. Säädös sisältää puolen vuoden siirtymäajan, jolloin sen soveltamisen on määrä alkaa 2.5.2023.[6]

---

[2] Euroopan komissio, Euroopan datastrategia 2020, s. 6–8.
[3] Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925 kilpailullisista ja oikeudenmukaisista markkinoista digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (digimarkkinasäädös).
[4] Euroopan parlamentin ja neuvoston asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus, TSA, GDPR).
[5] Datastrategian julkistamisen jälkeen uusia lainsäädäntöehdotuksia on julkaistu mainitun digimarkkinasäädöksen lisäksi neljä kappaletta: asetus eurooppalaisesta datahallinnosta (datahallintoasetus, DGA, voimaan 23.6.2022), asetus tekoälyä koskevista yhdenmukaistetuista säännöistä (tekoälysäännös, AIA, ehdotus julkaistiin 21.4.2021), asetus digitaalisten palvelujen sisämarkkinoista (digipalvelusäädös, DSA, voimaan 16.11.2022) ja asetus datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös, DA, ehdotus julkaistiin 23.2.2022).
[6] Finlex 2022.

Digimarkkinasäädöksellä on vahva kilpailuoikeudellinen tarkoitus ja sillä pyritäänkin puuttumaan suurten digitaalisten alustapalvelujen tarjoajien toimintaan. Näitä alustapalveluiden tarjoajia nimitetään asetuksessa *portinvartijoiksi*. Portinvartijoiksi luokiteltavilla yrityksillä on suuri vaikutus digitaalimarkkinoihin ja merkittävä määräysvalta markkinoille pääsyn suhteen sekä ylipäätään vakiintunut asema markkinoilla.[7] Digimarkkinasäädös on rajattu nimenomaan niihin portinvartijayrityksiin, joiden suhteen on havaittu ongelmia hyvän kauppatavan mukaisissa käytännöissä sekä kilpailullisuudessa. Näihin havaittuihin ongelmiin ei kuitenkaan aiemmin ole kyetty riittävän tehokkaasti puuttumaan.[8] Asetus itsessään täydentää voimassa olevia EU-oikeudellisia ja kansallisia kilpailusääntöjä sekä tietosuojalainsäädäntöä.[9] Digimarkkinasäädöksen soveltamisen alkaminen käynnistää Euroopan komission portinvartijoiden nimeämisprosessin, jota varten ydinalustapalveluja tarjoavien yritysten tulee tehdä komissiolle ilmoitus. Kun komissio on nimittänyt portinvartijat, niillä on edelleen kuusi kuukautta aikaa varmistaa digimarkkinasäädöksessä asetettujen velvoitteiden noudattaminen.[10]

1.2 Tutkimuskysymys ja aiheen rajaus

Tutkielmassa käsitellään teknologiayhtiöille asetettavan datan luovutusvelvollisuuden ja tietosuojan välistä suhdetta erityisesti henkilötietojen jakamisen näkökulmasta. Tarkastelussa kiinnitetään huomiota nykyisen voimassa olevan lainsäädännön lisäksi myös tulevaisuuteen niiltä osin, kun digimarkkinasäädöksen soveltaminen ei vielä tutkielman kirjoitusvaiheessa ole alkanut.

Tutkielmassa tutkimuskysymyksenä on se, miten tietosuoja-asetus tulee vaikuttamaan henkilötietojen luovuttamiseen digimarkkinasäädöksen mahdollistamana velvollisuutena yrityskäyttäjää kohtaan, kun toiminnassa noudatetaan yhtäaikaisesti tietosuoja-asetuksen ja digimarkkinasäädöksen sääntelyjä, ja mitä haasteita päällekkäisten sääntelyjen soveltamisesta voi muodostua dataa luovuttavan sekä sitä vastaanottavan yrityksen näkökulmasta.

---

[7] Ks. käsitteen ”portinvartija” määrittelystä lisää kohdassa 1.4, s. 9–10.
[8] DMA:n johdanto 5 kohta.
[9] Ks. esim. DMA:n johdanto kohdat 10, 11 ja 12.
[10] Euroopan komissio, EU:n digimarkkinasäädös varmistaa oikeudenmukaiset ja avoimet digitaalialan markkinat.

Datan luovutusvelvollisuutta lähestytään tutkielmassa yritysten välisenä toimintana, joka sisältää portinvartijayrityksen velvollisuuden myöntää kilpailijoinaan toimiville yrityskäyttäjilleen pääsyn kontrolloimaansa dataan. Kyseessä on siten DMA:n mukaan luovutustoimi, jolla myönnetään pääsy portinvartijan hallinnoimiin tietoihin, mukaan lukien henkilötietoihin. Jo alkuun on todettava, että luovutusvelvollisuus terminä ei suoranaisesti esiinny suomenkielisessä digimarkkinasäädöksen käännöksessä. Digimarkkinasäädöksessä velvollisuudet on suomeksi kuvattu siten, että portinvartijan on tarjottava ”– – *pääsy ja käyttömahdollisuus* – –” tietoihin.[11] Henkilötietoihin liittyen digimarkkinasäädöksessä on käännetty tietosuoja-asetuksen mukaisesti suostumuksen antaminen ”– – *tällaiseen tietojen jakamiseen* – –”.[12] Kyseessä on niin ikään tietojen luovuttaminen toisen toimijan käyttöön tarjoamalla tälle maksuton pääsy tietoihin. Tietojen luovuttaminen ja luovuttamisvelvollisuus kuvastaa säädöksen tuomaa kokonaisuutta tietojen jakamisen ja tietoihin myönnettävän pääsyn ja käyttömahdollisuuden osalta, minkä vuoksi myös tässä tutkielmassa on terminologiseksi lähtökohdaksi otettu tietojen ”*luovuttaminen*” ja ”*luovutusvelvollisuus*”.[13]

Tutkielmassa lähestytään tutkimuskysymystä alkuun datan määritelmällä, jolloin käsitellään datan ominaispiirteiden vaikutusta datan sääntelyyn. Tarkoituksena on lähestyä tutkimuskysymystä siitä näkökulmasta, miten datan oikeudellinen asema tämänhetkisen Euroopan unionin sääntelyn ja osittain Suomen kansallisen lainsäädännön perusteella muodostuu. Tältä osin on tavoitteena tuoda esille niitä tekijöitä, jotka säännösten taustalla ovat vaikuttaneet, ja miten datan luonne ja rooli vaikuttavat myös lainsäädännön nyt käsillä oleviin uusiin muutoksiin.

Digimarkkinasäädös tulee vaikuttamaan voimassa olevan tietosuojalainsäädännön tulkintoihin uudemman kerran. Datan luovuttaminen on mahdollista vain silloin, kun se täyttää yleisen tietosuoja-asetuksen asettamat vaatimukset henkilötietojen keräämiselle ja käytölle. Lähtökohtana on ajatus siitä, että henkilötietojen suoja on osa yksityisyyden suojaa, jota arvioidaan suhteessa kilpailuoikeudellisesti merkittävässä asemassa olevan yrityksen hallinnoimaan dataan. Tietosuojalainsäädännön tarkastelussa keskitytään henkilötietoja

[11] DMA 6(10) artikla. Ks. myös kyseisen artiklan englanninkielinen versio ”– – *provide access and use* – –”.
[12] DMA 6(10) artikla. Ks. myös kyseisen artiklan englanninkielinen versio, jossa tietojen jakaminen on käännetty termistä ”*sharing*”.
[13] Tietojen luovuttamista käytetään myös tietosuojalaissa sekä sitä koskevassa hallituksen esityksessä HE 30/2020 vp. Ks. myös kansallinen uutisointi esim. Etla 2021, jossa DMA-ehdotuksen sisältämää datan avaamista ja jakamista koskevia velvoitteita on kuvattu tietojen luovuttamisena ja luovutusvelvollisuutena.

koskevan tietosuoja-asetuksen sääntelyn läheisempään arviointiin huomioiden etenkin henkilötietojen käsittelyä ja siirrettävyyttä koskevat edellytykset.

Digimarkkinasäädöksen datan luovuttamista tarkastellaan erityisesti säädöksen 6(10) artiklan velvollisuuden edellytyksien mukaisesti. DMA asettaa 6(10) artiklassa oikeusperusteeksi henkilötietojen luovuttamiselle rekisteröidyltä saatavan suostumuksen, joka nousee tutkielmassa keskeiseen osaan niin dataa luovuttavan portinvartijan kuin dataa vastaanottavan yrityskäyttäjän kannalta. Siten tutkielmassa keskitytään henkilötietojen käsittelyperusteiden osalta erityisesti siihen, miten tietosuoja-asetuksen mukainen suostumus ja sille asetetut edellytykset sopivat yhteen digimarkkinasäädöksen edellyttämän henkilötietoja sisältävien tietojen luovuttamisen kanssa. Aiheuttaako luovutusvelvoite kuitenkin ongelmia tietosuojan ja tietojen siirrettävyyden kannalta tai voiko tietosuojasääntely aiheuttaa lopulta jopa esteen datan luovuttamiselle? Käsittelyperusteiden lisäksi analysoidaan tietosuoja-asetuksen periaatteita sekä DMA:n uusia edellytyksiä luovutuksen toteuttamiselle.

Teknologiayhtiöiden asemaa on jo lähtökohtaisesti pidetty pidemmän aikaa ongelmallisena lähinnä palveluiden käyttäjien tietosuojan sekä toisaalta kilpailun näkökulmasta. Tietosuoja ja kilpailuoikeus osa-alueina ovat painautuneet tiiviimmin yhteen niin, että tietosuojaan liittyviä kysymyksiä on voitu arvioida kilpailuoikeudellisesta näkökulmasta ja toisinpäin. Tietosuojan ja kilpailuoikeudellisten kysymysten välillä tutkielman pääpaino on datan luovutusvelvollisuuden tietosuojassa ja henkilötietojen suojaa koskevissa kysymyksissä. Tutkielmassa ei siis keskitytä datan luovuttamiseen varsinaisena kilpailuoikeudellisena toimenpiteenä, mutta kilpailullisen sääntelyn toimivuuden ollessa käytännössä digimarkkinasäädöksen tavoitteena, tulee sen yhteyttä tietosuojaan käsiteltyä tutkielmassa pintapuolisesti kokonaiskuvan saamiseksi.

1.3 Tutkimusmenetelmät ja lähdeaineisto

Tutkielma perustuu tutkimusmetodiltaan oikeusdogmatiikkaan eli lainoppiin. Lainopillista tutkimusta on kuvattu oikeustieteen perinteiseksi ydinalueeksi, jonka kohteena on voimassaoleva oikeus. *Hirvosen* mukaan lainoppi siis tutkii voimassaolevaa oikeutta ja sitä, mikä merkitys lailla ja muilla oikeuslähteillä sekä niistä löytyvällä aineistolla on.[14]

[14] Hirvonen 2011, s. 22–23.

Lainoppi voidaan erotella perinteisesti käytännölliseksi ja teoreettiseksi lainopiksi, jossa ensiksi mainittu kuvastaa tehtävää tulkintaa. Siihen sisältyy ensisijaisesti myös oikeusperiaatteiden punninta ja tasapainottaminen. Teoreettisen lainopin lähtökohtana taas on oikeusperiaatteiden systematisointi, jossa keskeisintä on tutkia ja jäsentää esimerkiksi oikeudenalaan kuuluvaa käsitteistöä ja oikeusperiaatteita.[15]

Tämän tutkielman lähtökohtana on käytännöllisen sekä teoreettisen lainopin näkökulmaan kuuluvan voimassaolevan oikeudentilan tutkiminen tukeutuen niin tulkintaan, punnintaan kuin systematisointiinkin liittyviin kannanottoihin.[16] Esimerkiksi datan luovutusvelvollisuuden määrittely sisältää tarpeen systematisoida datan käsitettä itsessään. Tarkoituksena on kokonaisuudessaan tulkita ja systematisoida tietosuojan ja datan sääntelyn juridiikkaan kohdistuvia säännöksiä sekä taustalla vaikuttavia oikeusperiaatteita. Tulkinnassa nojaudutaan myös EU-oikeuden lähtökohtana olevaan sanamuodon mukaiseen tulkintaan.[17] Koska EU:ssa on yli 20 virallista kieltä ja lisäksi EU:ssa käytetään osittain kansallista oikeusjärjestyksistä poikkeavaa kieltä, on sanamuodon mukaisessa tulkinnassa käytetty tutkielmassa lähtökohtaisesti säädösten englannin- sekä suomenkielistä versiota.[18] Digimarkkinasäädöksen ja tietosuoja-asetuksen yhteensopivuuden analysointiin nähden pelkkä sanamuodon mukainen tulkinta ei kuitenkaan anna jokaisessa tilanteessa täysin selvää vastausta, minkä vuoksi tutkielmassa tukeudutaan myös systemaattiseen ja teleologiseen tulkintaan, jotka ovatkin korostuneet nimenomaan EU-oikeuden tutkintaperiaatteina.[19]

Lainopissa lähtökohtana on mainittujen menetelmien lisäksi oikeuslähdeoppi, jossa on kyse oikeusperiaatteiden punninnan metodista, joka asettaa etusijajärjestykseen huomioitavat oikeusperiaatteet.[20] *Aarnion* oikeuslähdeopin mukaan oikeuslähteet jaotellaan etusijajärjestykseen niiden velvoitettavuuden mukaan. Oikeuslähteet ovat sen perusteella jaettu vahvasti velvoitettaviin, heikosti velvoitettaviin ja sallittuihin oikeuslähteisiin.[21] Tutkielma keskittyy EU-oikeudelliseen näkökulmaan ja siinä nojaudutaan pääsääntöisesti vahvasti velvoittavien oikeuslähteiden osalta tutkielman tavoitteiden mukaisesti Euroopan unionin yleiseen

[15] Hirvonen 2011, s. 25.
[16] Ks. Kolehmainen 2016, s. 2.
[17] Penttinen – Talus 2017, s. 28.
[18] Penttinen – Talus 2017, s. 28 ja 30.
[19] Ks. EU-oikeuden tulkintaperiaatteista esim. Ojanen 2016, s. 51–52 ja Raitio 2005, s. 276–277.
[20] Hirvonen 2011, s. 44.
[21] Aarnio 1989, s. 220–221.

tietosuoja-asetukseen sekä digimarkkinasäädökseen, joka myös tulee olemaan asetuksen tasoinen suoraan jäsenvaltioita velvoittava säädös.[22]

Tutkielman aihealue on pitkälti eurooppaoikeudellinen, mistä johtuen ainoastaan kotimaisen sääntelyn ja oikeuskäytännön sijaan on keskitytty pääsääntöisesti eurooppalaiseen sääntelyyn. Niin ikään kotimaista oikeuskäytäntöä aiheeseen liittyen on vain vähäisissä määrin olemassa, ja sen vuoksi käsiteltäväksi tulevat tarpeelliseksi katsotut tutkimusaiheeseen liittyvät ulkomaalaiset tuomioistuinten ratkaisut. Aihealueen ollessa digimarkkinasäädöksen osalta kuitenkin uusi, ei varsinaista digimarkkinasäädökseen liittyvää oikeuskäytäntöä liioin ole. Esille tuodut kilpailuoikeudelliset ratkaisut perustuvatkin tietosuojaoikeudellisten kysymysten huomiointiin ratkaisun perusteluina. Nimenomaisen oikeusvertailun sijaan tarkoituksena on eurooppalaisen oikeusjärjestyksen huomioiminen osana jäsenmaissa kansallisesti sekä yleisesti kansainvälisesti vaikuttavaa sääntelyä. Aihealue jää siten pääosin eurooppaoikeudelliseksi, mutta huomioi näkökulmana suurpiirteisesti myös kansainvälisen oikeuden.

1.4 Keskeiset käsitteet

Datalla tarkoitetaan tutkielmassa digitaalista dataa, joka on digitaalisessa muodossa olevaa tietoaineista. Datan käsitteessä olennaista on se, että kyse on sähköisessä muodossa olevasta tiedosta, joka voi olla ihmis- ja koneluettavissa.[23] Data toistuu tutkielmassa keskeisenä terminä, joka käsitteellisesti saa hyvinkin laajan merkityksen. Tietoa itsessään voidaan pitää ominaisuudeltaan muuttujana, joka ohjaa aina sillä hetkellä kyseeseen tulevaa toimintaa lainsäädännön asettamissa rajoissa.[24]

Data voi sisältää henkilötietoja tai olla itsessään jo luokiteltavissa henkilötiedoksi. *Henkilötietojen* määrittelyssä nojaudutaan koko tutkielman osalta yhdessä keskeisimmässä sääntelyssä, yleisessä tietosuoja-asetuksessa, avattuun käsitteen tarkempaan määrittelyyn. Yleisen tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan henkilötiedoilla tarkoitetaan kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti

[22] Ks. Penttinen – Talus 2017, s. 18.
[23] Ks. Datan käsitteen määrittelystä esimerkiksi Kaivola 2020, s. 232, Tarkela 2016, s. 62.
[24] Voutilainen 2019, s. 21.

tunnistaa erityisesti tunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen tekijän perusteella. Tunnistetietoina voidaan pitää nimeä, henkilötunnusta, sijaintitietoa tai verkkotunnistetietoja. Tunnusomaisia tekijöitä taas on fyysiset, fysiologiset, geneettiset, psyykkiset, taloudelliset, kulttuurilliset tai sosiaaliset tekijät. *Muut kuin henkilötiedot* ovat tietoja, joihin ei kuulu yleisen tietosuoja-asetuksen 4 artiklan 1 kohdassa määriteltyihin luonnolliseen henkilöön liittyviä tunnistettavia tietoja.

Henkilötietojen käsittelyllä tarkoitetaan yleisen tietosuoja-asetuksen 4 artiklan 2 kohdan mukaan toimintoa tai toimintoja, joita kohdistetaan henkilötietoihin tai henkilötietoja sisältäviin tietojoukkoihin käyttäen joko automaattista tai manuaalista tietojenkäsittelyä. Artiklan mukaan tällaista tietojenkäsittelyä on muun muassa tietojen kerääminen, tallentaminen, järjestäminen, jäsentäminen, säilyttäminen, muokkaaminen tai muuttaminen, haku, kysely, käyttö, tietojen luovuttaminen eri keinoin kuten siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista. Käsitteistö on hyvin laaja ja kattaa piiriinsä pitkälti toisistaan erilaisia toimintoja.

Rekisterinpitäjä voi olla yleisen tietosuoja-asetuksen 4 artiklan 7 kohdan mukaan luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot: jos tällaisen käsittelyn tarkoitukset ja keinot määritellään unionin tai jäsenvaltioiden lainsäädännössä, rekisterinpitäjä tai tämän nimittämistä koskevat erityiset kriteerit voidaan vahvistaa näiden mainittujen unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti. Rekisterinpitäjä siis määrittelee käsiteltävät henkilötiedot ja niiden käsittelytavan. Rekisterinpitäjä tulee erottaa *henkilötietojen käsittelijästä*, joka käsittelee henkilötietoja rekisterinpitäjän lukuun. Rekisterinpitäjä voi hankkia itselleen henkilötietojen käsittelijän esimerkiksi alihankintana tai erillisellä sopimuksella.[25]

Henkilötietoihin kytkeytyy läheisesti myös *tietosuojan* käsite. Yleisesti tietosuojasta puhuttaessa onkin tässä tutkielmassa kysymys ennen kaikkea siitä, miten ja missä tilanteessa oikeus käsitellä henkilötietoja muodostuu. Näiden lisäksi tietosuojasääntely pyrkii vastaamaan myös kysymyksiin kenellä ja milloin kyseinen oikeus on.[26] On kuitenkin

[25] Neuvonen 2019, s. 234.
[26] Voutilainen 2019, s. 29.

huomioitava, että tietosuoja ei käsitteenä suoraan vastaa ainoastaan henkilötietojen käsitettä, vaan se voidaan huomioida laajempana suojana koskien myös esimerkiksi yrityksen hallinnoimaa tietoa yrityksestä itsestään.[27] Tietosuojaa voidaan siis tulkita sisällöltään myös henkilötietoja laajemmaksi, jolloin suoja ulottuu myös muihin tietoihin. Tarkka määrittely ei kuitenkaan tässä vaiheessa ole tutkielman näkökulmasta tarkoituksenmukaista, sillä vaikka tietosuojan arvioitaisiin laajan tulkinnan mukaisesti kattavan henkilötietojen lisäksi myös muut tiedot, on yleinen tietosuoja-asetus rajautunut koskemaan vain henkilötietoja. Tästä syystä tutkielmassa yleisesti *tietosuojalla*, *tietosuojaoikeudella* ja *tietosuojasääntelyllä* viitataan pääsääntöisesti henkilötietojen suojaan, ellei toisin mainita.

Tietoturvallisuus on ymmärrettävissä informaatio-oikeudellisesti sekä periaatteena että käsitteenä, mikä tekee siitä kokonaisuudessaan vaikeasti hallittavan. Periaatteena tietoturvallisuus ilmenee, kun sen sisältämän tiedon luottamuksellisuutta, käyttökelpoisuutta ja käytettävyyttä turvataan lainsäädännöllisin keinoin. Tietoturvalla suojataan myös käytännön tasolla henkilötietoja, tekijänoikeuksia, asiakirjoja ja viestintää. Tietoturvallisuus varmistaa, että rekisteröidyllä on oikeus luottaa, että hänen henkilötietojaan käsitellään lainmukaisesti. Tietoturvallisuus on käänteiseltä puoleltaan myös velvollisuus, joka esimerkiksi asettaa rekisterinpitäjälle velvollisuuden huolehtia, että henkilötietoja käsitellään lainmukaisesti.[28] Tietoturvallisuudessa on siis kyse erilaisista keinoista ja järjestelyistä, joilla tiedon turvallisuutta, luottamuksellisuuta ja eheyttä pyritään turvaamaan.

Tutkielmassa keskeisessä osassa olevalla *portinvartijalla* sekä *portinvartijayrityksellä* tarkoitetaan ydinalustapalveluita tarjoavia ja ylläpitäviä suuria teknologiayhtiöitä. Uuden sääntelyn kohteena olevat portinvartijat erotetaan muista palveluntarjoajista digimarkkinasäädöksessä sellaisiin ydinalustapalveluihin, joissa havaitut kilpailuoikeudelliset ongelmat ja hyvän kauppatavan vastaiset käytännöt ovat ilmeisimpiä ja näkyvimpiä. Ydinalustapalvelujen tarjoajista kilpailullisesti ongelmallisiin yhtiöihin luetaan ehdotuksen mukaan ne yhtiöt, joilla on merkittävä vaikutus sisämarkkinoihin ja ne ylläpitävät yhtä tai useampaa tärkeää palveluväylää asiakkaille sekä niillä on tai niillä ennakoidaan olevan vakiintunut ja

[27] Neuvosen mukaan tietosuojan ja henkilötietojen suojan käyttö synonyymeina on siinä mielessä virheellinen, että tietosuojan oikeuspiiriin katsotaan usein kuuluvan yksilön lisäksi myös yritysten hallinnoima tieto tai niitä koskeva tieto. Tietosuojan määrittelyssä voidaan katsoa tietosuojan alaisuuteen kuuluvan myös liikesalaisuuksiksi katsottavat tiedot, jotka eivät välttämättä sisällä henkilötietoja eikä niiden ensisijainen peruste suojaamiselle ole henkilötietojen suojaaminen. Liikesalaisuuksista säädetään kuitenkin erikseen, eivätkä ne kuulu tietosuoja-asetuksen soveltamisalaan. Ks. Neuvonen 2014, s. 64.
[28] Voutilainen 2019, s. 36.

kestävä asema toiminnassaan.[29] Portinvartijan edellytykset täyttävistä yhtiöistä ei digimarkkinasäädöksessä ole mainittu konkreettisia esimerkkejä.[30]

Loppukäyttäjällä tarkoitetaan digimarkkinasäädöksessä luonnollista henkilöä tai oikeushenkilöä, joka käyttää ydinalustapalveluja muutoin kuin yrityskäyttäjänä.[31] *Yrityskäyttäjällä* taas tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, joka kaupallisessa tai ammatillisessa ominaisuudessa käyttää ydinalustapalveluja tavaroiden tai palvelujen tarjoamiseksi loppukäyttäjille tai tällaisen tarjoamisen aikana.[32]

[29] DMA 3(1) artikla ja DMA:n johdanto 15 kohta. Portinvartijan katsotaan täyttävän mainitut vaatimukset DMA 3(2) artiklan mukaan muun muassa silloin, kun portinvartijalla on vähintään 7,5 miljardin euron vuotuinen liikevaihto unionissa tai vähintään 75 miljardin euron keskimääräinen pörssiarvo tai vastaava käypä markkina-arvo, se tarjoaa ydinalustapalveluita vähintään kolmessa jäsenvaltiossa sekä sillä on vähintään 45 miljoonaa loppukäyttäjää unionissa.

[30] Suuriin teknologiayhtiöihin luetaan yleisesti tällä hetkellä niin kutsutut Big Tech -yhtiöt, joihin kuuluvat Google (Alphabet), Apple, Amazon, Facebook (Meta) ja Microsoft, ks. esim. JRC 2021, s. 9. DMA:n ehdotuksen aikana portinvartijoiksi on arvioitu kuuluvan myös mm. matkavarausalusta Booking.com ja verkkovaatekauppa Zalando, ks. Yle 2021. Euroopan komissio tekee kuitenkin lopullisen päätöksen siitä, mitkä yhtiöt luokitellaan portinvartijoiksi (DMA 3(4) artikla).

[31] DMA 2(20) artikla.

[32] DMA 2(21) artikla.

2 DATA JA DATATALOUS

2.1 Digitaalisen datan kehitys

Datan käsite tulee vastaan määriteltäessä niitä tietoja, jotka voivat olla lainsäädännön puitteissa luovutettavissa. Datalle annettu merkitys ja datan rooli määrittelevät sen, mitä ja miten tiettyä sääntelyä voidaan tapauskohtaisesti soveltaa ja miten tietojen luovuttamiseen lainsäädännössä suhtaudutaan. Datalla viitataan tässä tutkielmassa yksinkertaistettuna sähköisessä muodossa olevaan tietoon ja tietoainekseen, joka voi sen tarkempi sisältö, luonne ja alkuperä huomioiden olla varallisuusoikeudelliselta merkitykseltään pitkälti mitä tahansa.[33]

Tarkoituksena on lähestyä datan sääntelyä osana henkilötietojen suojan sääntelyä, minkä vuoksi datan sääntelykehikon analysointi rajautuu pääasiassa tietosuojaoikeudellisiin näkökulmiin. Datan sisällöllisestä laajuudesta ja monipuolisista käyttötarkoituksista johtuen on kuitenkin tarpeellista käydä seuraavaksi datan sisältöä, luonnetta ja alkuperää laajemmin läpi, jotta on mahdollista muodostaa käsitys myös datan sääntelyyn liittyvistä haasteista.

Digitaalisen teknologian muutettua viime vuosikymmenten aikana yhteiskuntaa, eri toimijoita ja toimialoja, on datasta tullut keskeinen osa muutosta. Vaikka dataa koskeva sääntely ei ole muodostunut kovinkaan yhtenäiseksi, on data ollut yhteiskunnallisen muutoksen ytimessä ja datan käyttöön on kohdistettu – ja kohdistetaan edelleen – jatkuvaa sääntelyä maailmanlaajuisesti. Kokonaisuudessaan yhteiskunnan tuottaman datan määrä on huomattava ja eri keinoin tuotettu data jatkaa kasvuaan teknologian kehittyessä.[34]

Tieto itsessään on muuttuva markkinahyödyke. Koska kyseessä on hyödyke, voi sen arvon myös määritellä esimerkiksi yritysten liiketoiminnassa, jossa tieto luo kilpailuetua markkinoilla.[35] Tätä tiedon arvoa voidaan mitata ja määritellä eri keinoin. Tiedon rahallinen arvo voi olla muun muassa immateriaalioikeuksien piiriin kuuluva tekijänoikeuden suojan alainen kohde, joka voi tuottaa tekijälleen rahallista arvoa. Tietojen arkistointi ilmentää tiedolla olevaa historiallista arvoa, ja varmuus- ja todistusarvo taas osoittaa yksilöille tai yhteisöille

[33] Tarkela 2016, s. 68.
[34] Ks. Euroopan komissio, Euroopan datastrategia 2020, s. 1.
[35] Voutilainen 2019, s. 21.

etuja, velvoitteita ja oikeuksia.[36] Sen sijaan sähköisessä muodossa olevan tiedon eli datan ominaisuudet, käyttö ja rooli yhdessä osoittavat datan moninaisuuden, jonka määrittely on tiedon määrittelyä itsessään haastavampaa. Data toimii markkinoilla tosiasiallisen vaihdannan kohteena, jolloin datalle muodostuu taloudellista arvoa eri toimintojen, kuten sen keräämisen, jalostamisen ja luovutustoimen yhteydessä. Tästä huolimatta datan varallisuusoikeudellinen asema on epäselvä.[37]

EU:ssa on pyritty korostamaan datan vapaata liikkuvuutta. Kuten yleisestikään datan sääntelyn kohdalla, ei myöskään datan vapaata liikkuvuutta ole löydettävissä yhden säädöksen alta. Sekä henkilötiedoille että muille tiedoille on oma oikeudellinen perustansa. Yleinen tietosuoja-asetus sääntelee henkilötietojen vapaata liikkuvuutta ja muiden tietojen osalta EU-oikeuden tasoisesti säädetään muiden kuin henkilötietojen vapaasta liikkuvuudesta annetussa asetuksessa[38]. Nämä molemmat asetukset pyrkivät sisämarkkinoiden toiminnan parantamiseen ja lisäksi henkilötietoja koskevan asetuksen olennainen tavoite on varmistaa henkilötietojen asianmukainen suoja.[39]

2.2 Datan ominaisuudet

Dataa on edellä esitetyin tavoin mahdollista arvioida myös oikeudellisesti ja sitä säännelläänkin monin eri tavoin. Data on ominaisuuksiltaan muuttuvaa ja sitä voidaan jalostaa, jakaa ja yhdistää. Datan arvon määritteleminen ei myöskään tästä syystä ole yksinkertainen. Alun perin arvottomaksi katsotusta datasta voi prosessin myötä muodostua arvokasta dataa ja saman prosessin toimiessa toisinpäin, voi datan arvo ikään kuin laskea tai hävitä. Datan arvo ei siten sellaisenaan ole välttämättä pysyvää. Niin ikään data ei kulu.[40]

Tarkelan mukaan datan ominaisuuksista juuri jatkojalostettavuus ja muokattavuus saavat korostetun aseman, kun dataa lähestytään raaka-ainetasoisena ilmiönä. Nämä ominaisuudet mahdollistavat datan kehittämisen esimerkiksi käyttötarkoituksen tai laadun osalta, mitä Tarkela kutsuu datan jalostamiseksi tai sen jalostusarvon lisäämiseksi.[41]

---

[36] Voutilainen 2019, s. 22.
[37] Tarkela 2016, s. 79.
[38] Euroopan parlamentin ja neuvoston asetus (EU) 2018/1807 muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa.
[39] Kaivola 2020, s. 234–235.
[40] Warma – Nieminen 2016, s. 552.
[41] Tarkela 2016, s. 68.

Koska data on vaihdannan kohteena, ei vaihdannan tulos ole kuitenkaan yhtä tarkkarajainen kuin esimerkiksi rahan käytön suhteen. Kun kuluttaja maksaa ostoksensa perinteisessä myymälässä rahalla, kuluttaja saa tällöin ostamansa tietyn tuotteen, kuten henkilöauton. Samanlainen tarkkarajaisuus ei kuitenkaan päde sellaisenaan dataan.[42] Kuluttajasta saatavan tiedon laatu, laajuus ja merkitys voi vaihdella, kun kuluttaja ikään kuin vaihtaa itsestään annettavat tiedot mahdollisuuteen käyttää tiettyä palvelua. Sama koskee myös sen palvelun laatua ja laajuutta, jonka kuluttaja saa. Kerätty data voi olla sitä keräävälle yritykselle erityisen hyödyllistä, mutta tämä hyödyllisyys ei välttämättä ilmene lainkaan samalla tavalla kuluttajalle tai palvelun käytössä. Tätä kuvastaa se, että data on ominaisuuksiltaan erilainen kuin esimerkiksi edellä mainitun tilanteen mukainen fyysinen tavara, jonka ominaisuuksien voidaan pitkälti ajatella olevan valmistajan sekä käyttäjän tiedossa.

2.3 Datan sisältö ja määrä jaottelun perusteena

Dataa voidaan sisällöllisesti jaotella eri tavoin, riippuen siitä, mitä jaottelulla pyritään selvittämään. Datasta ilmenevä informaatio voi olla pitkälti mitä tahansa oikeudellisessa merkityksessä.[43] Data saa merkityksensä vasta, kun dataa kyetään tulkitsemaan prosessoinnin kautta ja se muovaantuu hallittavaksi tiedoksi. Datan määrittelyssä olennaiseksi nousee datan sisältö, luonne ja käyttötarkoitus.[44] Mikäli data määritellään henkilötiedoiksi[45], on kyse tiedoista, joiden avulla yksittäinen henkilö on tunnistettavissa. Tekijänoikeudella taas suojataan dataa, jossa on kyse luodusta teoksesta.[46] Niin ikään liikesalaisuuksilla pyritään suojaamaan dataa, joka ei ole yleisesti tunnettua tai helposti saatavilla ja jolla voi ominaisuuksiensa vuoksi olla yrityksen liiketoiminnan kannalta taloudellista arvoa.[47] Esimerkiksi yrityksen kannalta arvokasta know-how'ta voidaan pitää salaisena tietona, jota arvioidaan

[42] Lehtioksa – Ljungman – Vainio 2019, s. 870.
[43] Tarkela 2016, s. 68.
[44] Alén-Savikko – Pitkänen 2016, s. 4.
[45] TSA 4(1) artikla.
[46] Tekijänoikeuslain (404/1961) 1 §:n 1 momentin mukaan tekijänoikeuden kohde on sillä, joka on luonut kirjallisen tai taiteellisen teoksen, on tekijänoikeus teokseen, olkoonpa se kaunokirjallinen tahi selittävä kirjallinen tai suullinen esitys, sävellys- tai näyttämöteos, elokuvateos, valokuvateos tai muu kuvataiteen teos, rakennustaiteen, taidekäsityön tai taideteollisuuden tuote taikka ilmetköönpä se muulla tavalla.
[47] Liikesalaisuuslaki (595/2018) määrittelee liikesalaisuudeksi tiedon, joka ei ole kokonaisuutena tai osiensa täsmällisenä kokoonpanona ja yhdistelmänä tällaisia tietoja tavanomaisesti käsitteleville henkilöille yleisesti tunnettua tai helposti selville saatavissa, jolla kyseisessä kohdassa tarkoitetun ominaisuuden vuoksi on taloudellista arvoa elinkeinotoiminnassa ja joka laillinen haltija on ryhtynyt kohtuullisiin toimenpiteisiin sen suojaamiseksi (liikesalaisuuslaki 2 § 1 momentin 1 kohta).

osana liikesalaisuutta.[48] Jaottelua voidaan myös tarkentaa entisestään ottamalla huomioon datan keräämisen tarkoitus, jolloin data voidaan jakaa esimerkiksi sosiaalisen dataan ja käyttäytymisdataan.[49]

Keskeisimpinä jaotteluina luovutusvelvollisuuden arvioinnissa on jako massadataan ja omaan dataan sekä jako henkilötietoihin ja muihin kuin henkilötietoihin. *Massadatalla* (*big data*) viitataan soveltamismahdollisuuksiltaan laajoihin data-aineistoihin ja datavirtoihin, jotka ovat usein määriltään suuria. Massadata kertyy myös suurella nopeudella ja se voi olla epäyhtenäistä.[50] Epäyhtenäisyydestä huolimatta massadata voi kuitenkin sisältää hyvinkin erilaista dataa. Massadatasta voidaan erottaa henkilöä itseään koskeva data eli *oma data* (*mydata*), jolla tarkoitetaan henkilöön liitettävää tietoaineistoa ja siihen liittyvää ihmiskeskeistä hallintatapaa ja periaatteita.[51]

Datan jaottelu henkilötietoihin ja muihin kuin henkilötietoihin perustuu pitkälti EU:n lainsäädäntöön, jota tarkastelemalla saadaan selville se, milloin yleistä tietosuoja-asetusta voidaan soveltaa.[52] Datan muuttuvan luonteen takia karkea erottelu on kuitenkin epätarkoituksenmukaista. Käsittelyn ja prosessoinnin myötä data voi muuttua henkilötiedosta muuksi tiedoksi ja toisinpäin. Data voi myös sisältää monenlaisia eri tietoja, jolloin se voi sisältää tietoja sekä henkilötiedoista että muista tiedoista. Lisäksi data voi koostua useammasta eri tiedosta yhtäaikaisesti: henkilötietoja sisältävä data voidaan katsoa myös esimerkiksi liikesalaisuuden alaiseksi.[53]

Edellä kuvatun mukaisesti muiden kuin henkilötietojen osalta datan sääntely voi olla immateriaalioikeudellista tai liikesalaisuussäännösten alaista. Taustalla on tällöin datan ja sen sisältämän informaation kontrollointi, jonka yhteydessä säädetään datan käytöstä, siihen pääsystä ja näiden rajoittamisesta. Kun etsitään vastausta käytännössä yhteen spesifimpään

[48] Ks. know-how'sta liikesalaisuutena Vapaavuori 2019, s. 94–95.
[49] Van Gorp ym. 2020, s. ii.
[50] Liikenne- ja viestintäministeriö 2016, päätösperustelut s. 1.
[51] Liikenne- ja viestintäministeriö 2016, päätösperustelut s. 1.
[52] Tarkelan mukaan jaottelua henkilötietoihin ja muihin kuin henkilötietoihin voidaan pitää ongelmallisena, kun tarkastelun kohteena on dataa massaluontoisesti käyttävät liiketoimintamallit, joissa data voi olla sekamuotoista (sekä henkilötietoja että muuta dataa sisältävä). Tarkelan mukaan kahtiajako pakottaisi sääntelyn keinotekoisiin ja sääntelyn koherenssia olennaisesti vähentäviin rajanvetoihin. Ks. lisää ko. jaottelusta mm. Tarkela 2016, s. 103–105.
[53] Tarkela 2016, s. 103–104 ja Kaivola 2020, s. 235.

dataan liittyvään ongelmaan, on aihealue usein yhtä alaa laajempi, jolloin säännökset ovat päällekkäisiä tai soveltuvat yhtäaikaisesti.[54]

2.4 Data sääntelyn kohteena

Dataa, kuten henkilötietoja, ei voida omistaa eikä niitä voida samaistaa omaisuuteen. Luonnolliset henkilöt, joita tiedot koskevat, eivät siis voi omistaa tai kontrolloida omia henkilötietojaan. Henkilöillä on kuitenkin tarkasti määriteltyjä oikeuksia henkilötietoihinsa liittyen, kuten pääsy omiin henkilötietoihinsa sekä oikeus niiden poistamiseen.[55] Datan omistajuuteen liittyy useita oikeudellisia kysymyksiä, kuten se, kenelle omistusoikeuden tulisi kuulua ja miten laajasti omistusoikeus tulisi määritellä. Mikäli käsittelemätöntä dataa eli niin sanottua *raakadataa* saadaan kerättyä ja muokattua hyödynnettäväksi ja jalostetuksi dataksi ainoastaan sellaisen teknologian avulla, mihin kyseistä dataa keräävä yritys on investoinut ja mitä se on itse kehittänyt, kuuluuko näin kerätty raakadata yksilölle, josta pitkälti arvoton raakadata on kerätty, vai yritykselle, jota ilman kyseistä jalostettua dataa ei olisi alun perinkään voitu hyödyntää? Jäljempänä mainittu näkökulma voisi myös johtaa omistajuuden määrittelemiseen siten, että omistajuus ei kuuluisi ainoastaan yhdelle oikeussubjektille, vaan useammalle.[56]

Datan omistajuuteen liittyvissä keskusteluissa on toisaalta myös esitetty, ettei omistajuuden selvittäminen lopulta edes olisi olennaisin kysymys. Datan ollessa tällä hetkellä kilpailuoikeudellisessa mielessä kilpailematon hyödyke, voisi sen omistajuuden määritteleminen jopa vähentää sen käyttöä.[57] Datan laajemman käytön hyödyntämistä tukisi näin datan käyttöoikeuden ja siirrettävyyden korostaminen, ei välttämättä omistajuuden määrittäminen.[58]

Ominaisuuksiensa ja hyödyntämistapojensa vuoksi data ei sääntelyobjektina sovellu nykyisiin järjestelmätasoisiin ratkaisumalleihin, kuten varallisuusoikeuden osajärjestelmien esineoikeuden tai immateriaalioikeuden piiriin. Tarkelan mukaan esineoikeudellisesta näkökulmasta katsottuna ongelmaksi muodostuu se, että datalta puuttuu edellä kuvattujen ominaisuuksien vuoksi pysyvyys. Niin ikään immateriaalioikeuden suojan kohteena olevat

[54] Alén-Savikko – Pitkänen 2016, s. 5.
[55] Byström 2014, s. 213.
[56] Ks. KKV 2019, s. 14.
[57] KKV 2019, s. 15.
[58] KKV 2019, s. 15 ja JRC 2017, s. 46–47.

perusominaisuudet poikkeavat datan ominaisuuksista siinä määrin kuin datan hyödyntämisen liiketoimintamallit perustuvat yksinoikeusrakenteiden sijaan datan vapaaseen yhdisteltävyyteen.[59]

Dataan kohdistuu oikeuksia ja velvollisuuksia siitä huolimatta, että sen oikeudellista asemaa sääntelyobjektina voidaan pitää epäselvänä. Datan epätyypillisen varallisuusaseman vuoksi tiedon varallisuusarvon määritteleminen on haastavaa ja monimutkaista.[60] Mainituista epäselvyyksistä huolimatta data on sääntelyn kohteena kasvavassa määrin. Vaikka data on vaihdannan kohteena ja sen arvo on sinänsä tunnustettu, varallisuusoikeudelle uutena resurssina data ei ole vielä saavuttanut vakiintunutta asemaa. Kysymys lainsäädännöllisen aseman vakiinnuttamisesta aiempaa tuntemattoman resurssin tai ilmiön esiintyessä, ei kuitenkaan ole sinänsä uusi. Immateriaalioikeuden kehitys teknologian kehittyessä on johtanut viimeisen sadan vuoden aikana erilaisiin ratkaisuihin omistus- ja varallisuusoikeuksien osalta esimerkiksi tietokoneohjelmien patentti- ja tekijänoikeudellisten kysymysten osalta.[61] Varallisuusoikeudellisesta näkökulmasta datan sääntely voisi siten edellyttää jopa varallisuusoikeudellisen järjestelmän kehitystä ja muutosta vastaanottaa data ominaisuuksiltaan erilaisena resurssina.[62]

2.5 Datan hyödyntäminen liiketoiminnassa

Datan hyödyntämisessä nykyisillä markkinoilla on huomion saanut datan käsittelyn alkupää, jossa yrityksiltä ja kuluttajilta kerätty data päätyy sitä hallinnoivalle yritykselle. Tällöin arvioidaan esimerkiksi sitä, millä perusteilla tietoa kerätään, mitä tietoa kerätään ja miten yksilö voi omalta osaltaan tähän vaikuttaa. Tietoa siitä, mitä kyseessä olevalle datalle tapahtuu sen jälkeen, kun se on siirtynyt yrityksen hallintaan ja määräysvallan alaiseksi, on kuitenkin sitä vastoin vähän.[63]

Henkilötiedot sellaisinaan tai jalostettuina muodostavat hyödykkeen, jota tietoja hallinnoiva tai keräävä yritys voi hyödyntää omassa toiminnassaan tai myydä sitä muille toimijoille.[64]

---

[59] Tarkela 2016, s. 89 ja 95.
[60] Warma – Nieminen 2016, s. 552.
[61] Tarkela 2016, s. 81–82.
[62] Tarkela 2016, passim.
[63] Tarkela 2016, s. 70–71.
[64] Lehtioksa – Ljungman – Vainio 2019, s. 869.

Kerättyä dataa voidaan hyödyntää liiketoiminnassa esimerkiksi käsitellen data anonyymiksi ja myyden se eteenpäin tiedon kerääjänä toimivan yhtiön yhteistyö- tai liikekumppanille. Henkilötiedoista tunnistettavuuden poistaminen voidaan tehdä tietoja luovuttaneen henkilön suostumuksin palvelun käyttöehdoissa tarkemmin määritellyillä tavoilla. Kuten mainitunlainen digitaalisen datan liiketoimintamalli, hyödyntävät myös muut liiketoimintamallit nimenomaan datan ominaisuuksina sen muokattavuutta ja jalostamismahdollisuutta. Dataa voidaan hyödyntää liiketoiminnassa kaupallisesti nimenomaan sen lukemattomien jatkokäyttömahdollisuuksien perusteella.[65] Datataloudessa on lisäksi kehittynyt liiketoimintamalleja, joiden avulla dataa hallinnoivat toimijat voivat kaupallistaa kerätyn datan arvon paljastamatta kuitenkaan dataa itsessään. Esimerkiksi silloin, kun hyödynnetään kerättyä dataa markkinoinnissa, tulee palvelunkäyttäjälle näkyviin markkinoitava kohde eikä se käyttäjästä kerätty data, johon markkinointi perustuu.[66]

Lähtökohtana myös datatalouden liiketoimintamalleissa on, että henkilötietoihin perustuvan datan keräämisessä ja käsittelyssä noudatetaan tietosuojalainsäädäntöä. Kerätyn datan kaupallisessa hyödyntämisessä voidaan kuitenkin jättää noudattamatta henkilötietoihin kohdistuvaa sääntelyä sillä perusteella, ettei dataa enää itsessään luetakaan henkilötietoja sisältäväksi dataksi. Näin se ei luonnollisestikaan enää kuulu henkilötietojen suojan sääntelyn piiriin. Dataa hallinnoivat yritykset voivat nähdä tietosuojasääntelyn yrityksen toimintaa jäykistävänä ja hidastavana, minkä takia kyseiset yritykset voivat tarkoituksellisesti pyrkiä saamaan toimintaa koskevan sääntely minimaaliseksi.[67]

Kerätty data-aines voi siten sisältää jopa tarkoituksenmukaisesti sekä henkilötietoja että myös muita kuin henkilötietoja, jolloin kerättyä dataa voidaan pitää sekamuotoisena.[68] Vaikka data ei tällöin suoranaisesti kaikilta osin kuuluisi henkilötietojen suojan piiriin, on tällaisen sekamuotoisen tietoaineksen käsittelystä säädetty myös toisessa Euroopan unionin asetuksessa. Muiden kuin henkilötietojen vapaata liikkuvuutta koskevan asetuksen 2(2) artiklan mukaan jos tietojoukko sisältää sekä henkilötietoja että muita kuin henkilötietoja, kyseessä olevaa asetusta sovelletaan muita kuin henkilötietojen koskevaan tietojoukon osaan. Jos tietojoukossa olevat henkilötiedot ja muut kuin henkilötiedot liittyvät

[65] Tarkela 2016, s. 89–90 ja Lehtioksa – Ljungman – Vainio 2019, s. 869.
[66] JRC 2017, s. 46–47.
[67] Tarkela 2016, s. 103.
[68] Tarkela 2016, s. 103–104 ja Kaivola 2020, s. 235.

erottamattomasti toisiinsa, kyseinen asetus ei rajoita yleisen tietosuoja-asetuksen soveltamista.[69] Näin myös sekamuotoinen data on pyritty tuomaan soveltamispiirin alaiseksi henkilötietojen sekä muiden kuin henkilötietojen osalta.

Mitä tulee yrityksen keräämiin muihin kuin henkilötietoihin, voi yritys hyödyntää kyseistä dataa liiketoiminnassaan usealla eri tavalla. Tuotteita ja tavaroita valmistava yritys voi toimittaa tuotteitaan hyödynnettäväksi edelleen käyttäjille. Tuotteen valmistanut yritys voi kuitenkin saada tuotteen luovuttamisen jälkeenkin dataa itselleen tuotteen käytöstä ja siitä, miten kyseinen tuote tai laite toimii. Laitteen valmistanut yritys saa itselleen näin arvokasta dataa, joka auttaa kehittämään tuotteita, niiden kunnossapitoa ja ennaltaehkäisemään laitevikoja. Sitä vastoin asiakkaana toimivalle yritykselle kyseinen data voi sisältää arvokkaita liikesalaisuuksiksi määriteltäviä tietoja tuotannon toiminnasta ja tuotteista itsestään. Tämäntyyppinen tieto ei välttämättä saa suojaa teollis- tai tekijänoikeuksin, mutta ollessaan silti arvokasta ja yrityksen kannalta arkaluontoista, on tiedon suojaaminen mahdollista yritysten välisten sopimuksin. Tietokantaa käyttävät toimijat voidaan siten sitouttaa sopimuksin datan luottamukselliseen käsittelyyn.[70] Sääntely on tällöin pitkälti sopimusoikeudellisen sääntelyn lisäksi yritysten välisten sopimuksien varassa.

[69] Euroopan parlamentin ja neuvoston asetus (EU) 2018/1807, annettu 14 päivänä marraskuuta 2018, muiden kuin henkilötietojen vapaan liikkuvuuden kehyksestä Euroopan unionissa.
[70] Ks. Alén-Savikko – Pitkänen 2016, s. 7 ja s. 17–18, jossa on avattu muun kuin henkilötietojen sisältämän datan käsittelyä ja hallinnointia Wärtsilä-yhtiön esimerkin kautta (”Case B”).

3 HENKILÖTIETOJEN SUOJA DATAN KÄSITTELYSSÄ

3.1 Yksityisyyden ja henkilötietojen suojan välinen suhde

Yksityisyyden suojalla on tärkeä merkitys henkilötietojen suojan määrittämisessä. Yksityisyys on sekä perus- että ihmisoikeus, joka vähitellen jakautuessaan useampaan perusoikeuteen muodostaa näin lopulta yksityisyyden suojan kokonaisuuden.[71] Sen lisäksi, että yksityisyyden suoja voidaan määritellä eri säädösperustein, on sen suojaaminen yksi tietosuojalainsäädännön tavoitteista.[72] Perinteisesti Suomessa yksityisyyden suojan on katsottu olevan perustuslain tasoinen oikeus, jolla suojataan jokaisen yksityiselämä, kunnia ja kotirauha.[73] Henkilötietojen suoja taas mahdollistaa henkilön oikeuden määrätä itseensä kohdistuvien tietojen keräämisestä ja käsittelystä, millä tarkoitetaan jäljempänä tarkemmin määriteltävää tiedollista itsemääräämisoikeutta. EU:ssa henkilötietojen suoja on katsottu tiiviisti primaarioikeuden tasoisesti osaksi yksityisyyden suojaa ja EU:n perusoikeuskirjan 7 artiklassa suojattua yksityiselämän kunnioittamista.[74]

Nykyään henkilötietojen suojan sääntelyn kehittymisen myötä voidaan yksityisyyden suoja ja henkilötietojen suoja nähdä myös toisistaan erotettuina. Tällöin henkilötietojen suoja luokitellaan yksityisyyden suojasta erilliseksi omaksi oikeudeksi, joka turvattiin EU:n perusoikeuskirjassa perusoikeutena jo 2000-luvun alussa.[75] Henkilötietojen suojan määrittelyssä olennaisena näyttäytyisi kuitenkin olevan sen kiinteä liityntä yksityis- ja perhe-elämään ja niiden kunnioittamiseen. Henkilötietojen suojan tarkastelun kohteena on yksityisyydeltään suojatun henkilön tunnistettavien tietojen suoja ja sen turvaaminen, että kyseisellä luonnollisella henkilöllä on valtaa omien tietojensa käsittelylle.

Riippumatta siitä, että henkilötiedot on suojattu esimerkiksi omana erillisenä EU-tasoisena perusoikeutena, vaikuttaisi henkilötietojen suojan kytkös yksityisyyteen olevan siinä määrin vahva, ettei näitä kahta tulisi arvioida toisistaan täysin erillisinä oikeuksina.

---

[71] Neuvonen 2014, s. 20–21.
[72] Warma – Nieminen 2016, s. 550.
[73] PL 10 § 1 momentti.
[74] Warma – Nieminen 2016, s. 551.
[75] Neuvonen 2019, s. 23 ja EU:n perusoikeuskirjan 8 artikla.

3.1.1 Yksityisyys perus- ja ihmisoikeutena

Yksityisyyden suoja on tunnustettu perus- ja ihmisoikeus kansallisella, EU-oikeuden tasoisella ja kansainvälisen oikeuden tasolla. Suomen perustuslain (731/1999, PL) 10 §:n 1 momentissa säädetyn yksityiselämän suojan mukaan jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. PL 10 §:n 2 momentin mukaan kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Yksityisyyden suojaan kuuluu siis moninaisesti yksityiselämän suojaan sisältyviä osa-alueita, kuten kotirauha ja kunnia. Tietoihin kohdistetun yksityisyyden suojan vastinparina on tietojen julkisuus. Laki määrittelee rajan yksityisen ja julkisen välillä.[76]

EU:n perusoikeuskirjassa yksityisyyden suoja on turvattu 7 artiklassa, jonka mukaan jokaisella on oikeus siihen, että hänen yksityis- ja perhe-elämäänsä, kotiaan sekä viestejään kunnioitetaan. Perusoikeuskirjan seuraavassa artiklassa 8 turvataan puolestaan erikseen henkilötietojen suoja. Ihmisoikeutena yksityisyyden suoja on turvattu YK:n ihmisoikeusjärjestelmässä KP-sopimuksen[77] 17 artiklassa sekä YK:n yleismaailmallisen ihmisoikeuksien julistuksen[78] 12 artiklassa. Molemmissa on turvattu oikeudet yksityiselämään, perheeseen, kotiin, kirjeenvaihtoon sekä kunniaan ja maineeseen. Valtiolle on asetettu velvollisuus turvata lailla kyseisten oikeuksien toteutuminen.

Euroopan ihmisoikeussopimuksen[79] 8 artiklan mukaan jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Lisäksi viranomaiset eivät saa puuttua tämän oikeuden käyttämiseen, paitsi silloin kun laki sen sallii ja se on demokraattisessa yhteiskunnassa välttämätöntä kansallisen ja yleisen turvallisuuden tai maan taloudellisen hyvinvoinnin vuoksi, epäjärjestyksen ja rikollisuuden estämiseksi, terveyden tai moraalin suojaamiseksi tai muiden henkilöiden oikeuksien ja vapauksien turvaamiseksi.

---

[76] Mäenpää 2016, s. 8.
[77] Kansalais- ja poliittisia oikeuksia koskeva yleissopimus SopS 7–8/1976, johon Suomi liittyi vuonna 1976.
[78] Yhdistyneiden Kansakuntien ihmisoikeuksien yleismaailmallinen julistus, hyväksytty YK:n yleiskokouksessa 10.12.1948.
[79] Yleissopimus ihmisoikeuksien ja perusvapauksien suojelemiseksi SopS 18–19/1990 (Euroopan ihmisoikeussopimus, EIS).

3.1.2 Yksityisyyden suoja, tietosuoja ja henkilötietojen suoja

Sen lisäksi, että yksityisyyden suoja on perus- ja ihmisoikeus edellä kuvatun tavoin, voidaan sitä tarkastella myös spesifimmin oikeutena tietosuojaan, tietoturvaan ja viestintään. Tietosuoja sisältää luottamuksellisen viestinnän suojan periaatteen, joka ilmenee perustuslain 10 §:n 2 momentissa taattuna viestintäsalaisuutena. Oikeus tietoturvaan pitää sisällään viranomaisille ja muille rekisterinpitäjille asetetun vaatimuksen hyvästä tiedonhallintatavasta; rekisteröidyn tulee voida luottaa siihen, että hänen tietojaan käsitellään lainmukaisesti. Kuten henkilötietojen suoja myös oikeus tietoturvaan perustuu tiedolliselle itsemääräämisoikeudelle, jonka johdosta tietojen kohteella tulisi olla oikeus tutustua itseään koskeviin tietoihin, korjata kyseisiä tietoja ja myös kieltäytyä tietojen rekisteröimisestä. Niin ikään oikeus viestintään edellyttää sitä, että mahdollisella viestinnän rajoituksella on asianmukaiset perusteet.[80] Nämä oikeudet ovat siten osittain limittäisiä ja mahdollistavat päällekkäisen tarkastelun.

Toisaalta henkilötietojen suojaa voidaan kuvata myös yksityisyyden yläpuolella vaikuttavaksi periaatteeksi, joka on kehittynyt ja laajentunut kokonaisvaltaisemmin tietosuojaksi.[81] Tietosuojaa ja henkilötietojen suojaa käsitellään oikeuskirjallisuudessa osittain samoilla termeillä, mutta terminologian osalta löytyy myös poikkeavia näkemyksiä. *Neuvonen* ei esimerkiksi pidä henkilötietojen suojan ja tietosuojan käsitteitä synonyymeina, sillä tietosuojan vaatimukset voivat hänen mukaansa ulottua myös yritystietoihin, kuten liikesalaisuuksiin.[82] Tietosuojan määrittely henkilötietojen suojaa laajemmaksi käsitteeksi on perusteltua, mutta käsitteiden sekoittumista ja käyttöä synonyymeina entisestään on korostanut yleinen tietosuoja-asetus, jonka suomenkielinen käännös nimensä mukaisesti rajoittuu tietosuojaan, eikä yleiseen henkilötietojen suojaan. Tämän vuoksi henkilötietojen suojasta voidaan käyttää myös nimitystä tietosuoja, jolla asian kontekstista riippuen tarkoitetaan joko henkilötietoihin liittyvää tietosuojaa tai muihin tietoihin liittyvää tietosuojaa.

[80] Neuvonen 2019, s. 47.
[81] Neuvonen 2019, s. 117 ja Mahkonen 1997, s. 19.
[82] Ks. Neuvonen 2014, s. 64.

3.1.3 Tiedollinen itsemääräämisoikeus

Henkilötietojen suojan taustalla vaikuttaa ajatus yksityisyyden suojaamisesta ja yksilön persoonallisuuden säilyttämisestä henkilötietojen käyttöön ja käsittelyyn kohdistetun sääntelyn avulla. Perustana henkilötietojen suojalle on luonnollisen henkilön tiedollinen itsemääräämisoikeus.[83] *Tiedollisella itsemääräämisoikeudella* tarkoitetaan sitä, että henkilöllä itsellään tulisi olla mahdollisimman suuri vaikutusvalta siihen, miten hänen tietojaan käsitellään. Henkilötietojen käsittely pitää sisällään kysymykset ja vastaukset siihen, kuka henkilötietoja käsittelee, missä tilanteissa niitä käsitellään ja miten niitä käsitellään.[84]

Tiedollinen itsemääräämisoikeus on kokonaisuus, joka ei niinkään ole yksi itsenäinen oikeus, vaan monien oikeuksien kattokäsite, joka sisältää henkilölle kuuluvia tiedollisia oikeuksia. Näitä tiedollisia oikeuksia ovat myös yleisessä tietosuoja-asetuksessa rekisteröidylle asetetut oikeudet, kuten oikeus saada itseään koskeva tieto, oikeus tarkastaa itseään koskeva tieto sekä oikeus itseään koskevien tietojen luovuttamiseen, julkaisemiseen ja antamiseen.[85] Kuten jäljempänä tutkielmassa tarkemmin käsitellään, eivät kyseiset tiedolliset oikeudet ole ehdottomia, vaan niitä voidaan rajata ja rajoittaa erilaisia toteutettavia tarkoituksia varten, kuten yhteiskunnan turvallisuuden varmistamiseksi, jonka nojalla rekisteröity voi olla velvollinen antamaan itseään koskevia tietoja viranomaisen käyttöön.[86]

Keskeistä henkilötietojen käsittelyssä ovat ne ehdot, joiden perusteella henkilötietoja saa käsitellä. Lisäksi henkilötietojen käsittelyyn kuuluu se, miten kerättyjä henkilötietoja voidaan luovuttaa ja yhdistellä toisiin henkilötietoihin.[87] Yhtenä käsittelyperusteena suostumuksella on olennainen merkitys tiedollisen itsemääräämisoikeuden toteutumisessa. Tiedollinen itsemääräämisoikeus toteutuu henkilön itsensä antaman tahdonilmaisun, eli suostumuksen, kautta henkilötietojensa käsittelylle, jolloin henkilö tietoisesti antaa hyväksyntänsä omien tietojensa keräämiselle ja myös käsittelylle.[88]

---

[83] Tarkela 2016, s. 97 ja Neuvonen 2014, s. 59.
[84] Neuvonen 2014, s. 59.
[85] Voutilainen 2019, s. 83.
[86] Voutilainen 2019, s. 84.
[87] Neuvonen 2014, s. 60.
[88] Ks. suostumuksesta tiedollisen itsemääräämisoikeuden toteuttamiskeinona Neuvonen 2014, s. 65–66, Tarkela 2016, s. 98 ja Voutilainen 2019, s. 85.

3.2 Henkilötietojen suojan sääntely EU:ssa

Datan luovutuksessa olennaista on henkilötietoja koskeva sääntely, jota noudatetaan myös digimarkkinasäädöksessä henkilötietoja sisältävän datan osalta. Henkilötietoja koskeva sääntely on olennaista myös sen tunnistamiseksi, milloin data kuuluu sääntelyn piiriin sekä miten sääntely toteutuu datan itsensä ja sitä hyödyntävien yritysten toiminnassa.

Henkilötietojen suoja rakentuu EU:ssa perussäännöksien varaan. Se on turvattu EU:n perusoikeuskirjan 8 artiklassa sekä sopimuksessa Euroopan unionin toiminnasta (SEUT) 16 artiklassa. Perusoikeuskirjan 8 artiklan ja SEUT:n 16 artiklan mukaan jokaisella on oikeus henkilötietojensa suojaan. Perusoikeuskirja täsmentää tietojen käsittelyä siten, että sen on oltava asianmukaista ja tapahduttava tiettyä tarkoitusta varten asianomaisen henkilön suostumuksella tai muun laissa säädetyn oikeuttavan perusteen nojalla. Jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi. Näiden säännösten noudattamista valvoo riippumaton viranomainen.

Henkilötietojen käsittelyn olennaisin sääntely keskittyy nykyään EU:n yleiseen tietosuoja-asetukseen. Tätä ennen henkilötietoihin ja henkilötietojen suojaan liittyvä sääntely koostui pitkälti EU:n henkilötietodirektiivissä[89] ja sen nojalla säädetyssä kansallisessa henkilötietolaissa (523/1999). Henkilötietolain korvasi kansallisella tasolla tietosuojalaki (1050/2018), joka täydentää yleistä tietosuoja-asetusta siltä osin kuin asetuksessa on jätetty liikkumavaraa kansalliselle sääntelylle. Tietosuoja-asetuksen voimaantulo herätti aikanaan paljon keskustelua globaalilla tasolla ja nosti tietosuojakysymykset myös uudella tavalla näkyville yhteiskunnassa. Uudistettu tietosuojasääntely ei näkyvyydestään huolimatta ollut täysi vallankumous, kuten *Talus* on artikkelissaan kuvannut, vaan ennemminkin vanhan sääntelyn päivitys vastaamaan uudistunutta sääntelyn tarvetta.[90]

Yleisen tietosuoja-asetuksen ja kansallisen tietosuojalain lisäksi henkilötietojen käsittelystä säädetään yhä lukuisissa erityislaeissa, mistä syystä sääntelyä voidaan edelleen pitää jokseenkin hajautuneena ja monimutkaisena.[91] Tietosuojalain uudistamisen yhteydessä

[89] Euroopan parlamentin ja neuvoston direktiivi 95/46/EY annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.
[90] Ks. Talus 2019, s. 213–214.
[91] Korpisaari 2019 s. 28 ja Valtioneuvoston selvitys- ja tutkimustoiminnan 2017 julkaisu, jossa on esitelty yhteensä 720 eri säädöstä ja arvioitu sitä, että ovatko ne olleet sopusoinnussa EU:n yleisen tietosuoja-asetuksen kanssa.

perustuslakivaliokunta on kuitenkin lausunnoissaan todennut, että henkilötietojen suojan sääntelyn kattavuuden, täsmällisyyden ja tarkkarajaisuuden vaatimuksien esteenä ei ole se, että niitä täytetään EU:n säädöksillä ja kansallisilla yleislaeilla.[92]

Yleisen tietosuoja-asetuksen lähtökohtana on henkilötietojen vapaa liikkuvuus unionin sisällä.[93] Asetuksella on yksilön perusoikeuksien ja -vapauksien suojaamisen lisäksi taloudellinen tarkoitus.[94] Oikeus henkilötietojen suojaan ei kuitenkaan ole absoluuttinen. Oikeutta henkilötietojen suojaan on ensinnäkin tarkasteltava suhteessa sen yhteiskunnalliseen tehtävään. Koska asetettu oikeus on perusoikeus, tulee sen myös noudattaa suhteellisuusperiaatetta muihin perusoikeuksiin nähden.[95]

Henkilötietojen käsittelyä koskeva tietosuoja-asetus rajaa soveltamisalastaan pois oikeushenkilöiden ja erityisesti oikeushenkilön muodossa perustettujen yritysten henkilötietojen käsittelyn.[96] Asetusta ei niin ikään sovelleta kuolleita henkilöitä koskevien tietojen käsittelyyn.[97] Erikseen asetuksessa on korostettu tunnistettujen ja tunnistettavissa olevien luonnollisten henkilöiden suojausta, millä viitataan siihen, että anonyymit tiedot, jotka eivät liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön taikka henkilötiedot, joiden tunnistettavuus on poistettu, eivät kuulu asetuksen soveltamisalan piiriin.[98]

Erikseen voidaan arvioida sitä, onko koko sääntely datatalouden alueella jälleen kerran uudistuksen tarpeessa, koska digitaalinen talous ja datan määrä kasvaa entisestään ja huomattavan nopeasti. Yksittäisen säädöksen, kuten yleisen tietosuoja-asetuksen, uudistaminen ei näyttäisi kuitenkaan olevan ratkaisun ydin, vaan ongelmaksi jää silti sääntelyn yhteensopivuus muiden oikeudenalojen suhteen sekä sääntelyn hajautuneisuus tietosuoja-asetuksella tavoitellusta oikeustilan yhtenäistämisestä huolimatta.[99] Yksittäisen oikeudenalan sääntelyn uudistaminen voi siten edellyttää muidenkin asiaan liittyvien alojen kuten kilpailuoikeuden sääntelyn päivitystä, jotta uudistuksella saavutettaisiin sillä tavoiteltu hyöty myös muiden oikeudenalojen ja niitä koskevien sääntelyjen suhteen.

[92] Ks. esim. perustuslakivaliokunnan lausunnot 2/2018 vp, s. 4–6, 31/2017 vp, s. 3–4 ja 38/2016 vp, s. 4.
[93] TSA 1(3) artikla.
[94] TSA:n johdanto 2 kohta.
[95] TSA:n johdanto 4 kohta.
[96] TSA:n johdanto 14 kohta.
[97] TSA:n johdanto 27 kohta.
[98] TSA:n johdanto 26 kohta.
[99] Ks. Ojanen 2016, s. 47.

3.3 Tietosuoja-asetuksen henkilötietojen käsittelyä koskevat periaatteet

Tietosuojaperiaatteet ovat tietosuoja-asetuksen 5(1) artiklan mukaan lainmukaisuus, kohtuullisuus ja läpinäkyvyys (*lawfulness, fairness and transparency*), käyttötarkoitussidonnaisuus (*purpose limitation*), tietojen minimointi (*data minimisation*), täsmällisyys (*accuracy*), säilytyksen rajoittaminen (*storage limitation*) sekä eheys ja luottamuksellisuus (*integrity and confidentiality*). Tietosuojaperiaatteet ovat osittain limittäisiä ja ne muodostavat yhdessä kokonaisuuden, joka määrittelee henkilötietojen käsittelyssä noudatettavaa linjaa.[100] Aiemmin voimassa ollut henkilötietodirektiivi sisälsi pitkälti samat periaatteet henkilötietojen käsittelylle kuin tietosuoja-asetus. Mainitut tietosuoja-asetuksen periaatteet ohjaavat henkilötietojen käsittelyä myös niissä tapauksissa, joissa ei ole tietosuoja-asetuksessa määrättyä ehdotonta sääntöä.[101] Periaatteet toimivat siten tulkinnan apuna.[102]

Henkilötietojen käsittelyn tulee olla lainmukaista ja asianmukaista.[103] Lainmukaisuus ja asianmukaisuus edellyttävät käsittelyyn oikeuttavaa oikeusperustetta. Kohtuullisuus periaatteena taas edellyttää reiluutta, jonka mukaan niin tietojen keräämisessä kuin käsittelyssä tulee huomioida rekisteröidyn yksityisyys sekä rekisteröidyn kohtuulliset odotukset. Rekisteröityä ei tule myöskään esimerkiksi painostaa toimittamaan itseään koskevia tietoja rekisterinpitäjälle tai hyväksymään tietynlaista tarkoitusta tai tietojen käsittelyä. Kohtuullisuus on siten kokonaisvaltainen periaate, joka näkyy rekisterinpitäjän toiminnan reiluna ilmentymänä etenkin rekisteröityä kohtaan.[104] Läpinäkyvyyden vaatimuksella taas taataan se, että toiminta tietojen keräämisen ja käytön osalta on avointa ja rekisteröidyille tietojen on oltava helposti saatavilla, ymmärrettävissä sekä kielenkäytöltään selkeää ja yksinkertaista.[105]

Käyttötarkoitussidonnaisuus rajaa henkilötietojen käytön siihen tiettyyn, nimenomaiseen ja lailliseen alkuperäiseen käyttötarkoitukseen. Käyttötarkoitussidonnaisuus ei suoranaisesti estä henkilötietojen käsittelyä myös jotain toista tarkoitusta varten, mutta tällöin edellytyksenä on, että tarkoitus on yhteensopiva alkuperäisen käyttötarkoituksen kanssa.[106] Käyttötarkoituksen tulee siten olla niin rekisteröidyn kuin rekisterinpitäjän itsensäkin tiedossa

[100] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 97.
[101] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 23.
[102] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 97.
[103] TSA 5(1)(a) artikla.
[104] Bygrave 2001, kohta Fair and lawful processing.
[105] TSA:n johdanto 39 kohta.
[106] TSA 5(1)(b) artikla.

ennen käsittelyn aloittamista. Tietojen minimointi taas edellyttää, että henkilötietojen on oltava asianmukaisia ja olennaisia sekä rajoitettuja siihen, mikä on tarpeellista suhteessa niihin tarkoituksiin, joita varten niitä käsitellään. Tarpeettomat tiedot ja tarpeettomiksi tulleet tiedot tulee poistaa.[107]

Edellä mainittujen lisäksi, henkilötietojen on oltava täsmällisiä ja tarvittaessa päivitettyjä. Rekisterinpitäjän tulee varmistaa kohtuullisin toimenpitein, että käsittelyn tarkoitukseen nähden epätarkat ja virheelliset tiedot poistetaan tai oikaistaan viipymättä.[108] Tietosuoja-asetuksen säilytyksen rajoittaminen koskee henkilötietojen säilytystä ja sen voidaan katsoa edellyttävän mahdollisimman lyhyttä säilytysaikaa. Joissain tilanteissa säilytysaika voi olla pidempi, mutta se edellyttää perustetta tietojen käsittelyn jatkumiselle. Peruste voi olla esimerkiksi suoraan lainsäädännön nojalla säädetty velvollisuus säilyttää tietoja tietyn ajan.[109]

Henkilötietojen käsittelyperiaatteena eheys ja luottamuksellisuus edellyttävät henkilötietojen käsittelyä siten, että niiden asianmukainen turvallisuus varmistetaan. Turvallisuuteen luetaan suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia.[110] Eheydellä tarkoitetaan sitä, että tietoja ei muuteta ilman rekisterinpitäjän suostumusta.[111]

TSA 5(2) artiklan osoitusvelvollisuuden mukaisesti rekisterinpitäjän on kyettävä osoittamaan, että kaikkia näitä tietosuojaperiaatteita on noudatettu rekisterinpitäjän toiminnassa (*accountability*). Osoitusvelvollisuus on asetettu rekisterinpitäjälle myös tietosuoja-asetuksessa yleisenä velvollisuutena TSA 24(1) artiklassa. Sen mukaan rekisterinpitäjän tulee arvioinnissa huomioida tietojen käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä rekisteröityihin kohdistuvat riskit. Rekisterinpitäjä ei voi kuitenkaan vain tyytyä riskiarvioinnin suorittamiseen uudessa käsittelytoimessa, vaan toimenpiteitä on jatkuvasti tarkastettava ja tarpeen mukaan päivitettävä.

[107] TSA 5(1)(c) artikla.
[108] TSA 5(1)(d) artikla.
[109] TSA 5(1)(e) artikla ja ks. Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 94.
[110] TSA 5(1)(f) artikla.
[111] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 94.

3.4 Tietosuoja-asetuksen mukaiset käsittelyperusteet

Henkilötietojen käsittelylle tulee aina olla tietosuoja-asetuksen 6(1) artiklan mukainen käsittelyperuste. Siispä rekisterinpitäjän kerätessä, käsitellessä, muokatessa ja niin ikään luovuttaessa henkilötietoja, tulee toimenpiteeseen olla laillinen peruste. Vaadittu laillinen peruste muodostaa tärkeän osan henkilötietojen käsittelyn arviointia: oikeusperusteella määritellään rekisteröidylle käsittelyn tarkoitus, laajuus ja sisältö.

Laillinen peruste on tavanomaisimmin tietosuoja-asetuksen 6(1) artiklassa ensimmäisenä mainittu rekisteröidyn antama suostumus.[112] Suostumuksen pyytämiseen, antamiseen ja muotoon liittyviä edellytyksiä on asetettu asetuksessa useita. Niin ikään suostumuksen hyödyntämiseksi on lisäedellytyksiä liittyen muun muassa rekisterinpitäjän osoitusvelvollisuuteen, suostumuksen antamista koskevaan pyyntöön, suostumuksen peruuttamiseen ja vapaaehtoisuuteen.[113] Lisäksi suostumukselle annettavia edellytyksiä on selvennetty asetuksen johdanto-osissa ja suostumukseen liittyviä tulkintaohjeita on koottu EU:n tietosuojaviranomaisista koostuvan työryhmän erillisiin ohjeisiin.[114]

Suostumuksella rekisteröity antaa oma-aloitteisesti hyväksyntänsä henkilötietojensa käsittelylle yhtä tai useampaa erityistä käyttötarkoitusta varten. Suostumus on huomioitu lisäksi EU:n perusoikeuskirjan 8 artiklassa. Tämä korostaa osaltaan rekisteröidyn tiedollisen itsemääräämisoikeuden toteutumista henkilötietojen suojan sääntelyn taustalla olennaisesti vaikuttavana tekijänä.[115] Suostumuksen olemassaolon ja pätevyyden olemassaolon osoittaminen kuuluu rekisterinpitäjälle. Suostumuksen olemassaolon osoittaminen ja sen saantiin liittyneet olosuhteet tulee voida todentaa jälkikäteen. Tämä rekisterinpitäjällä oleva näyttövelvollisuus koskee yleisesti myös muitakin lainmukaisia käsittelyperusteita.[116]

Suostumuksen lisäksi oikeusperuste voi TSA 6 artiklan perusteella syntyä tarpeesta sellaisen sopimuksen tekemiseksi tai täytäntöönpanemiseksi, jossa rekisteröity on osapuolena, sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä, rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi, rekisteröidyn tai toisen

[112] TSA 6(1)(a) artikla.
[113] TSA 7 artikla.
[114] WP 259 sekä ohje EDPB 2020.
[115] Voutilainen 2019, s. 164.
[116] TSA 5(2) artikla. Ks. Voutilainen 2019, s. 164 ja Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 100.

luonnollisen henkilön elintärkeiden etujen suojaamiseksi, yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi taikka oikeutetun edun toteuttamiseksi. Oikeutetun edun perusteeseen nojautuminen ei kuitenkaan ole mahdollista silloin, kun henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjättävät tällaiset edut ja erityisesti, jos rekisteröity on lapsi.[117]

3.5 Henkilötietoja sisältävän datan siirtämisen ja luovuttamisen eroista

Datan jakamiselle toimijoiden kesken ei tällä hetkellä ole yleistä sääntelykehystä, joka tekisi datan jakamisesta sen tapauskohtainen rooli ja luonne huomioiden riittävän turvallista.[118] Henkilötietojen luovuttaminen on yksi henkilötietojen käsittelyn muoto. Luovuttaminen voi tietosuoja-asetuksen mukaan olla tietojen siirtämistä, levittämistä tai tietojen asettamista muutoin saataville.[119]

Datan jakaminen ei esiinny terminä yleisessä tietosuoja-asetuksessa. Datan jakamisella voidaan tarkoittaa datan luovuttamista tai siirtämistä. Tietosuoja-asetuksen mukainen henkilötietojen luovutus tulee kyseeseen, kun rekisterinpitäjänä oleva toimija luovuttaa henkilötiedot kolmannelle osapuolelle käsiteltäväksi. Kolmannella osapuolella tarkoitetaan sellaista muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää ja henkilöä, jolla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.[120] Rekisterinpitäjä voi myös luovuttaa henkilötiedot kolmannelle osapuolelle siten, että tiedot vastaanottavasta osapuolesta tulee henkilötietojen uusi rekisterinpitäjä. Kolmas osapuoli ei näin ollen ole alusta alkaen ollut luokiteltavissa rekisterinpitäjäksi, vaan siitä tulee sellainen luovutuksen yhteydessä.

Henkilötietojen siirrosta taas on kyse esimerkiksi silloin, kun konserniyhtiön sisäisessä tietojen siirrossa tietoja siirtävä yhtiö tekee päätökset tietojen osalta ja tietoja vastaanottava yhtiö toimii vain henkilötietojen käsittelijänä, ei rekisterinpitäjänä. Tällöin tietojen käsittely ulkoistetaan esimerkiksi yhtiön rekisterin teknistä ylläpitoa varten, mutta tietoja koskeva päätösvalta ja tietojen käyttötarkoitus säilyy edelleen tiedot siirtäneellä yhtiöllä.[121]

[117] TSA 6(1)(f) artikla.
[118] Sitra 2022, s. 16.
[119] TSA 4(2) artikla.
[120] TSA 4(10) artikla.
[121] Ks. Hanninen ym. 2017, s. 93–94

Konsernin sisäpuolella tapahtuva henkilötietojen siirto voi tarkoittaa esimerkiksi tietojen tallentamisesta yhteiseen tietokantaan. Henkilötietoja käsitellään yhä rekisterinpitäjän lukuun, vaikka kyseessä olisi eri palveluntarjoaja.[122]

Olennaista henkilötietojen luovutuksen ja siirtämisen erossa on siis se, missä asemassa tietoja eteenpäin antava yritys sekä vastaanottava yritys ovat, ja minkä aseman ne tietojen luovutuksen jälkeen saavat. Henkilötietojen siirtäminen on laajempi käsite kuin henkilötietojen luovuttaminen.[123] Eron tekeminen näiden toimintojen välille vaikuttaa siihen, mitä edellytyksiä henkilötietojen luovutukselle tai siirtämiselle voidaan tietoja vastaanottavan yrityksen kannalta tietosuoja-asetuksen nojalla asettaa. Henkilötietojen luovutus ja siirtäminen edellyttävät käsittelytoimenpiteinä aina tietosuoja-asetuksen noudattamista kokonaisuudessaan, tietosuojaperiaatteet ja oikeusperusteet huomioiden. Eroja kuitenkin on sen suhteen, toimiiko yritys rekisterinpitäjänä vai ei. Toisin kuin henkilötietojen rekisterinpitäjänä toimiva yritys, henkilötietojen käsittelijä ei vastaa itsenäisesti henkilötietojen käsittelystä ja tietosuoja-asetuksen toteutumisesta toimiessaan rekisterinpitäjän lukuun.[124]

Henkilötietojen luovutus siten, että tiedot vastaanottavasta yrityksestä tulee itsenäisesti toimiva rekisterinpitäjä, edellyttää, että luovutuksensaajalla on tietoja luovuttavan rekisterinpitäjän lisäksi laillinen peruste henkilötietojen keräämiselle ja käsittelylle. Laillinen peruste on yleisimmin rekisteröidyn antamana suostumus, mutta suostumuksen lisäksi peruste voi syntyä esimerkiksi tarpeesta sopimuksen täytäntöönpanemiseksi tai oikeutetusta edusta. Yrityksen luovuttaessa henkilötietoja toiselle yritykselle, tulee kyseeseen yleensä luovutuksesta tehty kirjallinen sopimus. Sopimus ei välttämättä ole nimenomaisesti ”luovutussopimus” vaan esimerkiksi yhteistyösopimus. Joka tapauksessa näistä luovutus- tai yhteistyösopimuksista ei säädetä tietosuoja-asetuksessa, vaan ne kuuluvat yleisen sopimuskäytännön alaan.[125]

Eron tekeminen henkilötietojen siirtämisen ja luovuttamisen välillä ei kuitenkaan ole yksinkertaista, ja tietosuoja-asetuksen voimaantulon jälkeen ovat jopa henkilötietojen käsittelyyn liittyvät riitatilanteet ja erimielisyydet lisääntyneet.[126]

---

[122] Pitkänen – Tiilikka – Warma 2013, s. 183
[123] Pitkänen – Tiilikka – Warma 2013, s. 52.
[124] Hanninen ym. 2017, s. 93–95.
[125] Hanninen ym. 2017, s. 95.
[126] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 650.

3.6 Datan luovuttamista koskeva sääntely tietosuoja-asetuksessa

Tietosuoja-asetus mahdollistaa tietojen luovuttamisen ainoastaan tiettyjen henkilötietojen käsittelytoimenpiteenä. Nämä toimenpiteet voivat perustua joko rekisterinpitäjän itsensä tekemälle tietosuoja-asetuksen oikeusperusteen mukaiselle toiminnalle tai rekisteröidyn tekemään pyyntöön häntä itseään koskevien tietojen siirtämiseksi rekisterinpitäjän järjestelmästä toiseen. Ensin mainitulla tarkoitetaan rekisterinpitäjänä olevan toimijan vapaaehtoista datan siirtämistä yhtiöltä toiselle. Toimi koskee rekisterinpitäjän itsensä keräämiä ja omaa liiketoimintaa varten käsiteltyjä henkilötietoja. Luovuttaminen edellyttää tietosuoja-asetuksen noudattamista kaikilta osin ja perustuu yhtiön päätäntävallalle.[127]

Tietojen luovuttaminen rekisteröidyn pyynnöstä rajautuu taas rekisteröidylle tietosuoja-asetuksella annettuihin oikeuksiin. Ainoastaan rekisteröity voi saada tietonsa siirretyksi toiseen yhtiöön. Kolmannen osapuolen roolissa oleva yhtiö ei näitä tietoja voi määrätä, saati pyytää samalla tavoin siirrettäväksi. Tietojen siirrettävyys edellyttää lisäksi, että se on teknisesti mahdollista.[128] Miksi rekisteröity sitten oma-aloitteisesti pyytäisi tietojensa siirtämistä toiselle rekisterinpitäjälle? Sääntelyn tarkoituksena on antaa rekisteröidylle enemmän kontrollia omien henkilötietojen osalta.[129] Myös OECD:n taustamuistiossa liittyen massadatan rooliin kilpailuoikeudellisessa kontekstissa on katsottu, että jos kuluttajilla olisi sosiaalisissa verkostoissa mahdollisuus siirtää itseään koskevia kerättyjä tietoja eri sivustojen välillä, voisi se edistää toimijoiden välistä kilpailua markkinoilla ja rohkaista uusia yrityksiä tulla mukaan markkinoille.[130] Ongelmaksi on kuitenkin muodostunut se, etteivät niin yritykset kuin yksilötkään ole olleet riittävän motivoituneita jakamaan dataansa muiden toimijoiden kanssa. Tämä taas on osaltaan johtanut edelleen siihen, ettei järjestelmät datan jakamisen ja luovuttamisen suhteen ole kehittyneet riittävästi.[131]

Henkilötietojen siirrettävyyden osalta tietosuoja-asetuksessa on myös erilliset edellytykset tilanteisiin, joissa tietoja siirretään kolmansiin maihin tai kansainvälisille järjestöille.[132] Kyseessä on tietosuoja-asetuksen mukainen yrityksen päätäntävallan alainen tietojen siirto,

[127] Ks. Hanninen ym. 2017, s. 93–94.
[128] TSA 20 artikla ja WP 242, s. 5.
[129] WP 242, s. 4.
[130] OECD 2016, s. 27.
[131] Sitra 2022, s. 16.
[132] TSA V luku.

eikä tiettyyn lakisääteiseen määräykseen perustuva velvollisuus, mistä syystä aihealuetta ei ole tarpeen käsitellä tämän lyhyen esittelyn jälkeen enempää. Henkilötietojen siirtämisessä kolmansiin maihin tai kansainvälisille järjestöille edellytetään, että tietojen siirtäminen tapahtuu noudattaen tietosuoja-asetusta, ja että tietojen siirtäminen perustuu tietosuojan riittävyyttä koskevaan Euroopan komission päätökseen, rekisterinpitäjän tai tietojen käsittelijän toteuttamien asianmukaisina pidettyjen suojatoimien soveltamiseen, yritystä koskevien sitovien säännösten noudattamiseen tai tiettyihin poikkeuksiin, jotka koskevat erityistilanteita.[133]

3.6.1 Tietopyyntöön perustuva henkilötietojen luovutus

Henkilötietojen luovutus voi perustua rekisteröidyn tekemälle tietopyynnölle saada häntä itseään koskevat tiedot siirretyksi. Tietosuoja-asetus antaa 20 artiklassa rekisteröidylle oikeuden siirtää häntä koskevat henkilötiedot yhdeltä rekisterinpitäjältä toisen rekisterinpitäjän järjestelmään. Edellytyksenä on, että käsittely perustuu rekisteröidyn antamaan suostumukseen tai sopimuksen täytäntöönpanemiseksi ja näiden lisäksi käsittely suoritetaan automaattisesti. Luovutustoimi rajoittuu rekisteröidyn itse tekemälle pyynnölle henkilötietojen luovutuksesta, eikä perustu rekisterinpitäjän aloitteeseen luovuttaa hallussaan olevia henkilötietoja. Tietosuojatyöryhmä on ohjeissaan tarkentanut datan siirrettävyyden edellytyksiä kyseisessä tilanteessa.[134]

Rekisteröidyn omalle pyynnölle perustuva henkilötietojen luovutus on tietoja luovuttavan rekisterinpitäjän vastuuseen nähden kaksijakoinen. Kun rekisteröity pyytää henkilötietojensa siirtämistä toiselle rekisterinpitäjälle, ei pyynnön saanut rekisterinpitäjä ole vastuussa siirrettävyyden prosessista taikka tietoja vastaanottavan rekisterinpitäjän henkilötietojen käsittelystä. Rekisterinpitäjä ei ole valinnut tietojen vastaanottajaa, eikä siten ole vastuussa tältä osin siitä, että tiedot vastaanottava toimija noudattaa tietosuojalainsäädäntöä. Rekisterinpitäjä toimii tilanteessa siis rekisteröidyn puolesta.[135]

Tietosuojatyöryhmä on kuitenkin ohjeessaan tarkentanut, että rekisteröidyn puolesta toiminen edellyttää, että rekisterinpitäjä asettaa suojatoimia sen varmistamiseksi, että kyseessä

[133] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 391.
[134] Ks. WP 242.
[135] WP 242, s. 6.

on tosiasiallisesti tiedot, jotka rekisteröity itse haluaa siirrettävän. Tämä voidaan toteuttaa esimerkiksi hankkimalla rekisteröidyltä erillinen tietosuoja-asetuksen mukainen suostumus ennen tietojen luovuttamista.[136] Rekisterinpitäjällä on vastuu siltä osin kuin sen on varmistuttava siitä, että tietosuojaperiaatteita noudatetaan sen omassa toiminnassaan.[137] Ennen tietojen käsittelyn aloittamista tehtävä tietojen käyttötarkoituksen ilmoittaminen rekisteröidylle kuuluu kuitenkin tiedot vastaanottavalle yritykselle, jonka tulee huolehtia omassa toiminnassaan luonnollisesti tietosuojaperiaatteiden toteutumisesta.[138] Tiedot vastaanottavasta yrityksestä tulee siten uusi tietosuoja-asetuksen mukainen rekisterinpitäjä. Oikeus tietojen siirtämiseen sujuvasti edellyttää näin ollen myös vastaanottavalta uudelta rekisterinpitäjältä valmistautumista tietojen käsittelylle.[139]

Vaikka rekisterinpitäjällä ei siis varsinaista vastuuta tiedot vastaanottavan toimijan suuntaan ole, on tietosuojatyöryhmän ohjeista tulkittavissa, että edellisen rekisterinpitäjän tulee huolehtia oman toimintansa tietosuojasta siihen saakka, kunnes tiedot on saatu tietoturvallisesti siirrettyä toiselle toimijalle.

3.6.2 Rekisteröidyn informointi henkilötietojen käsittelyssä

Rekisterinpitäjällä on rekisteröityä kohtaan informointivelvollisuus, jonka nojalla rekisterinpitäjän tulee informoida rekisteröityä muun muassa henkilötietojen käsittelyperusteesta sekä siitä, millaisia tietoja tullaan keräämään ja mihin tarkoitukseen tietoja käsitellään. Rekisterinpitäjän on myös informoitava rekisteröityä aiotuista käsittelytoimista ja siitä, mille eri tahoille tietoja on tarkoitus siirtää tai luovuttaa rekisterinpitäjän toimesta.[140] Henkilötietojen luovuttaminen ja siirtäminen edellyttää siten informointivelvollisuuden täyttymistä. Sen tarkoitus on täsmentää tietosuojaperiaatteenakin taattua ja aiemmin käsiteltyä läpinäkyvyyden vaatimusta. Sääntelyllä tähdätään siihen, että rekisteröidyllä on jatkuvasti ymmärrys siitä, miten ja mihin tarkoituksiin hänen henkilötietojaan käsitellään.[141]

Rekisterinpitäjällä on valinnanvapaus siitä, miten se informointivelvollisuutensa täyttää käytännössä. Tietosuoja-asetus asettaa rajoituksia ja tarkennuksia velvollisuuden sisällölle,

[136] WP 242, s. 6.
[137] WP 242, s. 6 sekä Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 244.
[138] WP 242, s. 6.
[139] WP 242, s. 6–7.
[140] TSA 13 ja 14 artiklat.
[141] Ks. Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 174.

mutta tiettyä muotoa tai keinoa ei ole määrätty. Informointivelvollisuuden täyttyminen on siis pitkälti rekisterinpitäjän omalla vastuulla. Jotta informointi voidaan asetuksessa edellytettävin tavoin suorittaa oikein, on rekisterinpitäjän kannalta oleellista, että rekisterinpitäjä itse on tietoinen omassa toiminnassaan suoritettavan henkilötietojen käsittelystä kokonaisuudessaan.[142] Tietosuojavaltuutetun toimisto onkin ohjeistanut rekisterinpitäjiä kiinnittämään erityistä huomiota informointivelvollisuuden täyttämisessä käsittelyn tarkoituksen määrittämiseen. Tietosuojavaltuutetun toimiston antaman ohjeistuksen mukaan rekisteröidyllä on oltava selkeä käsitys kaikista häntä koskevien tietojen käyttötarkoituksista.[143]

[142] Ks. Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 175–176 ja Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille käsittelyn kertomisesta rekisteröidylle, Tietosuojavaltuutetun toimiston verkkosivut, Rekisteröidyn informointi, kohta Kerro käsittelystä rekisteröidylle, 1. Kartoita henkilötietojen käsittelyn kokonaiskuva.

[143] Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille käsittelyn kertomisesta rekisteröidylle, Tietosuojavaltuutetun toimiston verkkosivut, Rekisteröidyn informointi, kohta Kerro käsittelystä rekisteröidylle, Informaation ymmärrettävyys ja läpinäkyvyys.

4 DIGIMARKKINASÄÄDÖKSEN TAVOITE JA PERUSTA

4.1 Kilpailuoikeudellinen lähtökohta digimarkkinasäädöksen tavoitteena

EU:n uuden digimarkkinasäädöksen tarkoituksena on täydentää EU:n kilpailusääntöjä puuttumalla epäoikeudenmukaisiin käytäntöihin, joihin ei ole kyetty aiemmin puuttumaan kilpailuoikeudellisin keinoin ja voimassa olevin kilpailusäännöin. Portinvartijoiden harjoittamat toimet eivät joko kuulu laisinkaan kilpailusääntöjen soveltamisalaan tai niihin ei voida puuttua tehokkaasti.[144] Datan kontrolliin perustuvien markkinoiden määrittely ei ole saavuttanut yksimielisyyttä ja kilpailuoikeudellisten tulkintamenettelyjen käyttö ei ole ollut ajankäytöltään tehokasta.[145]

EU:n alueella jäsenmaiden kilpailua kontrolloidaan sisämarkkinaoikeuden avulla. Kilpailulainsäädännöllä puututaan markkinoilla toimivien yritysten kilpailua rajoittaviin toimiin. Perinteisesti kilpailuoikeuden keskeisiksi säännöksiksi EU:ssa on katsottu SEUT 101 artiklan kartellikiellot, SEUT 102 artiklan määräävän markkina-aseman väärinkäytön kielto ja säännökset liittyen yrityskauppavalvontaan.[146]

Yrityksen määräävän markkina-aseman merkitystä voidaan lähestyä kansallisen kilpailulain (948/2011) määritelmästä käsin. Kilpailulain 4 §:n 2 kohdan mukaan yrityksen määräävä markkina-asema tarkoittaa yhdellä tai useammalla elinkeinonharjoittajalla taikka elinkeinonharjoittajien yhteenliittymällä olevaa koko maan tai tietyn alueen kattavaa yksinoikeutta tai muuta määräävää asemaa tietyillä hyödykemarkkinoilla. Tällaisen aseman omaava yritys ohjaa merkittävästi hyödykkeen hintatasoa tai toimitusehtoja taikka vaikuttaa vastaavalla muulla tavalla kilpailuolosuhteisiin tietyllä tuotanto- tai jakeluportaalla.

Markkinoiden rakenteen kannalta määräävään markkina-asemaan noussut yritys hallitsee isoa osaa markkinoista ja sen kilpailijat ovat huomattavasti yritystä pienempiä. Määräävässä markkina-asemassa olevalla yrityksellä on lisäksi asiakkaidensa riippuvuussuhde. Yrityksen taloudellinen valta aiheuttaa sen, että yritys voi yksinään omalla toiminnallaan vaikuttaa hyödykkeen hintatasoon ja myös sulkea kilpailijoita markkinoiden ulkopuolelle ilman, että

[144] DMA:n johdanto 5 kohta.
[145] Kuoppamäki 2018, s. 272 ja ks. DMA:n johdanto 5 kohta.
[146] Raitio 2016, s. 699–700.

se ainakaan välittömästi menettää asemaansa kilpailijoilleen.[147] Määräävän markkina-aseman saavuttaminen itsessään ei ole kiellettyä, mutta kilpailulain 7 §:n perusteella sen väärinkäyttö puolestaan on.

Markkinoiden digitalisoituminen sekä teknologian ja talouden muutokset ovat aiheuttaneet kilpailuoikeudelle uusia haasteita. Osaltaan kyse on vanhojen liiketoimintamallien, kuten perinteisten kivijalkamyymälöiden, korvaantumisesta verkkokauppatoiminnalla, mutta osaltaan kokonaan uudenlaisesta jakamistalouden liiketoimintamallista, joka on rakennettu digitaalisen palvelualustan ympärille. Näillä alustoilla toimii erilaiset käyttäjäryhmät, kuluttajat ja myyjät. Tällainen toiminta perustuu pitkälti algoritmien ja datan hallintaan.[148]

Määräävään markkina-asemaan noussut yritys voi kerätä asiakasdataa suoraan omilta asiakkailtaan sekä välillisesti sen tarjoamaa alustapalvelua hyödyntäviltä yrityskäyttäjiltä niiden tekemien sopimusten ja rekisteröityjen antamien suostumuksien perusteella.[149] Yrityksen keräämä data vaikuttaa yrityksen käyttämien algoritmien tehokkuuteen, ja sitä kautta yrityksen liiketoiminnan kehittämiseen ja tulojen kasvattamiseen. Algoritmien ominaisuuksiin kuuluu itseoppivuus, ja siten ne kehittyvät ja oppivat sitä paremmaksi, mitä enemmän niillä on dataa hyödynnettävänä.[150] Kun algoritmien toiminta kehittyy, palveluita käytetään ja hyödykkeitä kulutetaan yhä enemmän ja useammin, mikä puolestaan tuottaa lisää dataa ja kehittää jälleen algoritmin toimintaa. Uudet toimijat eivät kykene kilpailemaan ja saavuttamaan samanlaista palvelun ja tuotteiden tasoa tiedon puutteen vuoksi. Suurten datamassojen hallinta tuo yritykselle myös erilaisia uusia oivalluksia, jotka ovat hyödynnettävissä jälleen uudella tavalla kuluttajien suuntaan. Myöskään tätä etua ei pienemmillä toimijoilla ole.[151]

Kilpailuoikeus on muuttuvasta ympäristöstä huolimatta oikeudenalana joustava. Sen soveltaminen erilaisilla toimialoilla kuitenkin edellyttää, että kyseisen sovellettavaksi tulevan alan erityisolosuhteet osataan analysoida riittävän tarkasti ja yksityiskohtaisesti, jolloin kilpailuoikeus kykenee sopeutumaan uusiin olosuhteisiin.[152] Tämä on otettava huomioon niin

[147] Kuoppamäki 2018, s. 9 ja 252.
[148] Kuoppamäki 2018, s. 19.
[149] Kuoppamäki 2018, s. 276.
[150] Kuoppamäki 2018, s. 20–21.
[151] JRC 2021, s. 20.
[152] Kuoppamäki 2018, s. 21.

tietosuojaoikeudellisten kuin digitalouden tuomien uusien kysymysten arvioimisessa kilpailuoikeudellisesta näkökulmasta.

4.2 EU:n tietosuojakysymykset ja kilpailuoikeus

Henkilötietojen suoja kuuluu osaksi yksityisyyden suojaa, ja yksityisyyden suojan tärkeys kytkeytyy tietosuojakysymyksiin esimerkiksi EU-oikeudessa ja EU-tuomioistuimen ratkaisukäytännössä. Tämä yhteys on noussut arvioitavaksi myös kilpailuoikeudellisessa merkityksessä, vaikka sitä ei täysin selvänä voidakaan pitää.[153] Kilpailuoikeudellisesta näkökulmasta on arvioitu sitä, miten datan määrä ja henkilötietojen käsittely vaikuttavat dataa kontrolloivan yrityksen kilpailulliseen toimintaan ja määräävän markkina-aseman muodostumiseen yleisestikin.[154]

Kilpailuoikeuden ja tietosuojakysymysten välinen yhteys on herättänyt uudelleen keskustelua digitaalisten markkinoiden kehittyessä etenkin Euroopassa ja EU-tuomioistuimen ratkaisukäytännössä. Ratkaisussa *Asnef-Equifax* EU-tuomioistuin esimerkiksi totesi, etteivät tietosuojakysymykset kuulu sellaisenaan kilpailulainsäädännön vaan tietosuojasääntelyn soveltamisalaan.[155] Lisäksi Euroopan komissio katsoi vielä vuonna 2014 tekemässään päätöksessään *Facebook/WhatsApp*, ettei tietosuojakysymykset kuulu Euroopan komission kilpailupääosastolle, vaan tietosuojaviranomaisille.[156] Sen sijaan *Microsoft/LinkedIn*-yrityskauppatapauksessa komissio otti päätöksessään taipuvaisemman linjan huomioidessaan yksityisyyden suojaan liittyvät näkökohdat arvioinnissaan.[157]

Suuntaukseen on myös tulossa uusia linjauksia. Niin kutsutussa Saksan *Facebook*-tapauksessa oli kyse kilpailuoikeudellisesta päätöksestä, jossa kansallinen kilpailuviranomainen otti nimenomaisesti huomioon yksityisyyden suojan.[158] Tapauksessa Saksan kilpailuviranomainen Bundeskartellamt katsoi Facebookin käyttäneen väärin määräävää markkina-asemaansa asettamalla käyttäjilleen hyväksyttäviä sopimusehtoja, joiden mukaan Facebook

[153] Lehtioksa – Ljungman – Vainio 2019, s. 865–866.
[154] Lehtioksa – Ljungman – Vainio 2019, s. 866.
[155] Asia C-238/05 (ECLI:EU:C:2006:734) - Asnef-Equifax, kohta 63.
[156] Euroopan komission päätös, 3.10.2014, COMP/M.7217 – Facebook/WhatsApp, kohta 164.
[157] Euroopan komission päätös 6.12.2016, M.8124 – Microsoft/LinkedIn, ks. arvioinnista esim. kohdat 176 ja 350. Arvioidessaan markkinoilla vallitsevaa tilannetta ja palveluntarjoajien sulkemista pois markkinoilta, komissio korosti esimerkiksi kilpailevan palveluntarjoajan tarjoavan käyttäjilleen paremman yksityisyyden suojan.
[158] Kerber – Zolna 2022, s. 2 ja Bundeskartellamt lehdistötiedote 7.2.2019.

pystyi yhdistelemään omistamiltaan yhtiöiltä sekä kolmansien osapuolten verkkosivuilta ja sovelluksista keräämänsä dataa.[159] Asian edetessä Saksan Düsseldorfin ylemmälle alueelliselle tuomioistuimelle, teki se EU-tuomioistuimelle asiassa ennakkoratkaisupyynnön. Siinä pyydetään selvittämään sitä, että voiko kansallinen kilpailuviranomainen soveltaa kilpailuoikeudellisen väärinkäytön valvonnan yhteydessä yleistä tietosuoja-asetusta ja antaa sen nojalla väärinkäyttöä koskevan päätöksen.[160] Asian käsittely on vielä kesken, eikä lopullista ratkaisua ole annettu. Ratkaisu tulee kuitenkin tuomaan esille EU-tuomioistuimen linjauksen muun muassa siihen, miten laajasti voidaan ottaa tietosuojaoikeudellista sääntelyä huomioon kilpailulainsäädännön valvonnassa ja täytäntöönpanoon kohdistuvassa viranomaisten toiminnassa.[161] Ratkaisu tulee vaikuttamaan myös tietosuoja-asetuksen mukaisen suostumuksen arvioimiseen ja määrittämiseen kilpailuoikeudellisesti.[162]

Mikäli tietosuojaan liittyvillä kysymyksillä arvioidaan olevan kilpailuoikeudellista merkitystä, voidaan ne jatkossa ottaa vielä aiempaa paremmin huomioon kilpailuoikeudellisissa ratkaisuissa.[163] Esimerkiksi jo sen perusteella, että yrityksen dataa ja tietosuojaa koskevat ehdot ja rajoitukset ovat nousseet keskeisiksi kilpailutekijöiksi digitaalisilla markkinoilla toimivan yrityksen menestykseen, tulisi dataan ja tietosuojaan liittyvät kysymykset huomioida kilpailuoikeudellisesti.[164] Lisäksi tiedon itsensä osalta olennaisena kysymyksenä on se, tuleeko tiedon itsessään olla kilpaileva hyödyke ja siten kilpailulainsäädännön piirissä. Toisaalta voidaan myös pohtia sitä, tulisiko sääntelyssä kuitenkin tiedon itsensä sijaan keskittyä tiedon saatavuuteen ja tiedon sisällön arviointiin.[165]

Kilpailu- ja tietosuojalainsäädännön välinen suhde ei siten ole vielä saavuttanut riittävän yhteneväistä linjaa ja niiden suhteen voidaan yhä arvioida olevan epäselvä. Keskustelu näiden kahden oikeudenalan yhteentoimivuudesta tulee jatkamaan kasvuaan myös osana EU:n ratkaisukäytäntöä erityisesti välittömässä lähitulevaisuudessa, kun digimarkkinasäädöksen sekä muiden EU:n digiuudistuksen säädösten soveltaminen alkaa.[166]

[159] Bundeskartellamt lehdistötiedote 7.2.2019.
[160] Asia C-252/21 ennakkoratkaisupyyntö – Meta Platforms and Others/Bundeskartellamt, 22.4.2021.
[161] Ks. Wasastjerna 2018, s. 31–32.
[162] Kerber – Zolna 2022, s. 23.
[163] Kuoppamäki 2018, s. 420.
[164] Kuoppamäki 2018, s. 420.
[165] Marini-Balestra – Tremolada 2017, s. 342–343.
[166] Kuoppamäki 2018, s. 318.

5 DATAN LUOVUTTAMINEN DIGIMARKKINASÄÄDÖKSESSÄ

5.1 Portinvartijoiden toimintaan puuttuminen digimarkkinasäädöksen avulla

Yleinen tietosuoja-asetus ei aseta suoranaista mahdollisuutta siihen, että rekisterinpitäjä velvoitettaisiin luovuttamaan dataa toiselle yritykselle, joka on jo valmiiksi rekisterinpitäjä tai siitä tulee luovutuksen myötä uusi rekisterinpitäjä. Sen sijaan tietosuoja-asetus mahdollistaa edellä esitetyin tavoin henkilötietoja sisältävän datan luovuttamisen rekisteröidyn omasta pyynnöstä. Lisäksi tietosuoja-asetus mahdollistaa henkilötietoja sisältävän datan luovuttamisen rekisterinpitäjän vapaaehtoisena toimena. Toiminta perustuu kuitenkin ainoastaan rekisteröidyn oma-aloitteisuuteen – ulkoapäin tulevaa velvoitetta toimintaan ei ole. Tietosuoja-asetuksen sääntely ei siten ole mahdollistanut rekisterinpitäjän ja rekisteröidyn välisen suhteen ulkopuolelta tulevaa puuttumista rekisterinpitäjän toimintaan, mikä on ongelmallista, kun kyseessä on kilpailullisesti merkittävä toimija.

Digimarkkinasäädöksen kilpailuoikeudellinen perusta on vahva. Sillä puututaan datan siirrettävyyttä koskevaan ongelmalliseen tilanteeseen ja asetetaan portinvartijoille velvollisuuksia liittyen niiden toimittamaan datan keräämiseen, hallinnointiin ja käsittelyyn. Lisäksi sillä luodaan yhtiölle datan siirrettävyyteen kohdistuva velvollisuus luovuttaa dataa kilpailijoidensa käyttöön. Kyseessä on tällöin tietojen luovuttaminen toisen toimijan käyttöön niin, että tarjotaan toiselle toimijalle pääsy tietoihin.

Digimarkkinasäädöksessä asetetaan III luvun 5 ja 6 artikloissa portinvartijoille velvollisuuksia kielletyn käytöksen ja kiellettyjen toimenpiteiden osalta. Näiden velvoitteiden tarkoituksena on vähentää portinvartijoiden yksinomaista määräysvaltaa keräämäänsä dataan ja siten saada vähennettyä niiden vaikutusvaltaa markkinoilla.[167] Datan kontrolliin liittyy sen luovuttamisen ja dataan pääsyn sallimisen lisäksi esimerkiksi portinvartijalle asetettu kielto suosia omia palveluitaan sekä kielto yhdistää asianomaisesta ydinalustapalvelusta peräisin olevia henkilötietoja muista ydinalustapalveluista tai mistä tahansa muusta portinvartijan tarjoamasta palvelusta oleviin tai kolmannen osapuolen palveluista saatuihin henkilötietoihin. DMA:ssa jätetään tähän kuitenkin mahdollisuus, mikäli loppukäyttäjälle on

[167] JRC 2021, s. 20.

annettu tätä koskeva valinnanmahdollisuus ja hän on antanut suostumuksensa yleisessä tietosuoja-asetuksessa tarkoitetulla tavalla.[168]

Sen lisäksi, että asetuksella luodaan portinvartijalle velvollisuus myöntää yrityskäyttäjille pääsy dataan, kieltää asetus portinvartijaa ylipäätään käyttämästä yrityskäyttäjien kanssa kilpaillen mitään dataa, joka ei ole julkisesti saatavilla ja joka on peräisin siitä, että kyseiset yrityskäyttäjät käyttävät tarjottuja ydinalustapalveluja. Tähän dataan katsotaan kuuluvan yrityskäyttäjien sekä yrityskäyttäjien asiakkaiden tuottama ja antamaa data.[169]

5.2 Luovutusvelvollisuuden sisältö ja edellytykset

Digimarkkinasäädöksessä loppukäyttäjälle myönnettävä pääsy omiin tietoihinsa täydentää tietosuoja-asetuksessa olevaa rekisteröidyn oikeutta siirtää tiedot toiselle toimijalle.[170] Yrityskäyttäjälle myönnettävässä pääsyssä taas on kyse uudesta velvollisuudesta, josta ei ole edeltäviä määräyksiä tietosuoja-asetuksessa. Portinvartijoille asetettujen velvoitteiden soveltamisessa tulee kuitenkin kaikilta osin varmistaa tietosuoja-asetuksen samanaikainen noudattaminen.[171]

Yrityskäyttäjien tietojen luovutus perustuu DMA 6(10) artiklaan, jonka mukaan portinvartijan on tarjottava yrityskäyttäjille ja yrityskäyttäjän valtuuttamille kolmansille osapuolille pyynnöstä ja maksutta tehokas, korkealaatuinen, jatkuva ja reaaliaikainen pääsy ja käyttömahdollisuus yhdistettyihin ja yhdistämättömiin tietoihin, mukaan lukien henkilötiedot. Artiklan mukaan tietojen on oltava sellaisia, mitä yrityskäyttäjät ja kyseisten yrityskäyttäjien tarjoamia tuotteita tai palveluja käyttävät loppukäyttäjät antavat tai tuottavat asianomaisten ydinalustapalvelujen käytön tai niiden yhteydessä tarjottujen tai niitä tukevien palvelujen käytön yhteydessä. Henkilötietojen osalta portinvartijan on tarjottava DMA 6(10) artiklan mukainen pääsy henkilötietoihin ja mahdollisuus käyttää niitä vain, jos tiedot liittyvät suoraan loppukäyttäjien toteuttamaan, sellaisten tuotteiden ja palvelujen käyttöön, joita asianomainen yrityskäyttäjä tarjoaa kyseessä olevan ydinalustapalvelun kautta, ja kun loppukäyttäjät antavat suostumuksensa tällaiseen tietojen jakamiseen.

---

[168] DMA 5(2)(b) artikla.
[169] DMA 6(2) artikla.
[170] TSA 20 artikla.
[171] DMA:n johdanto 65 kohta.

Tietojen luovuttamisessa on siten kyse toimesta, jolla portinvartija tarjoaa yrityskäyttäjille ja niiden valtuuttamille kolmansille osapuolille tosiasiallisen pääsyn ja käyttömahdollisuuden tietoihin.[172] Yrityskäyttäjän valtuuttamat kolmannet osapuolet käsittelevät henkilötietoja yrityskäyttäjien lukuun eli toimivat henkilötietojen käsittelijöinä, eivät rekisterinpitäjinä. Heidän välinen yhteistyönsä voi perustua esimerkiksi sopimukselle.[173] Yrityskäyttäjä voi olla valmiiksi rekisterinpitäjä tai siitä voi luovutuksen yhteydessä tulla rekisterinpitäjä.

Toimen tulee perustua portinvartijalle osoitettuun pyyntöön ja sen on oltava yrityskäyttäjälle maksutonta. Portinvartija ei siis saa rahallista vastinetta tietojen luovuttamiselle. Pääsy tietoihin sisältää myös pääsyn saman portinvartijan tarjoamien muiden palvelujen toimittamiin ja tuottamiin tietoihin siltä osin kuin pääsy kytkeytyy erottamattomasti asianomaiseen pyyntöön ja kyseessä on sama yrityskäyttäjä ja tämän loppukäyttäjät. Tähän luetaan mukaan myös ydinalustapalvelujen yhteydessä tai niiden tukemiseksi tarjotut palvelut.[174] Asetuksessa vaadittu pääsy tietoihin kattaa siis varsin laajasti portinvartijan kontrollissa olevaa dataa, riippumatta siitä, onko tiedot peräisin suoraan portinvartijan tarjoamasta palvelusta tai sen yhteydessä tarjoamasta palvelusta. Tiedot on kuitenkin rajattu vain kyseessä olevan yrityskäyttäjän toiminnassa esiintyviin tietoihin, eikä siis kaikkiin tietoihin, joita portinvartija olisi saanut esimerkiksi joltain toiselta yrityskäyttäjältä.[175]

Erikseen portinvartijaa kielletään asettamasta sopimusperusteisia tai muita rajoituksia tiedon luovuttamisen estämiseksi. Henkilötietojen osalta portinvartijan on myös annettava yrityskäyttäjille mahdollisuus saada loppukäyttäjiltä edellytettävä suostumus tietojen saannille ja hakemiselle.[176] Velvoitteiden kiertämisestä säädetään tarkemmin asetuksen 13 artiklassa, joka asettaa portinvartijalle velvollisuuden varmistaa muun muassa datan luovuttamiseen yrityskäyttäjälle liittyen, että luovutusvelvoitetta noudatetaan täysimääräisesti ja tosiasiallisesti. Portinvartija ei saa kiertää määrättyjä velvoitteita, yrittää kiertää niitä tai käyttäytyä heikentämällä velvoitteiden noudattamista.[177]

[172] DMA:n johdanto 60 kohta.
[173] DMA:n johdanto 60 kohta ja TEM 2022, s. 30.
[174] DMA:n johdanto 60 kohta.
[175] JRC 2021, s. 22.
[176] DMA:n johdanto 60 kohta.
[177] DMA 13(4) ja 13(6) artiklat.

5.3 Henkilötiedot luovutusvelvollisuuden kohteena

Digimarkkinasäädöksessä on huomioitu, että portinvartijoiden käytännöillä, joilla ne keräävät ja käsittelevät suuria datamääriä, voi olla loppukäyttäjien tietosuojaan ja yksityisyyden suojaan liittyviä kielteisiä vaikutuksia.[178] Kilpailullisen tavoitteen lisäksi tietosuoja-asetus on saanut tärkeän roolin DMA:ssa ja sen merkitys on otettu huomioon asetuksen johdantoosion lisäksi yksittäisissä artikloissa. DMA korostaa siinä asetettujen velvoitteiden noudattamista siten, että samalla varmistetaan erityisesti tietosuoja-asetuksen noudattaminen.[179]

DMA 6(10) artikla mahdollistaa henkilötietojen luovuttamisen portinvartijan yrityskäyttäjille, eikä henkilötietoja ole siten rajattu pois uudesta asetuksesta. Henkilötietojen luovuttamiseen liittyy kuitenkin DMA:ssa ja TSA:ssa asetettuja erityisiä ehtoja. Luovutettaessa yrityskäyttäjälle henkilötietoja DMA 6(10) artiklan perusteella, tulee henkilötietojen liittyä suoraan sellaiseen loppukäyttäjien toteuttamaan tuotteiden ja palvelujen käyttöön, mitä yrityskäyttäjä tarjoaa portinvartijan alustapalvelun kautta. Lisäksi henkilötietojen luovutus edellyttää tietosuoja-asetuksen mukaisena oikeusperusteena loppukäyttäjän osalta suostumusta tietojen luovuttamiselle.

Suostumus tietojen jakamiselle viittaa portinvartijan puolelta toteutettavaan jakamistoimeen. Yrityskäyttäjän osalta tietojen vastaanottamiselle ja tulevalle käsittelylle ei vastaavasti ole asetettu tiettyä TSA:n mukaista käsittelyperustetta. Kun loppukäyttäjältä edellytetään suostumuksen antamista portinvartijan toimittamaan tietojen jakamiseen artiklan 6(10) nojalla, vaikuttaisi kuitenkin luontevalta, että myös yrityskäyttäjien suhteen oikeusperuste henkilötietojen käsittelylle kääntyisi tietosuoja-asetuksen mukaiseksi suostumukseksi.

Portinvartijaa kielletään käyttämästä sopimusperusteisia tai muita rajoituksia estääkseen yrityskäyttäjiä pääsemästä asianomaisiin tietoihin. Portinvartijan on myös annettava yrityskäyttäjille mahdollisuus saada loppukäyttäjiltä suostumus tietojen vastaanottamiselle ja hakemiselle, mikä tukee edellä mainittua käsitystä siitä, että suostumus voisi muodostua käytännöllisimmäksi oikeusperusteeksi yrityskäyttäjän henkilötietojen käsittelylle.[180] Kun otetaan huomioon tämä DMA:ssa asetettu lähtökohta suostumuksesta käsittelyperusteena, on

[178] DMA:n johdanto 72 kohta.
[179] DMA:n johdanto 65 kohta.
[180] DMA:n johdanto 60 kohta.

pidettävä epätodennäköisenä, että yrityskäyttäjän henkilötietojen käsittely perustuisi muille tietosuoja-asetuksen mahdollistamille oikeusperusteille. Jotta voidaan selvittää, soveltuuko suostumus käytännössä luovutusvelvollisuuden mukaiseen henkilötietojen käsittelyyn, täytyy suostumusta tarkastella lähempää oikeusperusteena sekä portinvartijan että yrityskäyttäjän näkökulmasta.

Lisäksi DMA edellyttää portinvartijaa vielä erikseen varmistamaan, että yrityskäyttäjä saa tarvitsemansa suostumuksen henkilötietojen keräämiseen, käsittelyyn, ristiin käyttöön ja jakamiseen, mikäli sellaista tietosuoja-asetuksen nojalla edellytetään. Portinvartija ei saa tehdä kyseisen suostumuksen saamisesta yrityskäyttäjille hankalampaa kuin omien palvelujensa osalta. Vaihtoehtoisesti portinvartijan tulee noudattaa EU:n tietosuojaa ja yksityisyyttä koskevia sääntöjä ja periaatteita muilla tavoin, esimerkiksi antamalla yrityskäyttäjille tarvittaessa asianmukaisesti anonymisoituja tietoja.[181] Näin suostumus ei näyttäydy kuitenkaan pakollisena, vaan olennaista on yrityskäyttäjän tukeminen luovutusvelvollisuuden täyttämiseksi onnistuneesti.

5.4 Portinvartijan osoitusvelvollisuus

Digimarkkinasäädöksessä asetetaan portinvartijalle osoitusvelvollisuus toteutettavista toimenpiteistä ja velvoitteiden noudattamisesta. Portinvartijan tulee varmistaa ja osoittaa, että se noudattaa sille asetettuja velvoitteita. Toteutettavilla toimenpiteillä tulee voida tehokkaasti saavuttaa velvoitteen ja asetuksen yleiset tavoitteet. Portinvartijan tulee varmistaa lisäksi, että sen kyseiset toimenpiteet toteutetaan sovellettavan lainsäädännön mukaisesti, erityisesti tietosuoja-asetuksen; sähköisen viestinnän tietosuojadirektiivin[182]; kyberturvallisuutta, kuluttajansuojaa ja tuoteturvallisuutta koskevan lainsäädännön sekä esteettömyysvaatimusten mukaisesti.[183]

Portinvartijoiden tulee noudattaa asetusta sisäänrakennetusti. Tämä edellyttää sitä, että asetuksen mukaiset noudatettavat toimenpiteet sisällytetään mahdollisimman laajalti osaksi portinvartijoiden teknistä suunnittelua.[184]

---

[181] DMA 13(5) artikla.
[182] Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi).
[183] DMA 8(1) artikla.
[184] DMA:n johdanto 65 kohta.

5.5 Digimarkkinasäädöksen yhteys datasäädökseen ja digipalvelusäädökseen

Digimarkkinasäädös on osa laajempaa EU:n uutta datan sääntelykokonaisuutta, johon lukeutuu digimarkkinasäädöksen ohella useampi muu uusi säädös. Digimarkkinasäädös on keskeisin sääntelykehys, kun kyseeseen tulee datan luovuttaminen yrityskäyttäjille velvollisuutena, mutta kokonaisuuden kannalta on tarpeen huomioida lyhyesti myös muita säädöksiä, jotka ulottavat vaikutuksensa etenkin suuriin teknologiayhtiöihin eli DMA:n mukaisiin portinvartijoihin.

Digimarkkinasäädöksen ohella EU:n laajempaan digitaalistrategiaan on sisältynyt datasäädös (Data Act, DA). Datasäädös ei sinänsä ulota sääntelyään varsinaisesti digimarkkinasäädöksen tavoin portinvartijoihin ja kilpailuoikeudellisiin tavoitteisiin, mutta turvaa oikeudenmukaisuutta etenkin kuluttajana toimivan yksilön näkökulmasta.[185] DA:n tarkoituksena on edistää tietojen saatavuutta ja käyttöä, sekä varmistaa datan saatavan arvon oikeudenmukainen jakaminen datatalouden toimijoiden kesken.[186]

Datasäädöksessä on kyse datan asettamisesta saataville (”*to make data available*”), jolla näyttäisi kuitenkin olevan samansuuntainen tarkoitus kuin digimarkkinasäädöksen datan luovutuksella tai pääsyllä dataan (”*access to data*”). Datasäädöksen säännöksillä täydennetäänkin TSA 20 artiklan mukaista oikeutta siirtää dataa järjestelmästä toiseen. Soveltuminen edellyttää, että kyse on käyttäjistä, jotka ovat henkilötietojen osalta rekisteröityjä.[187] Kuten DMA:n, on DA:n tarkoitus olla yhteensopiva henkilötietojen käsittelyä koskevan sääntelyn kanssa.[188] DA:ssa tärkeä ero digimarkkinasäädökseen verrattuna on se, ettei datasäädöksellä luoda tietosuoja-asetuksen mukaista oikeusperustaa, jonka nojalla datan haltija voisi antaa pääsyn henkilötietoihin tai asettaa ne kolmannen osapuolen saataville sellaisen käyttäjän pyynnöstä, joka ei ole rekisteröity.[189] Sen sijaan datasäädös luo datan haltijaa kohtaan velvoitteen antaa *rekisteröidylle* pääsyn heitä itseään koskevaan dataan, ja asettamaan datan käyttäjän valitseman kolmansien osapuolten saataville.[190] Tästä syystä näkökulma on

[185] Euroopan komissio, EU:n digimarkkinasäädös varmistaa oikeudenmukaiset ja avoimet digitaalialan markkinat 2022.
[186] DA-ehdotus 2022, s. 3.
[187] DA-ehdotus 1(3) artikla.
[188] DA-ehdotus 2022, s. 4.
[189] DA-ehdotuksen johdanto 24 kohta.
[190] DA-ehdotuksen johdanto 24 kohta.

enemmän yksilön kontrollia korostava.[191] Mikäli käyttäjä on yritys ja luokiteltavissa tietosuoja-asetuksen mukaisesti rekisterinpitäjäksi, tulee sillä olla tietosuoja-asetuksen mukainen oikeusperuste pyytäessään tuotteen tai siihen liittyvän palvelun käytön tuloksena tuotettuja henkilötietoja. Oikeusperusteesta esimerkiksi on tuotu esille rekisteröidyn suostumus tai oikeutettu etu.[192]

Digipalvelusäädös (Digital Services Act, DSA) on toinen osa EU:n niin sanottua digipalvelupakettia, joka sisältää digipalvelusäädöksen ja digimarkkinasäädöksen. Toisin kuin DMA, digipalvelusäädös asettaa digitaalisia palveluita tarjoavia kohtaan laajemminkin hyvin pitkälle meneviä vastuita ja velvoitteita, jotka tulevat koskemaan suurten toimijoiden lisäksi myös muita palvelujentarjoajia.[193] DSA tuo EU:n verkkokäyttäjille paremman mahdollisuuden hallita näkemäänsä sisältöä verkossa, ja suojaamaan sananvapautta, elinkeinovapautta ja oikeutta syrjimättömyyteen. Keskeisessä roolissa on turvallisuuden ja vastuullisuuden korostaminen muun muassa siten, että DMA pyrkii estämään verkossa oleva laittoman sisällön leviämisen.[194]

Vaikka DMA ja DSA ovat niputettuina samaan pakettiin, on niiden sääntelykehykset ja tarkoitukset erilaiset. DMA keskittyy nimenomaisesti suurien teknologiayhtiöiden eli portinvartijoiden toiminnan tiukempaan sääntelyyn, ja sen tavoitteena on suojella vääristymätöntä kilpailua ja oikeudenmukaisia markkinoita.[195] Sen sijaan DSA:ssa portinvartija ei terminä esiinny lainkaan, vaan sääntely ulottuu laajemmin välityspalveluiden tarjoajiin, joskin ankarimmin nimenomaan suuriin teknologiayhtiöihin. Tavoitteena DSA:ssa on varmistaa turvallinen, ennustettava ja luotettava verkkoympäristö, jossa puututaan laittoman sisällön ja disinformaation levittämiseen verkossa sekä suojellaan perusoikeuksia.[196]

[191] Datasäädös ei kuitenkaan sulje pois yritysten välisen datan sääntelyä. Keskeisintä on henkilötietojen luovuttamisessa eron tekeminen sen välille, milloin osapuolet toimivat tietosuoja-asetuksen mukaisena rekisterinpitäjänä, rekisteröitynä tai ei näissä kummassakaan roolissa.
[192] DA-ehdotuksen johdanto 30 kohta.
[193] Sitra 2022, s. 23.
[194] Ks. Eurooppa-neuvosto, digipalvelupaketti 26.10.2022.
[195] DMA:n johdanto 11 kohta.
[196] DSA:n johdanto 9 kohta.

6 TIETOSUOJA-ASETUKSEN VAIKUTUKSET DATAN LUOVUTTAMISEEN VELVOLLISUUTENA

6.1 Säädösten yhteensopivuus yleisesti

Digimarkkinasäädöksen velvoitteita noudattaessa portinvartijan tulee varmistaa erityisesti tietosuoja-asetuksen täysimääräinen noudattaminen.[197] Toisaalta DMA:n johdannossa on myös todettu, että digimarkkinasäädöstä sovelletaan riippumatta säännöksistä, jotka johtuvat muista unionin oikeuden säädöksistä kuten tietosuoja-asetuksesta.[198] Tämä viittaa siihen, että tarkoituksena on ollut digimarkkinasäädöksen ja tietosuoja-asetuksen soveltuminen toisiaan täydentävästi ilman keskinäisiä jännitteitä.[199]

Tietosuoja-asetuksen vaikutukset datan luovutusvelvollisuuden täyttämiseksi ulottuvat portinvartijan lisäksi tietoja vastaanottavan yrityksen toimintaan sekä niihin rekisteröityihin, joita luovutettavat tiedot koskevat. Datan luovutusvelvollisuuden myötä yritysten liiketoimintamallit muuttuvat luonnollisesti siten, että luovutusvelvollisuus tulee huomioida uudella tavalla osana datan käsittelyä ja hallinnointia. On myös arvioitu, että luovutusvelvollisuus laajemmassa mittakaavassa voi johtaa jopa siihen, ettei datan investointia ole kannattavaa jatkaa entiseen tapaan, koska dataa luovuttavat yritykset joutuvat jakamaan datan kilpailijoidensa kanssa.[200] Toisaalta vaikuttaisi epärealistiselta, että portinvartijoiden kokoiset suuret yhtiöt suoranaisesti vähentäisivät investointejaan tältä osin, koska datan hyödyntäminen on edelleen pitkälti niiden liiketoiminnan perusta, eikä käytännön vaikutuksia digimarkkinasäädöksen soveltamisen osalta vielä tiedetä varmaksi. Mainittu skenaario voisi olla todennäköisempi, jos luovutusvelvollisuus ulottuisi muihinkin kuin portinvartijayrityksiin, mikä taas yksin digimarkkinasäädöksen perusteella ei ole mahdollista.

Luovuttamisvelvollisuus ei poista mahdollisuuksia toimia toisin. Tietosuoja-asetus jättää edelleen mahdollisuuden datan vapaaehtoiseen luovuttamiseen tai datan luovuttamiseen rekisteröidyn tekemään tietopyyntöön perustuen. Pakollinen luovutusvelvollisuus voi siis myös teoriassa lisätä yrityksen intressiä luovuttaa dataa vapaaehtoisesti. Tämä toisaalta edellyttäisi sitä, että vapaaehtoinen luovutus tulisi yrityskäyttäjän näkökulmasta heille

[197] DMA 8(1) artikla ja esim. johdannon kohdat 65 ja 68.
[198] DMA:n johdanto 12 kohta.
[199] Geradin – Bania – Karanikioti 2022, s. 2.
[200] Lehtioksa 2018, s. 119.

kannattavammaksi esimerkiksi sopimuksin kuin lainsäädäntöön perustuva oikeus tietojen saamiselle. Tämän arviointi edellyttäisi mahdollisen sopimusperusteisen luovutuksen tarkastelua. Lisäksi on myös otettava huomioon, että digimarkkinasäädös kieltää portinvartijaa kiertämästä velvollisuuksiaan muun muassa sopimusperusteisesti.[201]

Henkilötietojen luovuttamisen edellytykset DMA 6(10) artiklassa voidaan jakaa seuraavasti: luovutus on perustunut yrityskäyttäjän pyyntöön ja luovutus on maksutonta, tehokasta, korkealaatuista sekä jatkuvaa ja reaaliaikaista. Lisäksi tietojen on liityttävä suoraan loppukäyttäjien toteuttamaan portinvartijan ydinalustapalvelun kautta yrityskäyttäjän tarjoamiin tuotteiden tai palveluiden käyttöön ja loppukäyttäjä antaa suostumuksensa tietojen jakamiselle. Luovutustoimi yrityskäyttäjän pyynnön ja maksuttomuuden osalta ei tietosuoja-asetuksen näkökulmasta ole ongelmallista. Myöskään tehokkaan ja korkealaatuisen tietoihin pääsyn toteuttaminen ei vaikuttaisi ainakaan olevan ristiriidassa tietosuoja-asetuksen kanssa. Tietosuoja-asetus ei aseta näille erityisiä edellytyksiä, eikä kiellä niiden toteuttamista. Sen sijaan luovutusvelvollisuuden alaisten tietojen luokittelu siten, mitä kaikkea tietoja luovutusvelvollisuus kattaa ja mitkä tiedot katsotaan henkilötiedoiksi, voi osoittautua haasteelliseksi, kuten myös se, miten arvioidaan tuotettua tietoa ja mitä tarkoitetaan henkilötietojen osalta suoralla liitynnällä. Problematiikka näyttäisi kuitenkin tältä osin liittyvän datan määrittelyyn itsessään, eikä varsinaiseen tietosuojalainsäädäntöön. Joka tapauksessa näidenkin toimien osalta on säädösten yhteensopivuus lähtökohtana.

6.2 Digimarkkinasäädöksen mahdollistamat käsittelyperusteet

Tietosuoja-asetuksessa säädetyt käsittelyperusteet ja tietosuojaperiaatteet liittyvät erityisesti DMA 6(10) artiklan soveltamiseen. Näiden osalta analysoinnissa lähdetään liikkeelle käsittelyperusteista, joista suostumus on digimarkkinasäädöksessä valmiiksi asetettu käsittelyperuste tietojen luovuttamiselle. Sen sijaan käsittelyperuste yrityskäyttäjän osalta tietojen vastaanottamiseksi ja saatujen tietojen käsittelemiseksi jää yrityskäyttäjän valinnaksi, minkä vuoksi suostumusta tarkastellaan myös yrityskäyttäjän näkökulmasta, sekä sivutaan mahdollisuutta hyödyntää tietosuoja-asetuksen käsittelyperusteista lakisääteisen velvollisuuden täyttämistä sekä oikeutettua etua.

[201] DMA:n johdanto 60 kohta.

Riippumatta siitä, että suostumus on olennainen osa tietojen luovutusta, varmistaa tietosuoja-asetus sen, ettei pelkästään henkilön antama suostumus poista tietojen käsittelyyn kohdistuvia muita vaatimuksia. Näin varmistetaan se, että henkilötiedot yksilölle kuuluvana luovuttamattomana perus- ja ihmisoikeutena toteutuu silloinkin, kun henkilö olisi siitä itse valmis luopumaan.[202] Näin ollen käsittelyperusteiden jälkeen analysoidaan tarkemmin myös tietosuojaperiaatteita luovutusvelvollisuuden arviointiin nähden keskeisiltä osin.

6.2.1 Suostumukselle perustuva datan luovutus

Suostumusta edellytetään, jotta portinvartija voi digimarkkinasäädöksen 6 (10) artiklan nojalla luovuttaa henkilötietoja sisältävää dataa yrityskäyttäjälle. Suostumuksella viitataan digimarkkinasäädöksessä yleisesti tietosuoja-asetuksen mukaiseen suostumukseen.[203] Yrityskäyttäjästä tulee rekisterinpitäjä, kun se vastaanottaa tietoja portinvartijalta ja sen tulee noudattaa tietosuoja-asetusta. Siten myös yrityskäyttäjällä tulee olla laillinen peruste tietojen vastaanottamiseksi ja käsittelemiseksi. Laillisen perusteen ei tarvitse välttämättä olla suostumus. Digimarkkinasäädöksen mukaan portinvartijan tulee kuitenkin antaa yrityskäyttäjälle mahdollisuus saada loppukäyttäjiltään tietosuoja-asetuksen edellyttämä suostumus tietojen saamiseksi ja hakemiseksi.[204] Portinvartija ei myöskään saa tehdä suostumuksen saamisesta yrityskäyttäjälle hankalampaa kuin sille itselleen.[205] Mitä sitten edellytetään, että suostumus tietojen luovuttamiseksi voidaan katsoa riittävän päteväksi tietosuoja-asetuksen mukaisesti? Mikäli suostumusta ei loppukäyttäjältä saada, jääkö digimarkkinasäädöksen mukainen velvollisuus täyttämättä? Sen lisäksi, että seuraavaksi tarkastellaan suostumusta portinvartijan osalta, tarkastellaan suostumuksen mahdollisuutta myös yrityskäyttäjän osalta.

Suostumus on tietosuoja-asetuksessa tarkasti rajattu toimi, jonka muodolle ja pyynnölle on asetettu tiukkoja edellytyksiä. Suostumuksen tulee olla vapaaehtoinen, yksilöity, tietoinen toimi, minkä lisäksi sen tulee perustua yksiselitteiseen tahdonilmaukseen.[206] Vapaaehtoisella suostumuksella tarkoitetaan sitä, että suostumuksen tulee perustua todelliseen vapaan valinnan mahdollisuuteen. Siten rekisteröidyllä on aito mahdollisuus myös kieltäytyä tai

[202] Warma – Nieminen 2016, s. 553.
[203] DMA 2(32) artikla.
[204] DMA:n johdanto 60 kohta.
[205] DMA 13(5) artikla.
[206] TSA 4(11) artikla, englanniksi käännettynä suostumukselta edellytetään, että se on ”*freely given, specific, informed and unambiguous*”.

peruuttaa suostumuksensa.[207] Vapaaehtoisuus perustuu rekisteröidyn todelliselle valinnalle ja kontrollille itseään koskevista tiedoista. Vapaaehtoisuus toteutuu myös siten, että rekisteröidyllä on mahdollisuus peruuttaa antamansa suostumus myöhemmin ja kieltäytyä suostumuksen antamisesta ilman, että hänelle aiheutuu siitä haittaa.[208] Suostumuksen tulee kattaa kaikki käsittelytoimet, joita rekisterinpitäjän on tarkoitus toteuttaa omassa toiminnassaan, ja nämä käsittelytarkoitukset on yksilöitävä pyydettäessä suostumusta.[209]

Aikaisemmin suostumuksen saaminen on käytännössä ollut rekisteröidyille pakollinen ehto, jotta rekisteröity on voinut käyttää portinvartijan alustapalveluita. Mikäli suostumusta ei ole annettu, ei palvelua ole voinut käyttää. Suostumuksen ohella portinvartijat ovat voineet käyttää myös muita perusteita, kuten oikeutettua etua. Toiminnan laillisuus sekä portinvartijoiden ja loppukäyttäjien välinen epätasapaino on herättänyt huolta.[210] Oikeuskäytännössä tätä arvioitiin jo aiemmin esitetyssä Saksan Facebook-tapauksessa, jossa oli kyse rekisteröidyn tosiasiallisesta valinnanvapaudesta suostumuksen perustana. Saksan kilpailuviranomainen piti tapauksessa ongelmallisena suostumuksen antamista laajoihin käsittelykokonaisuuksiin, kuten henkilötietojen keräämiseen kyseisen ydinalustapalvelun ulkopuolisilta sivustoilta. Sen sijaan Düsseldorfin valitustuomioistun ei pitänyt kyseistä seikkaa ongelmallisena.[211]

Digimarkkinasäädöksessä on huomioitu portinvartijoiden henkilötietojen käyttöön liittyvä kilpailuetu, jonka portinvartijat saavat yhdistelemällä ja käyttämällä ristiin omasta ydinalustapalvelustaan kerättyjä loppukäyttäjien henkilötietoja muista palveluista kerättyihin tietoihin, ja kirjaamalla näiden välisiä henkilötietoja myös palveluissa, joita ei tarjota yhdessä ydinalustapalvelun kanssa.[212] Portinvartijoiden tulee jatkossa antaa loppukäyttäjille valinnanmahdollisuus tällaiseen heitä koskevien tietojen yhdistelemiseen ja ristiin käyttöön tarjoamalla heille vähemmän yksilöllistetty vaihtoehto. Vaihtoehdon tulee olla vastaava, mutta ilman, että palvelun tai joidenkin sen toimintojen käyttö edellyttää kyseistä suostumusta.[213] Tämä portinvartijalle asetettu velvoite heijastaa osaltaan Saksan Facebook-tapauksen

[207] TSA:n johdanto 42 kohta.
[208] EDPB 2020, s. 7 ja TSA:n johdanto 42 kohta.
[209] TSA:n johdanto 32 kohta.
[210] Geradin – Bania – Karanikioti 2022, s.9.
[211] Düsseldorfin ylemmän alueellisen tuomioistuimen lehdistötiedote 24.3.2021 ja ks. myös Lehtioksa – Ljungman – Vainio 2019, s. 875–876.
[212] DMA:n johdanto 36 kohta.
[213] DMA 5(2) artikla ja DMA:n johdanto 36 kohta.

ratkaistavina olevia kysymyksiä liittyen rekisteröidyn tosiasialliseen valinnanvapauteen suostumuksen perustana eri palveluista kerättyjen henkilötietojen yhdistämisen osalta. Riippumatta siitä, että Saksan Facebook-tapaus on edelleen EU-tuomioistuimessa käsiteltävänä, on digimarkkinasäädöksen johdannossa nimenomaan mainittu, että portinvartijoille osoitettu velvoite varmistaa sen, että ne eivät heikennä epäoikeudenmukaisesti ydinalustapalvelujen kilpailullisuutta.[214] Tämä näyttäisi puoltavan tulkintaa siitä, että aiempi toiminta, jossa suostumuksella on katettu laajat käsittelykokonaisuudet, ei olisi hyväksyttävää. Kyseessä ei kuitenkaan vielä ole EUT:n virallinen linjaus.

Suostumuksen yksilöitävyyden vaatimus edellyttää, että kaikki käsittelytoimet, joita rekisterinpitäjän on tarkoitus toteuttaa omassa toiminnassaan, on yksilöitävä. Jotta suostumus olisi myös rekisteröidyn tekemä tietoinen toimi, tulee rekisteröidyn olla tietoinen vähintäänkin rekisterinpitäjän henkilöllisyydestä ja häntä koskevien tietojen käyttötarkoituksesta.[215] Yksiselitteisen suostumuksen tarkempi kuvaus on avattu asetuksen johdannossa, jossa suostumuksen antamisen kuvataan edellyttävän selkeää suostumusta ilmaisevaa toimea, jolla niin ikään vastataan selkeään ja tiiviisti esitettyyn pyyntöön.[216] Suostumus toimena kytkeytyy siten läheisesti siihen, miten suostumusta pyydetään rekisteröidyltä alun alkaen.

Tietojen käyttötarkoitus korostuu myös yksilöitävyyden vaatimuksessa. Kun rekisteröity antaa suostumuksensa tietojen luovuttamiselle, tulee sen siis tietää, että mille yritykselle tiedot menevät ja mitä varten. Tämä tarkoittaa, että myös portinvartijalla tulee olla tieto vastaanottavan yrityskäyttäjän henkilöllisyydestä ja siirrettävien tietojen tulevasta käyttötarkoituksesta, jotta suostumus tietojen luovuttamista varten on pätevä. Yrityskäyttäjän henkilöllisyys selviää pyynnön yhteydessä, jolloin yksilöitävyyden täyttämiseksi yrityskäyttäjän tulisi ilmoittaa myös aiottu käyttötarkoitus.

Portinvartija ei näin ollen voi kattaa DMA:n vaatimia tietojen luovutuksia etukäteen valmiiksi saadulla suostumuksella tai muuten toimitetulla pelkällä informaatiolla. Edellä mainittu vaikuttaisi rajoittavan toimintaa myös niin, että niin sanotut massaluovutukset, joilla portinvartija voisi luovuttaa tiedot kerralla kaikille, eivät olisi mahdollisia. DMA:n mukainen henkilötietojen luovutus merkitsisi yrityskäyttäjän tekemän pyynnön perusteella

[214] DMA:n johdanto 36 ja Kerber – Zolna 2022, s. 24
[215] TSA:n johdanto 42 kohta.
[216] TSA:n johdanto 32 kohta.

tapauskohtaista suostumuksen arviointia, jotta tietosuoja-asetuksen asettamat edellytykset täyttyisivät. Tämä voi osoittautua haastavaksi portinvartijan lisäksi myös tietoja vastaanottavan yrityskäyttäjän puolelta. Yrityskäyttäjän tulee määritellä etukäteen tietojen käsittelyn käyttötarkoitus ja informoida tästä rekisteröityä. Olennaista on se, että mainitut toimenpiteet on toteutettu ennen tietojen käsittelyn aloittamista.[217]

Suostumuksen osalta siis edellytetään, että rekisterinpitäjillä on rekisteröidyltä saatu suostumus, ennen kuin henkilötietojen käsittely aloitetaan. Toimen toteuttamiseksi voisi olla mahdollista, että suostumus pyrittäisiin saamaan yhtäaikaisesti portinvartijan suorittamalle tietojen luovuttamiselle sekä tiedot vastaanottavan yrityskäyttäjän käsittelytoimille. Tällöin portinvartijalla olisi mahdollisuus varmistaa DMA:n edellyttämällä tavalla yrityskäyttäjän saama suostumus henkilötietojen käsittelylle. Tämäkin näyttäisi johtavan suostumuksen tapauskohtaiseen soveltamiseen, jossa huomioitaisiin yksilöllisesti tietoja pyytävä asianomainen yrityskäyttäjä, yrityskäyttäjään liittyvät tiedot ja tietojen käyttötarkoitus.

Suostumuksen tiukat edellytykset voivat aiheuttaa haasteita portinvartijalle käsittelyperusteen käytännön toteuttamisessa. Koska käsittelyperuste on kuitenkin DMA:ssa rajattu tältä osin nimenomaisesti suostumukseen, tulee portinvartijan soveltaa tätä toiminnassaan, eikä portinvartija voi tietosuoja-asetuksenkaan nojalla vaihtaa käsittelyperustetta toiseen. Tämä johtaa luonnollisesti siihen lopputulokseen, että mikäli rekisteröity ei anna suostumustaan tietojensa luovuttamiselle yrityskäyttäjälle DMA:n nojalla, ei tietoja voida luovuttaa. Samaan tulkintaan päädytään, mikäli rekisteröity tietosuoja-asetuksen nojalla peruuttaa aiemmin antamansa suostumuksensa.[218] DMA:n ja tietosuoja-asetuksen yhteensovittaminen suostumuksen osalta jättää portinvartijalle vastuun suostumuksen toteuttamiseen, mikä tarkasteltuna herättää jo valmiiksi aiheellista epäilystä siitä, miten suostumuksesta saadaan tietosuoja-asetuksen edellyttämällä tavalla riittävän pätevä.

Mikäli suostumuksesta voidaan loppukäyttäjän toimesta kieltäytyä tai suostumus peruuttaa, epävarmaksi jää, miten DMA:n luovutusvelvollisuuden tarkoitus tällaisessa tilanteessa asiaan suhtautuu. DMA 6(10) artiklan tarkoituksena on kuitenkin varmistaa, että

[217] Lehtioksa 2018, s. 122
[218] Geradin – Bania – Karanikioti 2022, s. 12 ja EDPB 2020, s. 25.

yrityskäyttäjillä on pääsy asiaankuuluviin tietoihin, mikä taas niin ikään toteuttaa asetuksen kilpailuoikeudellista tavoitetta.[219]

Vastaanottavan yrityksen osalta suostumuksen tiukat edellytykset kaventavat sen käyttömahdollisuutta ja suostumuksen puute näyttäisi mahdollistavan myös velvollisuuden täyttymättä jäämisen. Mikäli portinvartija saa suostumuksen, mutta yrityskäyttäjä ei, voi yrityskäyttäjän olla tarpeen hyödyntää muuta tietosuoja-asetuksen mukaista käsittelyperustetta, kuten lakisääteisen velvoitteen täyttämistä tai oikeutettua etua.

6.2.2 Yrityskäyttäjän henkilötietojen käsittelyn perusteena lakisääteisen velvoitteen noudattaminen

Henkilötietojen käsittely on tietosuoja-asetuksen 6(1)(c) artiklan perusteella mahdollista myös rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi. Velvoitteen tulee perustua 6(3) artiklan nojalla joko unionin oikeuteen tai rekisterinpitäjään sovellettavan jäsenvaltion lainsäädäntöön. Tietosuoja-asetuksen johdannon 41 kohdassa on täsmennetty lakisääteistä velvoitetta siten, että tällaisen käsittelyn oikeusperustan tai lainsäädäntötoimen tulee aina olla selkeä, täsmällinen ja sen soveltamisen oltava ennakoitavissa suhteessa niihin, joihin sitä sovelletaan. Kaikkia yksittäisiä velvoitteita varten ei kuitenkaan tarvitse olla sitä spesifisti koskevaa erityislakia, vaan riittävänä voidaan pitää yhtä lakia, joka toimii useiden käsittelytoimien perustana.[220] Oleellista on, että olemassa on riittävän selkeä perusta unionin laissa tai jäsenvaltion laissa.[221] Kansallisen lainsäädäntöön perustuvan lakisääteisen velvoitteen noudattaminen voi tulla kyseeseen esimerkiksi silloin, kun osakeyhtiölaki edellyttää osakeyhtiötä pitämään osakasluetteloa.[222]

Digimarkkinasäädös ja sen asettama velvollisuus datan luovuttamiseen on unionin oikeuteen perustuva lakisääteinen velvoite. Vaikka lakisääteisen velvoitteen täyttäminen sopisi unionin oikeuteen perustuvan luovutusvelvollisuuden osalta, on käsittelyperusteen sopivuus muilta osin epävarmempi. Käsittelyperusteen sopivuus edellyttää lainsäädännön

[219] DMA:n johdanto 60 kohta; englanniksi, jossa käy selkeämmin portinvartijalle käännetty velvollisuus varmistaa: ”*– – In order to ensure that business users have access to the relevant data thus generated, the gatekeeper should, upon request, provide effective access, free of charge, to such data.– –*“. Suomennettuna *“– – Jotta yrityskäyttäjillä olisi pääsy näin tuotettuihin merkityksellisiin tietoihin, portinvartijan olisi pyynnöstä ja maksusta tarjottava tosiasiallinen pääsy tällaisiin tietoihin. – –*”.
[220] TSA:n johdanto 45 kohta.
[221] ICO, Guide to the General Data Protection Regulation, kohta Legal Obligation.
[222] Hanninen ym. 2017, s. 31.

lisäksi, että unionin oikeudessa tai jäsenvaltion lainsäädännössä säädetään myös käsittelyn tarkoituksesta ja siitä, että peruste on riittävän selkeä ja ennakoitavissa oleva.[223] Käsittelyperusteen käyttöä rajaa se, että lakisääteisen velvoitteen täyttäminen vaikuttaisi olevan edellytyksiltään melko laaja. Jos perustaksi tulisi lakisääteinen velvoite, jäisi kysymykseksi yrittäjäkäyttäjäkohtainen tietojen käsittelyn tarkoitus, selkeys ja ennakoitavuus. Ennakoitavuutta vähentää se, että loppukäyttäjällä on mahdollisuus suostumuksellaan vaikuttaa siihen, onko tietojen luovutus ylipäätään mahdollista.

Yrityskäyttäjällä on velvollisuuden osalta harkintavaltaa jo senkin suhteen, että luovuttaminen aktivoituu vasta yrityskäyttäjän tekemästä pyynnöstä. Luovutuksen jälkeen tietojen käsittely jää niin ikään kokonaan yrityskäyttäjän harkintaan. Yrityskäyttäjä päättää sen, mitä tiedoilla tehdään ja miten niitä käytetään. Tämä harkintavalta käsittelyn tarkoituksesta ja mahdollisuudesta perustaa henkilötietojen käsittely toiselle käsittelyperusteelle, kuten suostumukselle, näyttäisivät tekevän tästä lakisääteisen velvoitteen täyttämisestä epävarman ja siten myös epätodennäköisen käsittelyperusteen.[224]

6.2.3 Yrityskäyttäjän henkilötietojen käsittelyn perusteena oikeutettu etu

Henkilötietojen käsittely voi olla tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi tietosuoja-asetuksen 6(1)(f) artiklan nojalla. Oikeutettu etu voi olla tietosuoja-asetuksen johdannon mukaan olemassa esimerkiksi silloin, kun rekisteröidyn ja rekisterinpitäjän välillä on merkityksellinen ja asianmukainen suhde, kuten silloin, kun rekisteröity on rekisterinpitäjän asiakas tai tämän palveluksessa.[225] Oikeutettu etu voi mahdollistaa henkilötietojen käsittelyn esimerkiksi tilanteissa, joissa on kyse suoramarkkinoinnista, tieteellisestä ja historiallisesta tutkimuksesta tai tilastoinnista taikka henkilötietojen siirtämisestä konsernin sisällä hallinnollisista syistä.[226]

Oikeutetun edun toteuttaminen edellyttää huolellista arviointia sen suhteen, voiko rekisteröity kohtuudella odottaa henkilötietojen keräämisen ajankohtana ja sen yhteydessä, että henkilötietoja käsitellään kyseistä tarkoitusta varten.[227] Etua voidaan pitää oikeutettuna,

[223] ICO, Guide to the General Data Protection Regulation, kohta Legal Obligation.
[224] ICO, Guide to the General Data Protection Regulation, kohta Legal Obligation.
[225] TSA:n johdanto 47 kohta.
[226] Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille henkilötietojen käsittelystä, tietosuojavaltuutetun toimiston verkkosivu, kohta Rekisterinpitäjän oikeutettu etu.
[227] TSA:n johdanto 47 kohta.

mikäli se on unionin tai kansallisen lainsäädännön mukainen, selkeästi ilmaistu ja edustaa todellista ja välitöntä tarvetta.[228]

Lähtökohtana on, että yksityishenkilönä olevan loppukäyttäjän edut ja oikeudet ovat suojatumpia kuin rekisterinpitäjän. Etujen vertailu perustuu niin kutsulle tasapainotestille, jossa arvioidaan ja punnitaan osapuolilla olevia etuja ja oikeuksia. Jos nämä edut ja oikeudet syrjäyttävät rekisterinpitäjän edun, ei henkilötietoja saa käsitellä oikeutetun edun perusteella.[229]

Jotta yrityskäyttäjä voisi vastaanottaa ja käsitellä portinvartijan luovuttamia henkilötietoja oikeutetun edun nojalla, edellyttää se, että rekisteröity voi kohtuudella odottaa sitä ja toimilla on minimaalinen vaikutus rekisteröidyn yksityisyyteen. Huolimatta siitä, että oikeutetuiksi eduiksi katsottujen etujen määrä on laaja ja käsittelyperuste siten laajasti käytettävissä, ei käsittelyperuste todennäköisesti riittäisi kuitenkaan kattamaan yrityskäyttäjän henkilötietojen keräämisen käyttötarkoitusta ja jokaista eri käsittelyä. Käytännön tasolla on vaikea arvioida, voidaanko siten myöskään yrityskäyttäjän portinvartijalta saamien tietojen vastaanottaminen eriyttää muista käsittelyistä yhdeksi omaksi toimeksi, johon oikeutettu etu käsittelyperusteena sopisi. Mikäli tietojen vastaanottaminen halutaan perustaa oikeutettuun etuun, on yrityskäyttäjän arvioitava sitä edellä mainittujen perusteiden mukaisesti ja lisäksi on huomioitava, ettei oikeutettu etu välttämättä ole riittävä henkilötietojen käsittelyn jatkamiselle, vaikka se kattaisi tietojen vastaanottamisen. Yrityskäyttäjän tulee olla vähintäänkin varovainen ja pyrkiä siihen, ettei se ainakaan oleta oikeutetun edun käyvän perusteeksi jokaiselle henkilötietojen käsittelytoimelle.[230]

6.3 Keskeiset tietosuojaperiaatteet

Henkilötietojen käsittelyssä, mukaan lukien luovuttamisessa ja vastaanottamisessa, tulee noudattaa tietosuoja-asetuksen 5(1) artiklan tietosuojaperiaatteita. Tutkielman rajauksen kannalta lähestytään seuraavaksi periaatteista tarkemmin ainoastaan käyttötarkoitussidonnaisuutta ja tietojen minimoinnin periaatetta, jotka ovat edellä esitetyn rekisteröidyltä

[228] Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille henkilötietojen käsittelystä, tietosuojavaltuutetun toimiston verkkosivu, kohta Rekisterinpitäjän oikeutettu etu.
[229] WP 217, s. 30–31 ja Tietosuojavaltuutetun toimiston antamat ohjeet organisaatioille henkilötietojen käsittelystä, tietosuojavaltuutetun toimiston verkkosivu, kohta Rekisterinpitäjän oikeutettu etu.
[230] ICO, Guide to the General Data Protection Regulation, kohta Legitimate interests.

vaadittavan suostumuksen kanssa osittain päällekkäisiä, ja voineen siten aiheuttaa myös ristiriitaa henkilötietojen luovutusvelvollisuuteen.[231]

6.3.1 Käyttötarkoitussidonnaisuus

Käyttötarkoitussidonnaisuus edellyttää henkilötietojen keräämistä tiettyä, nimenomaista ja laillista tarkoitusta varten. Lisäksi se edellyttää, että henkilötietoja ei käsitellä tämän alkuperäisen käyttötarkoituksen kanssa yhteensopimattomasti myöhemmin.[232] Portinvartijan ja yrityskäyttäjän henkilötietojen käyttötarkoituksien yhteensopivuutta luovutuksen yhteydessä on siten olennaista arvioida. Portinvartija määrittelee omassa toiminnassaan henkilötietojen käyttötarkoituksen siten, että se vastaa portinvartijan tavoitteita. Kuten edellä on ilmennyt, tulee yrityskäyttäjän tietosuoja-asetuksen mukaisesti määritellä ja informoida sen aiottu käyttötarkoitus rekisteröidylle, ennen kuin se vastaanottaa tietoja, jotka sille luovutetaan DMA:n asettaman velvoitteen nojalla.

Käyttötarkoituksia voi olla useita, eikä tietosuoja-asetus rajoita henkilötietojen käsittelyä vain yhteen tarkoitukseen. Käyttötarkoituksien määrä ei siten itsessään aiheuta haasteita, vaan mainittu yhteensopivuus. Myöhemmin tapahtuva käyttötarkoitus, joka on erilainen kuin alkuperäinen, ei kuitenkaan automaattisesti tarkoita, että se olisi yhteensopimaton. Yhteensopivuuden tarkastelu perustuu tapauskohtaiselle arvioinnille.[233]

Käyttötarkoitussidonnaisuuden arviointi osoittaa sen, että varminta olisi, mikäli vastaanottavan yrityskäyttäjän tietojen käyttötarkoitus vastaisi portinvartijan käyttötarkoitusta. Mikäli käyttötarkoitukset eivät ole yhdenmukaisia portinvartijan ja yrityskäyttäjän välillä, perustuisi henkilötietojen käsittely toisin sanoen muita tarkoituksia varten kuin niitä, joita varten tiedot on alun perin kerätty.[234] Yhteensopivuuden osalta voidaan vertailla uutta käyttötarkoitusta alun perin ilmoitettuun käyttötarkoitukseen. Vertailu voi perustua alkuperäisen käyttötarkoituksen kirjalliseen muotoiluun sen selvittämiseksi, voidaanko alkuperäisen käyttötarkoituksen arvioida kattavan myös uusi käyttötarkoitus. Vertailussa kiinnitetään huomiota siihen, minkälainen suhde uudella käyttötarkoituksella on alkuperäiseen

[231] Warma – Nieminen 2016, s. 553.
[232] TSA 5(1)(b) artikla ja WP 203, s. 3.
[233] WP 203, s. 21.
[234] TSA:n johdanto 50 kohta sekä ks. Lehtioksa 2018, 124.

käyttötarkoitukseen nähden.[235] Käyttötarkoituksia voi arvioida niiden kirjallisen muodon lisäksi myös sisällöllisesti, jolloin kyseeseen tulee käyttötarkoituksen ymmärrettävyys, asiayhteys ja muut tapauskohtaiset tekijät.[236]

Henkilötietoja voidaan käsitellä myös suoraan tietosuoja-asetuksen 6(4) artiklan nojalla muita kuin alkuperäisiä käyttötarkoituksia varten, jos rekisteröity on antanut suostumuksen tai laissa on tällaisesta säädetty. Laissa säädetyllä muilla käsittelyillä viitataan tietosuoja-asetuksen 23(1) artiklassa tarkoitettujen tavoitteiden turvaamiseen. Näitä on muun muassa kansallinen ja yleinen turvallisuus, puolustus sekä oikeudellisen riippumattomuuden ja oikeudellisten menettelyjen suojelu. Mikäli suostumusta tai lakiin perustuvaa perustetta ei ole, on yhteensopivuuden arvioinnissa otettava huomioon alkuperäisen ja myöhemmän käsittelyn käyttötarkoitukset, asiayhteys, henkilötietojen luonne, myöhemmän käsittelyn mahdolliset seuraukset rekisteröidylle sekä asianmukaisten suojatoimien, kuten salaamisen tai pseudonymisoinnin, olemassaolo.[237]

Käyttötarkoitussidonnaisuuden arvioinnissa DMA:n luovutusvelvollisuudessa kyse on rekisteröidyn suostumukselle perustuvasta luovutustoimesta, joka perustuu unionin tasoisen lainsäädännön velvoitteen noudattamiselle. Mikäli yrityskäyttäjän suorittama myöhempi henkilötietojen käsittely perustuu myös rekisteröidyn antamalle suostumukselle, vaikuttaa käyttötarkoitussidonnaisuuden arviointiin myös se, missä määrin suostumus annettiin vapaaehtoisesti sekä miten täsmällisiä suostumukseen liittyvät ehdot ovat olleet. Yleisesti ottaen yhteensopivuuden arviointi on sitä tiukempi, mitä vähemmän rekisteröidylle on suostumuksen pyytämisen yhteydessä annettu valinnanvapautta, ja mitä enemmän vaaditut ehdot ovat olleet epätäsmällisiä. Mahdollisuutta henkilötietojen myöhempään käsittelyyn pienentää itsessään se, jos alkuperäinen käyttötarkoitus on hyvin tarkasti rajattu.[238] Kun yrityskäyttäjä pyytää suostumusta rekisteröidyltä tietojen käsittelylle, näyttäisi olevan hyvä varmistaa, että rekisteröidylle annetaan tietosuoja-asetuksessa edellytettävin tavoin tosiasiallinen vapaus valita varteenotettavista vaihtoehdoista tietojensa käsittelyn laajuus. Tällä edesautetaan myös käyttötarkoituksien yhteensopivuutta. Portinvartijan osalta tarkoittaisi tämä

[235] WP 203, s. 3.
[236] WP 203, s. 21.
[237] TSA 6(4) artikla.
[238] WP 203, s. 24–25.

sitä, ettei portinvartijan tulisi rajata alkuperäistä käyttötarkoitustaan liian tiukasti, mikä hankaloittaisi yrityskäyttäjän käyttötarkoituksen määrittämistä.

Tietosuojatyöryhmä on ennen tietosuoja-asetuksen säätämistä laatimissaan ohjeissaan antanut merkitystä sille, perustuuko myöhempi käsittely suoraan lakiin.[239] Tällä viitataan kuitenkin suoraan tietosuoja-asetuksen sääntelyyn siitä, mitä ei pidetä käyttötarkoituksissa yhteensopivana. Tietosuoja-asetuksen mukaan henkilötietojen myöhempää käsittelyä arkistointitarkoituksia, tieteellisiä tai historiallisia tutkimustarkoituksia taikka tilastollisia tarkoituksia varten ei katsota yhteensopimattomiksi alkuperäisen käyttötarkoituksen kanssa.[240]

Käyttötarkoitussidonnaisuuden tulkinta mahdollistaa kuitenkin joustavan tulkinnan käyttötarkoituksien osalta tilanteissa, joissa yhteiskunnan ja rekisteröidyn itsensä kohtuulliset odotukset siitä, mihin lisäkäyttöön henkilötietoja voidaan käyttää, ovat muuttuneet.[241] Lisäksi lainsäätäjä on kieltänyt yhteensopimattomuuden yhteensopivuuden vaatimisen sijasta ja näin antanut tietosuoja-asetuksella joustoa henkilötietojen myöhemmälle käytölle, eikä tällaista käyttöä eri tarkoitusta varten tule suoraan pitää yhteensopimattomana.[242] Tietosuojatyöryhmä on kuitenkin korostanut käyttötarkoitussidonnaisuuden ja siihen kuuluvaan yhteensopivuuden arviointiin liittyen asiayhteyttä ja tapauskohtaista harkintaa, mikä voi osoittautua haastavaksi DMA:n luovutusvelvollisuuden osalta.[243] Tämän perusteella sekä suostumus että käyttötarkoitussidonnaisuuden arviointi edellyttävät molemmat tapauskohtaista arviointia, mikä voi suuressa mittakaavassa voi muodostua epäkäytännölliseksi tai jopa mahdottomaksi, ja siten olla esteenä tietojen sujuvalle luovuttamiselle. Toisaalta DMA:n luovutusvelvollisuuden käyttötarkoitussidonnaisuuden arvioinnissa rekisteröidyltä saatava suostumus sekä unionin oikeuteen perustuvan velvoitteen noudattaminen tukevat taas enemmissä määrin käsitystä siitä, että yhteensopivuudesta ei muodostuisi välttämättä luovutuksen yhteydessä ongelmaa.

[239] WP 203, s. 28–29.
[240] TSA 5(1)(b) artikla ja tarkemmin TSA 89 artikla.
[241] WP 203, s. 21.
[242] WP 203, s. 39.
[243] WP 203, esim. s. 3 ja 39.

6.3.2 Tietojen minimointi

Henkilötietojen käyttötarkoitus määrittää henkilötietojen tarpeellisen suhteen siihen, mitä varten niitä käsitellään. Henkilötietojen käsittelyn tulee olla asianmukaista ja olennaista, ja rajoittua ainoastaan määriteltyyn käyttötarkoitukseen.[244] Tietojen minimointi edellyttää, että henkilötietojen tulee rajoittua vain siihen, mikä on välttämätöntä niiden käsittelyn tarkoituksen kannalta. Tämä edellyttää myös henkilötietojen mahdollisimman lyhyttä säilytysaikaa.[245]

Henkilötietojen kerääminen vain silloin, kun niitä voidaan pitää tarpeellisina, edellyttää asianmukaisuuden ja olennaisuuden lisäksi sitä, etteivät tiedot ole liian laajoja niihin tarkoituksiin, mihin ne on kerätty ja mitä varten niitä käsitellään.[246] Käytännössä tietojen minimoinnin vaatimus siis edellyttää, että henkilötietoja kerätään mahdollisimman vähän ja ainoastaan silloin, kun niiden käyttö on täysin tarpeellista.[247]

Luovutettavien henkilötietojen tulee siten olla niin rajoitettuja kuin mahdollista ja kattaa ainoastaan vastaanottavan yrityskäyttäjän tarkasti määritelty tietojen aiottu käyttötarkoitus.[248] Portinvartijan tulee varmistaa, että tiedot ovat luovutettavissa DMA:n mukaisesti eli portinvartijan tulee luovuttaa ainoastaan yrityskäyttäjän käyttötarkoitukseen nähden tarpeellinen data.[249] Näin ollen myös tietojen minimoinnin vaatimus näyttäisi edellyttävän, että portinvartijan tulee olla etukäteen ennen luovutustoimen täyttämistä tietoinen myös yrityskäyttäjän tietojen käyttötarkoituksesta. Käyttötarkoitussidonnaisuus ja tietojen minimointi tietosuojaperiaatteina johtavat yhdessä siihen lopputulokseen, että luovutusvelvollisuuden alaisen datan tulee olla mahdollisimman rajattua.[250]

6.4 Jatkuva ja reaaliaikainen pääsy dataan

Datan luovuttamisessa on DMA 6(10) artiklan perusteella kyse yrityskäyttäjille ja yrityskäyttäjien valtuuttamille kolmansille osapuolille tarjottavasta jatkuvasta ja reaaliaikaisesta

[244] TSA 5(1)(c) artikla.
[245] TSA:n johdanto 39 kohta.
[246] Henkilötietolain hallituksen esitys HE 96/1998 vp, s. 42.
[247] Korpisaari – Pitkänen – Warma-Lehtinen 2018, s. 93
[248] Van Gorp ym. 2020, s. 34.
[249] DMA:n johdanto 59 kohta.
[250] Van Gorp ym. 2020, s. 70.

pääsystä (*continuous and real-time access*) ja käyttömahdollisuudesta tietoihin. Artiklan mukaan samanlainen pääsy on tarjottava myös henkilötietoihin. Kyseisenlainen jatkuva ja reaaliaikainen datan siirrettävyys on uudenlainen tietojen siirtämisen muoto, eikä se ole kuulunut tietosuoja-asetuksen sääntelyn piiriin aiemmin. DMA:ssa jatkuvan ja reaaliaikaisen pääsyn toteuttaminen on portinvartijan vastuulla varmistaa. DMA:n johdannossa todetaan, että pääsyn on oltava mahdollista asianmukaisin teknisin toimenpitein, kuten korkealaatuisten sovellusrajapintojen avulla tai pieniä yrityksiä varten integroitujen välineiden avulla.[251] DMA jättää siis jatkuvan ja reaaliaikaisen pääsyn toteuttamisen edellytykset melko avoimeksi, jolloin asianmukaiset velvollisuuden täyttävät keinot jäävät portinvartijan vastuulle kehitettäväksi ja toteutettavaksi.

Reaaliaikainen dataan pääsy on tärkeää, jotta saatavat tiedot säilyttävät merkityksensä. Tiedon liikkuminen, kertyminen ja muuttuminen on hyvin nopeaa ja uutta tietoa kertyy jatkuvasti. Tästä syystä se, mikä tekee juuri kyseisestä datasta yrityskäyttäjälle relevanttia, voi muuttua tai myös hävitä nopeasti.[252] Reaaliaikainen siirrettävyys edellyttää portinvartijalta sellaisia teknisiä toteutuksia, jotka ovat tasapuolisesti mahdollisia yrityskäyttäjille, riippumatta yrityskäyttäjän koosta ja teknisten käytäntöjen mahdollisuuksista. Vaikka tämä jättää portinvartijalle edelleen päätäntävaltaa keinoista ja käytännön toteutuksesta, poistaa jatkuvan ja reaaliaikainen dataan pääsy pullonkauloja enemmän kuin kertaluonteinen tietojen luovuttaminen.[253]

Teoriassa jatkuva ja reaaliaikainen pääsy dataan vaikuttaisi siis olevan tehokas keino varmistaa, että yrityskäyttäjät saavat pyytämiään ja tarvitsemiaan tietoja käyttöönsä. Kuitenkin se, miten TSA:n edellytykset toimivat käytännössä kyseisen jatkuvan ja reaaliaikaisen datan luovuttamisen suhteen, on epäselvää. Epäselväksi DMA:n ja TSA:n perusteella jää esimerkiksi se, miten käyttötarkoitussidonnaisuus suhtautuu jatkuvan ja reaaliaikaisen datan käsittelyyn. Asiayhteyden säilyminen on olennaista käyttötarkoitussidonnaisuuden noudattamisessa silloinkin, kun datan virta on jatkuvaa. Lisäksi jatkuva ja reaaliaikainen pääsy dataan on otettava huomioon määriteltäessä rekisteröidylle suostumusta tietojen käsittelyperusteeksi.

[251] DMA:n johdanto 60 kohta.
[252] Van Gorp ym. 2020, s. 20.
[253] Van Gorp ym. 2020, s. 46.

Jatkuvan ja reaaliaikaisen dataan pääsyn on myös arvioitu olevan toimena datan varsinaisen luovuttamisen sijaan ainoastaan oikeus päästä käsiksi tietoihin. Pääsy tietoihin tapahtuisi silloin paikan päällä portinvartijan tarjoamalla alustalla ja yrityskäyttäjä voisi hyödyntää ja käyttää tietoja ilman suoraa pääsyä yksittäisiin tietoihin.[254] Kun yrityskäyttäjä kuitenkin saa hyödyntää dataa pääsemällä käsiksi jatkuvaan ja reaaliaikaiseen datavirtaan, soveltuu yrityskäyttäjän toimintaan joka tapauksessa tietosuoja-asetuksen sääntely tältäkin osin. Datan jakamisessa eri toimijoiden välillä on lopulta kuitenkin kyse henkilötietoja sisältävän datan suojaamisesta.[255] Jatkuva ja reaaliaikainen datan luovutus asettaa kyllä portinvartijalle laajemmin vastuuta, jota on hankalampi kiertää kertaluonteiseen verrattuna, mutta se toisaalta asettaa yksilöille myös laajemman tietosuojariskin.

6.5 Anonymisointi ja pseudonymisointi luovutusvelvollisuuden täyttämisen keinoina

Digimarkkinasäädöksen 13(5) artiklan mukaisesti portinvartijalta edellytetään tarvittavien toimenpiteiden toteuttamista, jotta yrityskäyttäjä voi saada rekisteröidyltä suostumuksen henkilötietojen käsittelyyn. Portinvartija voi myös vaihtoehtoisesti noudattaa tietosuoja-säännöksiä antamalla yrityskäyttäjille asianmukaisesti anonymisoituja tietoja. Tarkemmin siitä, miten tätä anonymisointia tulisi tällaisessa tilanteessa konkreettisesti toteuttaa, ei DMA:ssa säädetä. Anoymisoinnin mahdollisuutta tietojen luovutuksessa tulee arvioida suhteessa luovutusvelvollisuuden tavoitteeseen eli siihen, että yrityskäyttäjälle tulee varmistaa velvoitteen mukainen pääsy portinvartijan hallussa olevaan dataan.[256]

Anonymisoinnin lisäksi henkilötietoja voidaan pseudonymisoida. Nämä toiminnat perustuvat molemmat ikään kuin henkilötietojen poistamiselle tai tarkemmalle suojaukselle, mutta johtavat kuitenkin täysin eri lopputuloksiin. Pseudonymisoinnilla ei anonymisoida dataa siten, että tunnistettavuus poistuisi kokonaan. Siten pseudonymisoinnin jälkeiset tiedot ovat edelleen tietosuoja-asetuksen alaisia, toisin kuin anonymisoidut eli anonyymit tiedot.[257]

[254] JRC 2021, s. 22.
[255] Ks. EDPS 2021, s. 3.
[256] DMA:n johdanto 60 kohta
[257] TSA:n johdanto 26 kohta.

6.5.1 Anonymisointi

Varsinaista anonymisointia DMA:ssa edellytetään silloin, kun portinvartija velvoitetaan tarjoamaan hakukysely-, klikkaus- ja näkymädataan sisältyviä henkilötietoja hakukoneita tarjoavalle yritykselle.[258] Anonymisoinnissa portinvartijan tulee varmistaa loppukäyttäjien henkilötietojen suoja myös mahdollisilta jälleentunnistamisen riskeiltä. Anonymisointi ei saa kuitenkaan heikentää merkittävästi datan laatua tai käyttökelpoisuutta.[259]

Henkilötiedoissa olennaista on tietojen tunnistettavuus. Kun henkilötiedoista poistetaan niiden tunnistettavuus, ei tietoja luokitella enää henkilötiedoiksi, eikä niiden soveltaminen kuulu enää tietosuoja-asetuksen piiriin. Anonyymit tiedot eivät liity tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön taikka niiden tunnistettavuus on poistettu niin, ettei rekisteröidyn tunnistaminen ole enää mahdollista.[260] Anonyymit tiedot voivat poistaa tiedoista sen käytön mahdollisuuden, jota varten tietoja alun alkaen on kerätty.[261] Voisiko portinvartija hyödyntää datan luovuttamisessa anonymisointia tai pseudonymisointia täyttääkseen DMA:ssa sille asetetun velvoitteen, mutta välttääkseen tietosuoja-asetuksen edellytysten tuomia sääntelyjä ja niistä muodostuvia riskejä? Anonymisoinnille on annettu DMA:ssa mahdollisuus, mutta sen käyttämisen ehtoina olevat datan laadun ja käyttökelpoisuuden säilyttäminen vaikuttavat anonymisoinnin käytännön toteutumiseen. Toisin kuin pseudonymisoitujen henkilötietojen, anonymisoitujen tietojen ei tulisi olla enää käsittelyn jälkeen palautettavissa tiettyyn tunnistettuun henkilöön. Vaikka anonyymit tiedot eivät kuulu tietosuoja-asetuksen piiriin, sovelletaan itse anonymisointiin toimenpiteenä tietosuoja-asetuksen sääntelyä.[262]

Datan anonymisoinnin hyötynä dataa voidaan luovuttaa väljemmin perustein. Anonymisointia voidaan käyttää, jotta dataa voidaan luovuttaa siten, ettei samalla tarvitse huolehtia erillisestä tietosuoja-asetuksen noudattamisesta. Anonymisointi ei kuitenkaan ole välttämättä yrityskäyttäjän näkökulmasta se kaikkein hyödyllisin ratkaisu.[263] Anonymisoinnin yhteensopivuus datan käyttöarvoon nähden voi osoittautua ristiriitaiseksi. Datan hyöty kertyy datan muokkaantuvuudesta eli käytöstä, jatkojalostamisesta ja erilaisista

[258] DMA 6(11) artikla.
[259] DMA:n johdanto 61 kohta.
[260] TSA:n johdanto 26 kohta ja DMA:n johdanto 61 kohta.
[261] Lehtioksa 2018, s. 120
[262] Van Gorp ym., s. 33.
[263] Lehtioksa 2018, s. 120.

käsittelytoimista, kuten tietojen yhdistelemisestä. Jos datasta poistetaan olennaisia tietoja sen käyttötarkoitukseen nähden, kuten tunnistettavuuteen liittyviä tekijöitä, ei datan arvo välttämättä säily ennallaan. Poistettava tieto voi ilmentää juuri sitä, mikä tekee kyseisestä datasta arvokkaan. Yrityskäyttäjät voivat menettää anonymisoinnin kautta datan hyödyn ja siten anonymisoitu data voi olla hyödytöntä datan jakamisessa.[264] Mikäli näin kävisi, ei anonymisointi täyttäisi yrityskäyttäjän pääsyä dataan eikä siten DMA:n tavoitteita.

Anonymisointi voi kohdistua massadataan, mikäli hallittavan datan määrä on suuri ja tarkoitus on toimia sen käsittelyssä nopeasti ja tehokkaasti. Massadatan anonymisointi voi kuitenkin osoittautua ongelmalliseksi. Portinvartija voi tavoitteidensa saavuttamiseksi yhdistellä erilaista kerättyä dataa. Kerätty data voi olla portinvartijan itsensä suoraan keräämää dataa, luovutuksen kautta saatua dataa esimerkiksi yhtiökumppanilta, tytäryhtiöltä tai eri sopimuksin kolmannelta osapuolelta taikka data voi olla lähtökohtaisesti julkista. Tietojen yhdistämisessä voi tulla tilanne, jossa toinen tieto on anonyymiä ja toinen ei. Tällöin anonymisoitu data voi muuttua tunnistettavaksi, jos se kyetään yhdistämään toiseen dataan. Kyseessä ei siis olisi pseudonymisoitu data, vaan puhtaasti anonymisoitu data, joka jossain toisessa kontekstissa tai yhdistettynä julkiseen dataan voi muuttua tunnistettavaksi. Tällöin data palautuisi sinänsä lain nojalla henkilötietojen suojan piiriin.[265] Käytännössä tämä viittaisi siihen mahdollisuuteen, että liian yksityiskohtaista dataa ei ole edes mahdollista anonymisoida ilman, että se palautuu tunnistettavaksi tiedoksi jossain vaiheessa datan käsittelyä.[266] Vaikka lähtökohta on, ettei anonymisoitu data ole palautettavissa tunnistettavaan muotoon, voi siitä tulla – poikkeuksellisesti, mutta mahdollisesti – tunnistettava, mikä lisää riskiä anonymisoinnin käytölle.

Anonymisoinnin mahdollisuus henkilötietojen luovutuksessa voisi tulla kyseeseen, mikäli vastaanottava yrityskäyttäjä ei tarvitse datan käyttöön lainkaan henkilötietoja tai tilanteessa, jossa loppukäyttäjä ei antaisi yrityskäyttäjälle suostumusta henkilötietojensa vastaanottamiseen ja käsittelyyn. Yrityskäyttäjän pyynnössä tietojen saamiselle tulisi ilmetä, mikäli tiedot on mahdollista ja tarkoituksenomaista vastaanottaa anonyymisti. Kun otetaan huomioon

[264] Van Gorp ym., s. viii.
[265] Van Gorp ym. s. 15 ja Koenigswarter 2019.
[266] Esimerkiksi Yhdysvalloissa kaksi yliopiston tutkijaa (The University of Texas at Austin, USA) pystyivät uudelleentunnistamaan Netflixin julkaisemien arvostelujen taustalla olevat henkilöt, joiden tiedot olivat täysin anonymisoituja, kun he vertasivat anonymisoituja arvosteluja IMDb-nettisivun julkisiin elokuva-arvosteluihin. Ks. tapauksesta lisää Koenigswarter 2019.

luovutusvelvollisuuden tavoite ja luovutuksen oikeusperustana oleva suostumus, on epätodennäköistä, että portinvartija voisi täyttää luovutusvelvollisuuden vaatimuksen anonymisoimalla ainoastaan omalla päätösvallalla luovutettavissa olevat tiedot.

6.5.2 Pseudonymisointi

Tietosuoja-asetuksen mukaan pseudonymisoinnissa on kyse henkilötietojen käsittelemisestä niin, ettei henkilötietoja voida enää yhdistää yhteen tiettyyn rekisteröityyn käyttämättä lisätietoja. Näitä lisätietoja tulee säilyttää erillään pseudonymisoiduista henkilötiedoista ja niihin sovelletaan sellaisia toimenpiteitä, joilla varmistetaan, että henkilötietojen yhdistämistä rekisteröityyn ei tapahdu.[267] Pseudonymisoidut tiedot voivat näyttäytyä anonyymeinä, mutta ovat kuitenkin palautettavissa takaisin tunnistettavaan muotoon. Tyypillisin esimerkki tällaisista tiedoista on peitenimellä koodatut henkilöihin liittyvät tiedot, kuten nimi, syntymäaika ja osoite, joita säilytetään erikseen. Pseudonyymi tieto katsotaan siten henkilötiedoksi.[268] Henkilötietoja voi pseudonymisoinnilla minimoida, jolloin tietojen käsittely ja myös luovuttaminen voi helpottua.[269]

Kun henkilötietojen säilyttämiselle ei enää ole tietosuoja-asetuksen mukaista laillista käsittelyperustetta, on henkilötiedot poistettava tai anonymisoitava. Pseudonymisointi tarjoaa kuitenkin toimenpiteitä tietosuojariskien lieventämiseksi silloin, kun henkilötietojen käsittely on edelleen tarpeen. Pseudonymisointia käytetään yksilöiden yksityisyyden suojaamiseksi yleisesti esimerkiksi terveydenhuoltoalalla, jossa yksilöistä on kerättynä erityisesti suojattuja terveystietoja, joiden osalta pidetään kirjaa siitä, mitkä tiedot koskevat kutakin yksilöä. Pseudonymisoinnilla tietosuojaa parannetaan niin, ettei henkilötietoja esimerkiksi potilastiedoissa korvata muilla tiedoilla, vaan ne suojataan eri muuntamis- ja erotteluteknii-koiden avulla.[270]

Pseudonymisointi on olennaista myös sen arvioimisessa, voidaanko henkilötietojen myöhempää käsittelyä tai luovutusta toteuttaa eri tarkoituksiin kuin mihin ne on alun perin kerätty ilman rekisteröidyltä hankittavaa uutta suostumusta.[271] Pseudonymisointi voi vähentää

[267] TSA 4(5) artikla.
[268] WP 136, s. 18 ja Warma – Nieminen 2016, s. 555.
[269] Tietosuojavaltuutetun toimisto, henkilötietojen minimointi tieteellisessä tutkimuksessa.
[270] Zerdick 2021.
[271] TSA 6(4) artikla.

asianomaisiin rekisteröityihin kohdistuvia riskejä ja auttaa rekisterinpitäjiä tietosuojavelvoitteiden noudattamisessa.[272] Tästä johtuen pseudonymisointi voisi ainakin teoriassa helpottaa tietojen luovuttamista ja luovutusvelvollisuutta siltä osin, kun tietosuoja-asetus edellyttää käyttötarkoituksien yhdenmukaisuutta ja tietojen tarpeellisuutta.[273]

DMA:n edellyttäessä portinvartijan osalta joka tapauksessa henkilötietojen luovutukseen rekisteröidyn suostumusta, ei velvollisuuden täyttymiseksi riitä välttämättä pseudonymisointi yksinään. Lisäksi portinvartijan ja yrityskäyttäjän on noudatettava pseudonymisoitujen tietojen luovutuksessa muitakin tietosuoja-asetuksen mukaisia velvoitteitaan, ja informoitava rekisteröityä luovutuksesta ja yrityskäyttäjän uudesta tietojen käsittelystä.[274]

[272] TSA:n johdanto 28 kohta.
[273] Warma – Nieminen 2016, s. 555–556.
[274] Warma – Nieminen 2016, s. 556.

7 LOPUKSI

Suuret teknologiayhtiöt, jotka tarjoavat ydinalustapalveluita yksilöiden ja yrityksien käyttöön, ovat saavuttaneet datan keräämisellä ja kyvyllä muuttaa dataa arvoksi vankkumattoman aseman markkinoilla maailmanlaajuisesti.[275] Datan ominaisuuksien hyödyntämien ja dataan perustuvat liiketoimintamallit ovat asettaneet nämä yhtiöt sellaisiin portinvartijoiden asemiin, että heidän toimintansa vie tilaa pienemmiltä kilpailevilta toimijoilta. Portinvartijoiden toimintaa on arvioitu ja arvosteltu maailmanlaajuisesti etenkin kilpailun puutteen sekä tietosuojariskien vuoksi. Lainsäädäntöehdotuksia, joilla pyritään puuttumaan portinvartijoiden asemaan, on EU:n ohella syntynyt myös EU:n ulkopuolella esimerkiksi Iso-Britanniassa ja Yhdysvalloissa.[276] Yksilöiden halu hallita omaa dataa on korostunut ja tietoisuus portinvartijoiden asemasta kasvanut. EU:n tietosuoja-asetus on tuonut turvaa yksilöiden oikeuksille ja velvollisuuksia henkilötietojen käsittelylle. Tietosuoja-asetuksella ei kuitenkaan ole kyetty puuttumaan portinvartijoiden kilpailulliseen asemaan, eikä sen tarkoitus se ollutkaan. Jakamisen yhteiskunnassa, jossa tietoa kertyy jatkuvasti lisää, on ajauduttu jäämään sääntelyssä portinvartijoiden jälkeen. Ongelmaksi on muodostunut etenkin se, ettei kukaan näyttäisi edelleenkään täysin tietävän mitä ja kuinka paljon tietoja portinvartijat hallinnoivat ja miten tietoja käsitellään.[277]

Tutkielman keskiössä oli digimarkkinasäädöksen tuoma datan luovutusvelvollisuus datan ominaisuuksien ja tietosuojakysymysten näkökulmasta. Portinvartijayritykset tulevat uuden EU-tasoisen säädöksen myötä velvolliseksi luovuttamaan niiden keräämää ja hallussa olevaa dataa suoraan kilpailijoilleen. Tällöin tietosuojakysymykset yhdistyvät kilpailevien yritysten välillä. Digimarkkinasäädös osana EU:n laajempaa datatalouden lainsäädäntöuudistusta on aihealueena siinä määrin laaja, että rajaus ainoastaan eurooppaoikeudellisiin tietosuojakysymyksiin on ollut tarpeellinen. EU:n datatalouden lainsäädäntöuudistuksilla on pyritty luomaan sääntelykokonaisuus, joka kattaisi portinvartijoiden, rekisteröityjen ja datatalouden lainsäädäntöä kattavasti. Niin ikään tietosuoja-asetus on vahvasti datan hallinnoinnin taustalla vaikuttavana sääntelykehyksenä henkilötietojen osalta, ja se määrää sen, miten henkilötietoja sisältäviä tietoja voidaan laillisesti luovuttaa.

[275] Ks. Wiewiórowski 2019, kohta Some have more to share than others.
[276] Uusia lainsäädäntöesityksiä on tehty Yhdysvalloissa esim. American Innovation and Choice Online Act (AICO) sekä Iso-Britanniassa Digital Markets Unit (DMU).
[277] Wiewiórowski 2019, kohta Is it really just about the data?.

Tutkimuskysymyksenä se, miten tietosuoja-asetus tulee vaikuttamaan henkilötietojen luovuttamiseen digimarkkinasäädöksen mahdollistamana velvollisuutena yrityskäyttäjää kohtaan, kun yritysten toiminnassa noudatetaan yhtäaikaisesti tietosuoja-asetusta ja digimarkkinasäädöstä, edellytti kysymyksen tarkastelua osa-alueittain. Tutkielmassa ensimmäisenä arvioitiin datan merkitystä. Tämän tarkoituksena oli määrittää velvollisuuden kohteena olevan datan oikeudellista luonnetta itsessään. Tarkastelussa keskityttiin datan ominaisuuksien, sisällön, sääntelyn ja hyödyntämisen analysointiin. Tutkielmassa datan luovuttamisen oikeudellinen arviointi perustui datan jaottelulle henkilötietoja sisältäväksi dataksi ja muuksi dataksi. Datan läheisempi analysointi osoitti ne haasteet, joita datan määrittämiseen edelleen liittyy. Datan oikeudellinen asema ja sääntelykehys näyttäytyivät tutkimuksen tuloksena hyvinkin epäselvänä, kun otetaan huomioon datan yhteiskunnallisesti merkittävä asema niin määrältään kuin liiketoiminnassa hyödynnettävältä arvoltaan. Tähän osittaisena syynä näyttäisi olevan datan ominaisuudet, kuten jatkojalostettavuus ja muokattavuus.[278]

Datan sääntelyssä on tyypillistä, että useampi eri säädös soveltuu yhtäaikaisesti ja päällekkäin, eikä tästä syystä olekaan poikkeuksellista, että myös digimarkkinasäädöksen kohdalla huomioidaan erityisesti tietosuojalainsäädäntö. Tutkielmassa datan analysointi osoitti sen, että myös tietojen määrittely yksiselitteisesti henkilötiedoiksi ja muuksi tiedoiksi voi tulla ongelmalliseksi etenkin, jos tietojen luovutuksen kohteena tulisi olla suuret määrät jatkuvaa ja reaaliajassa olevaa datavirtaa. Sääntelyllä näytettäisiin tältä osin tähtäävän siihen, että datasta pitäisi kyetä käytännössä erottelemaan henkilötietoja sisältävä data kuin myös muu data, joka voi myös sisältää esimerkiksi liikesalaisuuksia. Tutkielmassa kävi ilmi, että datan sääntelykehikon ja sääntelyn tarpeellisuuden arviointi edellyttäisi kuitenkin sen tarkempaa analysointia omana tutkimuksenaan.

Datan ja datatalouden analysoinnin jälkeen tutkielmassa lähestyttiin tarkemmin henkilötietojen suojaa ja tietosuoja-asetusta. Tarkoituksena oli tuoda esille henkilötietojen sääntelykehystä Euroopan unionin tasoisen tietosuoja-asetuksen näkökulmasta. Analysointi aloitettiin yksityisyyden suojan määrittelystä. Tietosuoja-asetuksen tavoitteena on suojata luonnollisten henkilöiden perusoikeuksia ja -vapauksia sekä erityisesti heidän oikeuttaan henkilötietojen suojaan. Lisäksi asetuksen tavoitteena on varmistaa henkilötietojen vapaa liikkuvuus unionissa.[279]

[278] Ks. Tarkela 2016, s. 68.
[279] TSA 1 artikla ja esim. TSA:n johdanto 166 kohta.

Henkilötietojen suojan sääntely on kattavaa kaikessa henkilötietojen käsittelyssä. Tietosuoja-asetus korostaa henkilötietojen käsittelyn lainmukaisuuden lisäksi yleisesti soveltuvia tietosuojaperiaatteita, joiden noudattaminen ei riipu siitä, mitä käsittelyperustetta rekisterinpitäjä toiminnassaan hyödyntää. Datan jakaminen on tietosuoja-asetuksessa mahdollista pääasiassa kahdella eri tavalla: rekisterinpitäjän vapaaehtoisena toimena jakaa tietoja kolmannelle osapuolelle ja rekisteröidyn omaan pyyntöön perustuvana toimena TSA 20 artiklan nojalla. Tietosuoja-asetus ei kuitenkaan sellaisenaan vastaa kilpailuoikeudelliseen tarpeeseen velvoittaa portinvartijaa luovuttamaan dataa yrityskäyttäjilleen, joilla ei muutoin ole mahdollisuutta hyödyntää heidän itsensä tai heidän omien palveluiden käyttämisestä kertyvää dataa, saati edes saada kyseistä dataa itselleen ydinalustapalvelun tarjoajalta.

Tutkielmassa lähestyttiin tietosuoja-asetuksen ja digimarkkinasäädöksen yhteentoimivuutta näiden sääntelyjen sanamuodon mukaisen tulkinnan sekä systemaattisen ja teleologisen tulkinnan mukaisesti. Keskeisimpänä havaintona tehtiin se, että digimarkkinasäädöksen tavoite on vahvasti kilpailuoikeudellinen, toisin kuin tietosuoja-asetuksen. Tämä asettaa jo lähtökohtaisesti näiden säädösten yhdistämisen mielenkiintoiseen asemaan. Tilanne ei sinänsä ole poikkeuksellinen, kun otetaan huomioon säädösten päällekkäisen soveltamisen tavanomaisuus ylipäätään. Mielenkiintoisen tästä näyttäisi kuitenkin tekevän kilpailuoikeuden ja tietosuojalainsäädännön yhdistäminen. Tutkielmassa käsiteltiin aihetta suurpiirteisesti nimenomaan digimarkkinasäädöksen vahvan kilpailullisen tavoitteen ja perustan vuoksi, menemättä kuitenkaan tältä osin tarkempaan analysointiin, mikä olisi edellyttänyt jo tutkielman alusta lähtien enemmän kilpailuoikeudellista näkökulmaa. Tarkastelun tuloksena havaittiin erityisesti se, että näiden oikeudenalojen yhdistämisessä vallitsee edelleen epäselvyyttä. Tietosuojakysymysten ja kilpailuoikeuden yhteentoimivuutta on arvioitu oikeuskirjallisuuden lisäksi oikeuskäytännössä esimerkiksi EU-tuomioistuimessa. Vaikka oikeuskäytäntö ei vielä ole antanut täysin yhteneväisiä tulkintalinjauksia, havaittiin tutkielmassa, että näiden kahden oikeudenalan välinen kuilu on jo nyt pienentynyt.

Digimarkkinasäädöksessä datan luovuttaminen asettaa portinvartijoille uuden velvollisuuden luovuttaa liiketoimintansa perustana olevaa tietoa kilpailijoilleen saamatta tästä kompensaatiota. DMA 6(10) artikla edellyttää pyyntöön perustuvaa luovutustoimea, joka on maksuton, tehokas ja korkealaatuinen. Tietojen tulee olla yrityskäyttäjien itsensä tuottamia tai yrityskäyttäjien palveluita käyttävien loppukäyttäjien tuottamia. Tietosuoja-asetuksen

näkökulmasta edellä mainitut edellytykset näyttäytyivät selkeimmiltä. Arvioinnissa lähdettiin siitä, mitä edellytetään, kun tieto on jo määriteltävissä henkilötiedoksi. Henkilötietojen luovutusta ei ole DMA:ssa rajattu luovutusvelvollisuudesta pois, mutta sen soveltamiseksi on asetettu lisäehtoina tietojen suora liityntä yrityskäyttäjän tarjoamien tuotteiden ja palveluiden käyttöön sekä rekisteröidyltä suostumuksen saaminen luovutustoimelle.

Henkilötietojen luovutuksessa on aina tietosuojaoikeudellinen riski lähinnä siitä syystä, että tiedot yksinkertaisesti siirtyvät toimijalta toiselle. DMA:ssa on rajattu portinvartijan henkilötietojen käsittelyperusteeksi tietojen luovuttamisessa rekisteröidyltä saatava suostumus. Tämän vuoksi tutkielmassa tarkasteltiin luovutustoimesta ensin suostumuksen luonnetta tietosuoja-asetuksen mukaisena käsittelyperusteena.

Tiukasti rajattuna toimena suostumus voi käytännössä osoittautua haastavaksi toteuttaa. Suostumuksen tulee olla vapaaehtoinen, tietoinen ja yksilöity toimi. Nämä edellyttävät, että luovutustoimen tulee olla tapauskohtaista, eikä sen kohteena voi olla kohtuuttoman suuria kokonaisuuksia. Suostumuksessa olennaista on myös se, että rekisteröidyllä tulee olla tiedossa kyseessä olevan yrityskäyttäjän vastaanotettavien henkilötietojen käyttötarkoitus, mikä korostaa yhdessä käyttötarkoitussidonnaisuuden kanssa rekisteröidyn etukäteistä informointia etenkin aiotusta käyttötarkoituksesta. Riippumatta siitä, että suostumuksen hyödyntämisessä on haasteita, havaittiin tutkielmassa, että se on kuitenkin yrityskäyttäjän näkökulmasta kannattavin peruste henkilötietojen vastaanottamiseksi ja käsittelemiseksi. Lakisääteisen velvoitteen täyttäminen ja oikeutettu etu käsittelyperusteina ovat suostumuksen saamista epävarmempia ja siten hyödynnettävinä epätodennäköisiä. Portinvartijan kannalta suostumuksen edellytykset ja tietosuojaperiaatteet korostavat käytännössä tapauskohtaista harkintaa luovutuksien suhteen sekä estävät massaluovutuksien ja etukäteisten suostumuksien käyttämisen.

Olennaista suostumuksen osalta on se, että rekisteröidyllä on mahdollisuus kieltäytyä sen antamisesta tai mahdollisuus peruuttaa antamansa suostumus. Tietosuoja-asetus voi siten estää luovutusvelvollisuuden täyttymisen ainakin teoriassa, koska toimen laillinen peruste on digimarkkinasäädöksessä rajattu suostumukseen. Tällä on siis suljettu pois se mahdollisuus, että suostumuksen saamatta jäämisessä portinvartijan tulisi esimerkiksi laillisen velvoitteen täyttämiseksi luovuttaa dataa joka tapauksessa. Suostumuksen saamatta jääminen – ja siten myös luovutusvelvollisuuden täyttämättä jääminen – ei kuitenkaan toteuta

digimarkkinasäädöksen kilpailuoikeudellista tavoitetta ja tavoitetta myöntää pääsyä dataan, mitä voisi arvioida suhteessa yksilön tiedollisen itsemääräämisoikeuden toteutumiseen suostumuksen antamisena.

Portinvartijoiden tähänastinen logiikka suostumuksien saamiselle on ollut se, että suostumus on nimenomaan pyritty saamaan mahdollisimman kattavasti kaikkeen mahdolliseen käsittelyyn ja vähän sen ylikin. Kun luovutusvelvollisuus voidaan tietosuoja-asetuksen nojalla jättää täyttämättä, mikäli suostumusta ei saada, voisi menettely muuttua tältä osin toiseksi. Kyseessä olisi tilanne, jossa portinvartijat voisivat pyrkiä siihen, että suostumuksen antaminen näyttäytyisi loppukäyttäjille epäedullisena ja tietosuojaoikeudellisesti turvattomana toimena, mikä johtaisi toivotusti siihen, ettei suostumusta luovutukseen edes saada.

Mikäli portinvartija ei saisi luovutukselle rekisteröidyltä suostumusta, voisi kyseeseen mahdollisesti tulla henkilötietojen anonymisointi ja anonyymien tietojen luovuttaminen. Anonymisoinnin osalta tutkielmassa havaittiin, että anonymisointi, jonka tarkoitus olisi kiertää henkilötietojen luovutus, ei ole mahdollista. Jotta voidaan varmistaa se, ettei yrityskäyttäjä koe datasta saamaansa hyötyä menetetyksi, tulisi tietojen anonyymina luovuttaminen perustua yrityskäyttäjän omaan pyyntöön saada tiedot nimenomaisesti anonyymeina. Pseudonymisointi voisi taas vähentää sinänsä tietosuojariskejä yksilöiden osalta, mutta ei kuitenkaan poista tietosuoja-asetuksen soveltumista muilta osin. Näin käsittelyperusteiden ja tietosuojaperiaatteiden soveltaminen tulevat edelleen kyseeseen. Henkilötietojen luovuttamisessa riskinä vaikuttaisi olevan suostumuksen saamisen lisäksi käyttötarkoituksien yhteensopivuuden menettäminen silloin, kun tietoja siirretään toimijalta toiselle.

Tietosuojakysymykset ovat nousseet merkittäväksi osaksi datan ympärillä käytävää keskustelua. Tutkielma osoittaa, että tietosuojaoikeudellisten ja kilpailuoikeudellisten kysymysten yhdistyminen on olennaista säädösten arvioinnissa. Tietosuojan ei tulisi vaarantua datan luovutuksessa, mutta käytännön toteuttaminen asettaa sen haasteelliseksi. Digimarkkinasäädöksen asettamilla velvoitteilla odotetaan olevan suuri vaikutus markkinoihin siinä olevan käyttäjädatan avaamisen vuoksi. Asetuksen voimaantulon myötä, sen tulkinta ja oikeuskäytäntö tulevat kuitenkin lopulta osoittamaan sen, kuinka suuresta vaikutuksesta on kyse.[280] Ei voida pitää vielä selvänä, miten digimarkkinasäädöksen asettamat uudet

[280] TEM 2022, s. 30.

velvoitteet tulevat suoraan vaikuttamaan henkilötietojen suojaan ja loppukäyttäjien yksityisyyteen. Portinvartijoiden lisäksi datan luovutusta tullaan mitä todennäköisemmin arvioimaan eri tavoin myös niiden muiden toimijoiden näkökulmasta, joihin tietosuoja-asetuksen sääntely yltää.[281]

Digimarkkinasäädös, tietosuoja-asetus ja kilpailulainsäädäntö yhdessä sääntelevät päällekkäisesti pakollisen datan luovutusvelvollisuuden järjestelmää, eivätkä sulje toisiaan pois. Siksi on tärkeää, että nämä kolme kokonaisuutta toimivat digimarkkinasäädöksen tavoitteen mukaisesti yhteensopivasti ja vuorovaikutuksessa keskenään.

[281] CIPL 2021, s. 3.