SITRA

MUISTIO

25.1.2024

Sanna Toropainen

OIKEUS DATAN SIIRTÄMISEEN JÄRJESTELMÄSTÄ TOISEEN REILUSSA DATATALOUDESSA

Kuinka laajentaa yksilöiden oikeutta hyötyä tietojensa hallinnasta

Sitran muistio
© Sitra 2024

Oikeus datan siirtämiseen järjestelmästä toiseen reilussa datataloudessa – Kuinka laajentaa yksilöiden oikeutta hyötyä tietojensa hallinnasta

Kirjoittaja: Sanna Toropainen

Sitran työryhmä: Kristo Lehtonen, Meeri Toivanen, Reijo Aarnio, Kristine Alanko, Johanna Kippo
Taitto: PunaMusta Oy

ISBN 978-952-347-349-2 (PDF)
ISSN 2737-1034 (verkkojulkaisu)
www.sitra.fi

Sitran muistiot ovat tulevaisuustyömme taustaksi tuotettuja sisältöjä.

Sisällysluettelo

Esipuhe

Digitaalisessa muodossa tallennettu tieto eli data on aikamme arvokkain resurssi. Meidän kunkin henkilötietomme kertovat yksityiskohtaista tarinaa siitä, keitä olemme kuluttajina, äänestäjinä ja yhteiskunnan jäseninä. Yrityksille data on elintärkeä osa prosessien optimointia ja innovatiivisten ratkaisujen kehittämistä vastaamaan aikamme merkittäviin haasteisiin ilmastokriisistä ja luontokadosta terveyskriiseihin ja disinformaatioon. Tällä hetkellä käsillä on historiallinen teknologian ja talouden murros, jossa digitalisaation eteneminen ja datan määrän räjähtävä kasvu muuttavat yhteiskuntia. Datan avulla on mahdollista tehdä paljon hyvää, mutta meillä on vastassamme myös ongelma. Nykyinen datatalous ei ole reilu, koska se vahvistaa muutaman digijätin valtaa yksilöiden ja yhteiskuntien kustannuksella.

Datataloudessa reiluus tarkoittaa sitä, että yksilöiden oikeuksia suojellaan ja kaikkien osapuolten tarpeet otetaan huomioon. Me uskomme, että nykyisen datatalouden muuttaminen reilummaksi vaatii teknologisia, taloudellisia ja lainsäädännöllisiä innovaatioita, jotka tukevat erityisesti yksilöiden oikeuksia, koska he ovat perinteisesti olleet datataloudessa heikoimmassa asemassa. Tällä hetkellä me ”maksamme” käyttämistämme digitaalisista palveluista datallamme ja meillä on hyvin vähän tai ei lainkaan näkymää siihen, miten meistä kerättyä dataa käytetään ja kuka sitä käyttää. Jotta datatalous voi toimia, meidän yksilöinä on pystyttävä paremmin hallitsemaan dataamme ja kokemuksiamme digitaalisessa maailmassa. Esimerkiksi mahdollisuutemme päästä käsiksi meistä kerättyyn dataan ja siirtää se kilpailevan palvelun käyttöön on reilun, ihmiskeskeisen datatalouden kulmakivi.

Yksityisyyden suoja ja kuluttajansuoja eivät riitä vastaamaan tähän haasteeseen. Reilussa datataloudessa kuluttajilla on oltava myös taloudellinen oikeus. Tämän muistion tarkoituksena on tutkia, voisiko oikeus siirtää dataa järjestelmästä toiseen olla osa ratkaisua.

Euroopan unionissa on luotu kunnianhimoista datataloutta koskevaa lainsäädäntöä, alkaen vuoden 2016 yleisestä tietosuoja-asetuksesta (GDPR). Se toi yksilöille oikeuden siirtää henkilötietojaan järjestelmästä toiseen, vahvistaen yksilöiden asemaa datataloudessa suhteessa yrityksiin.

Vuoden 2020 datastrategiassa Euroopan komissio asetti tavoitteeksi viedä eteenpäin datan siirrettävyyden periaatteen toimeenpanoa, jotta yksilöiden asemaa voitaisiin tukea datataloudessa. Kun datastrategiaa seurannutta datasääntelyä ja muita lainsäädännöllisiä keinoja tarkastellaan kokonaisuutena, voidaan todeta, että käynnissä on todellinen sääntelytsunami. Euroopan unioni pyrkii uudella sääntelyllään näyttämään tietä maailmanlaajuisesti hyödyntämällä sisämarkkinansa voimaa (ns. Bryssel-efekti). Datastrategian kunnianhimoisimpia ehdotuksia on uusi datasäädös, joka laajentaa datan siirrettävyyden periaatteen koskemaan esineiden internetiin (IoT) liitettävien laitteiden tuottamaa dataa ja tarjoaa laajemman lainsäädännöllisen perustan kuin yleinen tietosuoja-asetus.

Varmistamalla, että oikeus datan siirtämiseen voidaan panna täytäntöön mahdollisimman helposti ja tehokkaasti, on myös keino vahvistaa digitaalista itsemääräämisoikeuttamme ja tehdä datataloudesta entistä reilumpaa. Asiaan on kiinnitettävä huomiota, koska uudet teknologiat, kuten virtuaalitodellisuudet, ja entistä tiiviimmin meihin kytketyt laitteet, kuten VR-lasit, tulevat vaikeuttamaan tilannetta entisestään. Enemmän kuin koskaan tarvitsemme nyt uusia tapoja tasapainottaa digijättien markkinavoimaa suhteessa yksilöiden ja pienempien yritysten asemaan.

Haluamme kiittää muistion kirjoittajaa Sanna Toropaista, joka sopi raportin kirjoittajaksi erityisen hyvin alan oikeudellisena asiantuntijana ja datanvälityspalveluyrityksen toimitusjohtajan ja perustajan taustansa vuoksi. Haluamme myös kiittää kaikkia niitä Euroopan komission, jäsenmaiden, viranomaisten, kansalaisjärjestöjen ja yritysten asiantuntijoita, jotka osallistuivat European Policy Centerin kanssa toteuttamaamme pyöreän pöydän tilaisuuteen Brysselissä toukokuussa 2023. Tämä tilaisuus, joka oli osa Datastrategia 2.0 -hankettamme, poiki useita suosituksia seuraaviksi askeliksi Euroopan digipolitiikan viemisessä eteenpäin. Tilaisuudessa käyty vuoropuhelu vei selvitystämme merkittävästi eteenpäin.

21.6.2023

Kristo Lehtonen
Reilun datatalouden teemajohtaja, Sitra

Reijo Aarnio
vanhempi neuvonantaja, Sitra
entinen tietosuojavaltuutettu

Tiivistelmä

Yksilöiden oikeutta hallita omaa dataansa tulee vahvistaa digitaalisen ajan perusoikeutena, kuten Sitra on esittänyt suosituksissaan digitaalisen vallan epätasapainon korjaamiseksi (Sitra 2022a). Lähtökohtana on, että yksilön tulee voida tietää, mitä dataa hänestä kerätään ja miten sitä käsitellään ja jaetaan. Hänellä tulee myös olla todellinen mahdollisuus vaikuttaa datan keruun ja käsittelyn eri vaiheissa sekä mahdollisuus siirtää häntä koskevaa dataa järjestelmästä toiseen. Oikeus siirtää dataa järjestelmästä toiseen on yksi tapa pyrkiä korjaamaan nykyistä vallan epätasapainoa yksilöiden ja heistä kerättyä dataa yhdistelevien ja sillä ansaitsevien teknologiatoimittajien välillä.

Tässä muistiossa todetaan, että oikeus datan siirtämiseen on keskeinen osa reilua datataloutta, koska myös yksilöiden tulisi olla aktiivisia toimijoita datataloudessa yritysten ja instituutioiden rinnalla. Heillä tulisi olla päätäntävaltaa heistä kerättyyn ja heitä koskevaan dataan sen sijaan, että heitä pidetään vain suojaamista tarvitsevina osapuolina.

Oikeus datan siirtämiseen ei ole absoluuttinen oikeus, vaan se tulee tasapainottaa suhteessa muihin oikeuksiin ja vapauksiin. Muistiossa analysoidaan ensin Euroopan unionin lainsäädännöllistä viitekehystä, joka koskee datan siirtämistä. Johtopäätöksenä on, että nykyinen lainsäädäntökehys lähestyy datan siirtämisen oikeutta sirpaleisesti, olipa kyse sitten tuon oikeuden sisällöstä tai toimeenpanosta. Tämä voi vaikeuttaa yksilöiden mahdollisuuksia käyttää täysimääräisesti oikeuttaan oman datansa siirtämiseen.

Oikeus datan siirtämiseen on lähtöisin yleisen tietosuoja-asetuksen (GDPR) artiklasta 20. Muistio luo katsauksen sitä seuranneisiin lainsäädäntöehdotuksiin datan siirtämisen oikeuden laajentamisesta. Niissä se ulottuisi kattamaan henkilötietojen lisäksi myös verkkoon kytkettyjen laitteiden ja palveluiden käytössä syntynyttä dataa (komission ehdotus datasäädökseksi) ja terveysdataa (komission ehdotus eurooppalaisesta terveystietoalueesta). Muistio käy myös läpi, miten EU:n digimarkkinasäädös (DMA) käsittelee oikeutta datan siirtämiseen. Analyysi osoittaa, miten ehdotettu lainsäädäntö kokonaisuutena ulottaa oikeuden datan siirtämiseen koskemaan muutakin dataa kuin vain henkilötietoja ja ihmisten ”antamia” tietoja. Samanaikaisesti oikeutta datan siirtämiseen rajaavat toimialakohtaiset erot toimeenpanossa ja GDPR:n artikla 20:n asettamat rajoitukset.

Oikeudellisen tarkastelun lisäksi muistiossa nostetaan esiin neljä käytännön rajoitusta datan siirtämiselle. Näitä ovat puutteellinen toteutus yrityksissä, yksityisyydensuojaan ja tietoturvaan liittyvät riskit, puutteet yhteentoimivuudessa ja välittäjäpalveluiden roolien epäselvyys.

Virtuaalitodellisuudet ja web 3.0 -teknologiat tarjoavat mahdollisuuden tarkastella datan siirtämisen soveltamista oikeudellisen kehyksen ja tunnistettujen käytännön haasteiden kautta. Ne edustavat tulevan teknologisen kehityksen aluetta, jossa käyttäjien osallisuudella on entistäkin keskeisempi rooli. Web 3.0:n hajautettu päätöksenteko mahdollistaa datan hienojakoisemman hallinnan ja yksilön vahvemman päätösvallan toteutumisen datatalousessa. Samalla virtuaaliympäristö ja siihen liittyvä kasvava arkaluontoisen datan keruu saattavat aiheuttaa uusia uhkia yksityisyydensuojalle.

Lopuksi muistiossa ehdotetaan neljää mahdollisuutta, joilla oikeutta datan siirtämiseen voidaan vahvistaa ja siten edistää reilumman datatalouden kehitystä sääntelyn avulla Euroopan unionissa. Ensinnäkin GDPR:n artiklaa 20 voisi laajentaa niin, että se koskisi yksilöiden ”antamien” henkilötietojen lisäksi myös ”yhdisteltyä” dataa. Tämän lisäksi artikla 20:n soveltamisalaa tulisi laajentaa niin, että yksilöt voisivat käyttää oikeutta henkilötietojen käsittelyperustasta riippumatta, jotta he voisivat käyttää datan siirto-oikeutta myös suhteessa julkisen sektorin toimijoihin. Toisena vaihtoehtona on GDPR:n artiklan 20 ulottaminen koskemaan myös muuta dataa kuin henkilötietoja (nk. yhdistetyt data-aineistot), jolloin se ottaisi huomioon datan monimuotoisen luonteen. Näin voitaisiin varmistaa, että oikeus datan siirtämiseen toimii tehokkaasti käytännössä. Kolmanneksi oikeus datan siirtämiseen voitaisiin liittää Euroopan unionin perusoikeuskirjaan yksityisyyden suojan ja tietosuojan lisäksi erillisenä oikeutena. Se voisi pitää sisällään oikeuden hallita omaa dataansa ja oikeuden siitä saataviin taloudellisiin hyötyihin. Neljäntenä vaihtoehtona on uusi lainsäädäntö, joka määrittäisi tarkasti, millaista dataa voidaan siirtää ja jonka soveltamisala olisi kuitenkin riittävän laaja. Tämä voisi parantaa ihmisten mahdollisuutta päättää heitä koskevan datan käytöstä.

Sammanfattning

Individens rätt att kontrollera sina egna data måste stärkas som en grundläggande rättighet i den digitala tidsåldern, vilket Sitra föreslagit i sina rekommendationer för korrigering av obalansen i den digitala makten (Sitra 2022a). Den bakomliggande idén är att individer ska ha möjlighet att veta vilken data om dem som samlas in, bearbetas och delas. De måste också ha en verklig möjlighet att påverka de olika stadierna av insamlingen och behandlingen av data samt möjligheten att överföra data om dem från ett system till ett annat. Rätten att överföra data från ett system till ett annat är ett sätt att ta itu med den nuvarande maktobalansen mellan individer och de teknikleverantörer som kombinerar och tjänar pengar på data som samlats in från dem.

Det här dokumentet hävdar att rätten till dataportabilitet är ett nyckelelement inom den rättvisa dataekonomin eftersom individer bör vara aktiva deltagare som arbetar tillsammans med företag och institutioner, med ett avgörande inflytande över sina data snarare än att bara vara subjekt i behov av skydd.

Eftersom rätten till dataportabilitet inte är en absolut rättighet utan måste balanseras mot andra rättigheter och friheter, börjar detta dokument med att analysera den rättsliga ramen i Europeiska unionen som styr denna rättighet. Slutsatsen är att det nuvarande ramverket riskerar att anta ett stycke-vis förhållningssätt till rätten till dataportabilitet både i sak och efterlevnad, vilket kan få skadliga effekter för individer som utnyttjar sin rätt till dataportabilitet fullt ut.

Med utgångspunkt i ursprunget till rättigheten i artikel 20 i den allmänna dataskyddsförordningen (GDPR), ger dokumentet en översikt över de lagförslag som utökar omfattningen av dataportabilitet från personuppgifter till data som genereras genom användning av anslutna enheter och relaterade enheter och tjänster (den föreslagna datalagen) och till hälsodata (Den europeiska hälsodatarymden) samt tittar på hur rätten beaktas i EU:s rättsakt om digitala marknaders dataportabilitet (DMA, Digital Markets Act).

Analysen pekar på hur de föreslagna lagstiftningsakterna utökar omfattningen av dataportabilitet till icke-personliga uppgifter och bortom uppgifter som "tillhandahålls av" individerna, men samtidigt förblir begränsade på grund av sektoriell tillämpning och begränsningar vad gäller tillämpningsområdet för artikel 20 i GDPR.

Utöver den rättsliga ramen observerar dokumentet fyra nuvarande begränsningar för dataportabilitet från praxis: otillräcklig implementering av företagen, risker för integritet och datasäkerhet, bristande kompabilitet och mellanhändernas oklara roll.

VR- och webb 3.0-tekniker undersöks som ett användningsfall för dataportabilitet mot det rättsliga ramverket och de identifierade implementeringsutmaningarna eftersom de representerar ett område för framtida tek-

nisk utveckling med intensifierad användarmedverkan. Där decentraliserat beslutsfattande inom webb 3.0 möjliggör mer detaljerad kontroll över data och självbestämmande i dataekonomin, kan den virtuella miljön utgöra nya typer av integritetsrisker på grund av en ökande datainsamling av känslig data.

Slutligen undersöker artikeln fyra möjligheter till att förbättra rätten till dataportabilitet för att genom reglering främja utvecklingen av en mer rättvis dataekonomi i Europa. För det första kunde artikel 20 i GDPR utvidgas på så sätt att den gällde utöver personuppgifter som individer ”gett” även ”kombinerad” data. Dessutom bör tillämpningsområdet för artikel 20 utvidgas så att individerna kan utöva sin rättighet oavsett på vilken grund deras personuppgifter behandlas, så att de kan utöva rätten till dataportabilitet även i förhållande till aktörer inom den offentliga sektorn. För det andra, en utvidgning av tillämpningsområdet för artikel 20 i GDPR utöver personuppgifter till att även omfatta icke-personliga uppgifter (blandade datauppsättningar) skulle återspegla uppgifternas dynamiska natur och skulle kunna säkerställa att rätten till dataportabilitet fungerar effektivt i praktiken. För det tredje, rätten till dataportabilitet skulle kunna “läggas till” i EU:s stadga om de grundläggande rättigheterna vid sidan av rätten till privatliv och dataskydd, omfattande både självbestämmande (kontrollerande) av sin data och rätten till de ekonomiska fördelarna hos denna data. Slutligen kan ny lagstiftning med en specifik definition av de uppgifter som kan porteras och med en tillräckligt bred tillämpning förbättra individers självbestämmande när det gäller deras uppgifter.

Summary

The right of individuals to control their data must be strengthened as a basic right in the digital age, as proposed by Sitra in its recommendations for rectifying the imbalance of digital power (Sitra 2022a). The starting point is that individuals should be able to know what data is collected about them and how it is processed and shared, and to have a sovereign say in the process, including the right to data portability. The right to data portability is a way of redressing the current power imbalance between individuals and the technology providers that aggregate and monetise the data collected about individual users.

This paper argues that the right to data portability is a key element in the fair data economy because individuals should be active participants working alongside companies and institutions with a sovereign say on their data rather than just subjects in need of protection.

As the right to data portability is not an absolute right, but has to be balanced with other rights and freedoms, this paper first analyses the legal framework in the European Union governing the right to data portability. It concludes that the current framework risks taking a piecemeal approach to the right to data portability, both in substance and in enforcement, which could have a detrimental effect on the ability of individuals to fully exercising it.

Starting with the origin of the right in Article 20 of the General Data Protection Regulation (GDPR), the paper provides an overview of the legislative proposals that extend the scope of data portability from personal data to data generated by the use of connected devices and related services (the proposed Data Act) and to health data (the European Health Data Space), and looks at how the right is considered in the Digital Markets Act (DMA). The analysis shows how the proposed legislation broadens the scope of data portability to non-personal data and beyond data 'provided by' individuals, but at the same time remains limited due to sectoral application and limitations on the scope of Article 20 of the GDPR.

In addition to the legal framework, the paper identifies four current practical limitations to data portability: inadequate implementation by the companies, privacy and data security risks, lack of interoperability, and the unclear role of intermediaries.

Virtual realities and web 3.0 technologies are examined as a use case for data portability in light of the legal framework and the implementation challenges identified, because they represent an area for future technological developments with increased user involvement. While the decentralised decision-making of web 3.0 allows for more granular control over data and empowerment in the data economy, the virtual environment may pose new privacy risks due to the increased collection of sensitive data.

Lastly, the paper explores four ways in which the right to data portability could be strengthened to further the development of a fairer data economy in Europe through regulation. First, widening the scope of Article 20 of the GDPR beyond personal data 'provided by' the data subject to include inferred data could enable individuals to use the right more broadly. Thus, allowing individuals to port their data regardless of the legal base, would enable individuals to invoke the right against public authorities. Second, expanding the scope of Article 20 of the GDPR beyond personal data to include non-personal data (mixed data sets) would reflect the dynamic nature of data, and could ensure that the right to data portability works effectively in practice. Third, the right to data portability could be 'added' to the EU Charter of Fundamental Rights, alongside the right to privacy and data protection, to include both the right to control one's own data and the right to the economic benefits from data. Finally, new legislation with a specific definition of the data that can be transferred, and with a sufficiently broad application could improve the self-determination of individuals with regard to their data.

1. Johdanto

Päivittäinen toimintamme, valintamme ja mieltymyksemme digitaalisessa ympäristössä synnyttävät valtavan määrän dataa ja se kasvaa räjähdysmäisesti. Tämä data voi olla arvokasta raaka-ainetta, kun innovoidaan parempia palveluita ja ratkaisuja, joilla voidaan vastata esimerkiksi ilmasto- ja luonnonvarakriisiin sekä luonnon monimuotoisuuden kriisiin. On kuitenkin tärkeää ottaa yksilöt mukaan aktiivisiksi datatalouden toimijoiksi ja asettaa heidän etunsa etusijalle (Euroopan komissio 2020a). Euroopan komissio määrittelee datatalouden talouden osa-alueeksi, joka perustuu täysin tai suurelta osin datan käyttöön ja hyödyntämiseen eri tavoin ja jossa datan saatavuus ja käytettävyys on varmistettu (Euroopan komissio 2017a). Euroopan unionissa datavetoinen siirtymä rakentuu eurooppalaisille arvoille, ihmiskeskeisyydelle ja reiluudelle. Reiluus datataloudessa tarkoittaa sitä, että yksilöiden oikeuksia suojellaan ja kaikkien osapuolten tarpeet otetaan huomioon tasapuolisesti. Tähän kuuluu yhtenä osana oikeus siirtää dataa järjestelmästä toiseen.

Yleisen tietosuoja-asetuksen (General Data Protection Regulation, GDPR) 20 artiklassa kuvattu oikeus siirtää tiedot järjestelmästä toiseen antaa Euroopan kansalaisille oikeuden saada yritysten käsittelemät, heitä itseään koskevat henkilötiedot ja siirtää ne toiselle yritykselle. Oikeus siirtää data järjestelmästä toiseen vahvistaa yleisen tietosuoja-asetuksen 15 artiklassa määritettyä rekisteröidyn oikeutta saada pääsy tietoihin, joka takaa yksilöille oikeuden saada tietää heidän henkilötietojensa käsittelystä. Yleinen tietosuoja-asetus onkin ensimmäinen horisontaalinen laki, joka sisältää yksilöiden oikeuden siirtää datansa järjestelmästä toiseen.

Oikeus siirtää tiedot järjestelmästä toiseen on työkalu, jolla voidaan oikaista vallan epätasapainoa yksilöiden ja teknologiatoimittajien välillä (De Hert ym. 2018). Sitran selvitys osoitti, että yksilöillä on vain vähän valtaa päättää heitä koskevan datan käytöstä, kun samalla muutama yhdysvaltalainen teknologiayritys on keskittänyt itselleen taloudellista valtaa yhdistelemällä käyttäjien dataa ja tienaamalla sillä mainosrakenteen kautta (Sitra 2022a).

Suurin osa tästä datasta kerätään käyttäjien suostumuksella käyttäen ns. evästeteknologioita, jotka seuraavat käyttäjiä eri verkkosivustoilla. Evästeiden käyttöä on kritisoitu avoimuuden puutteesta: vain harvat ymmärtävät suostuneensa henkilötietojensa siirtoon kolmansille osapuolille tai sitä, millaisia seurauksia siitä aiheutuu (Euroopan komissio 2017b). Kuluttajajärjestöt peräänkuuluttavat EU:ta muuttamaan evästeitä koskevia säädöksiään ja hyväksymään jo vuonna 2017 esitetyn sähköisen viestinnän tietosuoja-asetuksen eli ePrivacy-asetuksen pikaisesti (BEUC 2021). Nykymuodossaan ePrivacy-asetusehdotus ei kuitenkaan ota kantaa evästeiden avulla kerätyn datan tuottaman arvon jakamiseen useammille ja uhkana onkin (epäreilun) datatalouden nykytilan jatkuminen.

Nykymuotoiseen ePrivacy-asetusehdotukseen verrattuna datan siirrettävyys lupaa yksilöille mahdollisuutta päästä ”jakamaan big datan luomaa varallisuutta” ja saada päätösvaltaa omaan dataansa (29 artiklan mukainen työryhmä 2014). Datan siirtämisen oikeutta on kuitenkin otettu heikosti käyttöön liike-elämässä, koska kannustimet sen mahdollistamiseen ovat puutteellisia, kun taas yksilöiltä puuttuu tietoa oikeuden käytöstä. Yleisen tietosuoja-asetuksen voimaantulon jälkeen syitä vähäiseen datan siirtämiseen ovat olleet muun muassa oikeuden rajallinen soveltamisala, oikeuden tekniseen soveltamiseen liittyvät haasteet ja eri palveluiden yhteentoimivuuden puutteet, mikä haittaa oikeuden käytettävyyttä, kun yksilöt eivät pysty siirtämään henkilötietojaan alustalta toiselle (Euroopan komissio 2020a).

Euroopan komissio teki vuonna 2022 kaksi uutta lainsäädäntöehdotusta, datasäädöksen ja eurooppalaisen terveystietoalueen (EHDS), jotka toteutuessaan vahvistaisivat yksilöiden oikeutta datan siirrettävyyteen. Näistä ensimmäinen säätelee verkkoon kytkettyjen laitteiden datan saatavuutta ja jakamista (Euroopan komissio 2022a). Jälkimmäinen takaa oikeuden terveystietojen siirtämiseen ja niiden toisiokäyttöön (Euroopan komissio 2022c).

Uusien ehdotusten tavoitteena on jakaa datan tuottamaa arvoa tasaisemmin erikokoisten yritysten ja dataa tuottavien yksilöiden välillä. Tästä seuraisi kilpailukykyisempi ja nykyistä toimivampi datan jakamisen markkina Euroopassa, jossa yleinen tietosuoja-asetus ja sen 20 artikla ovat ensisijaisia välineitä yksilöiden perusoikeuksien toteutuksessa.

Vaarana on, että uudet ehdotukset luovat hajanaisen lähestymisen datan siirrettävyyteen ja oikeuden soveltamisala muuttuu niin kontekstisidonnaiseksi ja monimutkaiseksi, etteivät yksilöt pysty käyttämään sitä (Tombal & Graef 2023). Datan siirrettävyyttä koskevaan oikeuteen liittyvä monimutkaisuus vain lisääntyy uusien teknologisten suuntausten, kuten metaversumin ja Web 3.0:n myötä. Yhtäältä ne antavat käyttäjille paremmat mahdollisuudet käyttää päätösvaltaa hajautetun päätöksenteon prosesseissa digitaalisissa ympäristöissä entistä paremmin, mutta toisaalta ne voivat johtaa arkaluontoisen ja käyttäytymiseen liittyvän datan räjähdysmäiseen keruuseen käyttäjistä.

Tämä muistio pyrkii synnyttämään keskustelua siitä, miten yksilöiden oikeus datan siirtämiseen voidaan toteuttaa käytännössä ja kattavasti. Se vastaa seuraaviin tutkimuskysymyksiin: ”Mitkä ovat tärkeimmät oikeudelliset ja tekniset rajoitteet, jotka koskevat oikeutta datan siirtämiseen?” ja ”Miten datan siirrettävyyttä koskevaa oikeudellista kehystä tulisi muuttaa, jotta saavutettaisiin toteutuskelpoinen ja kattava oikeus datan siirtämiseen?”. Selvitys tehtiin käymällä läpi voimassa olevaa ja ehdotettua lainsäädäntöä, Euroopan unionin asiakirjoja ja pohtimalla viimeaikaista akateemista keskustelua aiheesta.

Muistiossa käydään läpi datan siirrettävyyttä säätelevää oikeudellista viitekehystä Euroopassa, jotta voidaan tunnistaa keskeisiä oikeudellisia haasteita, jotka rajoittavat oikeuden hyödyllisyyttä yksilöiden kannalta (luku 2). Siinä tarkastellaan datan siirtämistä koskevan oikeuden tärkeimpiä teknisiä rajoitteita (luku 3) ja analysoidaan näitä rajoitteita metaversumin ja Web

3.0:n yhteydessä (luku 4). Lopuksi muistiossa esitetään neljä hypoteettista tapaa parantaa oikeutta datan siirtämiseen ja ylittää tunnistetut haasteet (luku 5).

Datasäädös ja EHDS sääntelevät myös datan jakamista yritysten välillä sekä yritysten ja viranomaisten välillä. Tämän muistion näkökulma on kuitenkin rajattu yksilöiden oikeuteen siirtää dataa järjestelmästä toiseen. Ehdotettua sähköisen viestinnän tietosuoja-asetusta eli ePrivacy-asetusta ei myöskään käsitellä tässä muistiossa, sillä siinä ei säädetä datan siirtämisen oikeudesta.

2. Oikeus datan siirtämiseen Euroopan unionissa

Euroopan datastrategia (Euroopan komissio 2020a) määrittelee datan siirrettävyyden tärkeäksi välineeksi, jolla yksilöt voivat lisätä vaikutusmahdollisuuksiaan omaan dataansa ja jonka avulla he voivat "päättää itse yksityiskohtaisesti, mitä heidän tiedoillaan tehdään". Strategiassa viitataan myös "henkilötietojen data-avaruuksiin" eli henkilötietojen tietoalueisiin tapana päästä osaksi dataekosysteemiä. Yksilöt voivat hyödyntää datan siirtämistä esimerkiksi vaihtaakseen palvelua ja siirtääkseen tietonsa toiseen palveluun, pyytääkseen toisen lausunnon siirrettyjen tietojen perusteella tai käyttääkseen lisäpalveluita, kuten saadakseen oivalluksia kulutustiedoistaan.

Tässä luvussa tarkastellaan datan siirrettävyyttä koskevaa Euroopan unionin oikeudellista kehystä yksilön näkökulmasta. Tavoitteena on arvioida, miten EU:n eri säädökset käsittelevät oikeutta datan siirtämiseen ja niiden yhteisvaikutusta. Tarkastelun kohteena ovat yleinen tietosuoja-asetus, ehdotus datasäädökseksi ja ehdotus eurooppalaiseksi terveystietoalueeksi (EHDS) sekä digimarkkinasäädös (DMA).

2.1. Yleisen tietosuoja-asetuksen 20 artikla

Yleinen tietosuoja-asetus (GDPR) pähkinänkuoressa

Mistä tietosuoja-asetuksessa on kyse? Yleinen tietosuoja-asetus yhtenäistää Euroopan unionin kansalaisten perusoikeuksien ja vapauksien suojaa heidän henkilötietojensa käsittelyssä. Henkilötietojen suoja taataan Euroopan unionin perusoikeuskirjan 8 artiklan 1 kohdassa ja Euroopan unionin toiminnasta tehdyn sopimuksen (SEUT) 16 artiklan 1 kohdassa. GDPR tuli voimaan vuonna 2016 ja se oli vastaus teknologian maailmanlaajuiseen nopeaan kehitykseen, joka toi henkilötietojen suojeluun uusia haasteita esimerkiksi yritysten nopeasti lisääntyneen tietojenkeruun sekä talouden ja yhteiskunnallisen elämän digitalisoitumisen vuoksi (yleisen tietosuoja-asetuksen johdanto-osan 6 kappale).

Keitä ovat asetuksen tarkoittamat rekisteröidyt? Tietosuoja-asetuksen 4 artiklan 1 kohdan mukaan rekisteröity on luonnollinen henkilö, jonka henkilötietoja rekisterinpitäjä tai henkilötietojen käsittelijä käsittelee. Rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, viranomainen, virasto tai muu elin, joka "määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot" (yleisen tietosuoja-asetuksen 4 artiklan 7 kohta). Henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö (tai muu), joka käsittelee henkilötietoja rekisterinpitäjän puolesta (yleisen tietosuoja-asetuksen 4 artiklan 8 kohta).

Mitkä ovat rekisteröidyn oikeudet? Tietosuoja-asetus säätää kahdeksasta rekisteröidyn oikeudesta, jotka antavat yksilöille enemmän päätäntävaltaa heidän dataansa ja antaa heille käytännön työkaluja henkilötietojen hallintaan. Datan siirrettävyyttä koskevan oikeuden lisäksi näihin oikeuksiin kuuluvat esimerkiksi oikeus saada tietoa henkilötietojen käsittelystä, oikeus saada pääsy henkilötietoihin, oikeus tulla unohdetuksi ja oikeus vastustaa henkilötietojen käsittelyä.

Mitä tietosuoja-asetus sanoo datan siirrettävyydestä? Tietosuoja-asetuksen 20 artikla takaa yksilöille oikeuden saada henkilötietonsa ja oikeuden siirtää nämä tiedot kolmannelle osapuolelle. Artikla velvoittaa yritykset toimittamaan henkilötiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa (yleisen tietosuoja-asetuksen 20 artiklan 1 kohta). Mikäli yritys ei vastaa datan siirtopyyntöön, henkilö voi valittaa jäsenvaltionsa tietosuojaviranomaiselle (yleisen tietosuoja-asetuksen 77 artikla). Tietosuojaviranomainen voi määrätä hallinnollisia sakkoja, jos säännöksiä ei nodateta, tietosuoja-asetuksen 83 artiklan mukaisesti.

Yleistä tietosuoja-asetusta voidaan pitää tärkeimpänä datan siirrettävyyden oikeuden lähteenä EU:ssa. Siihenkin liittyy kuitenkin omat rajoituksensa. Vuonna 2020 tehdyssä tietosuoja-asetuksen arvioinnissa selvisi, että vaikka ihmiset olivat “enenevissä määrin tietoisia oikeuksistaan”, oikeutta siirtää tiedot järjestelmästä toiseen ei käytetty täysimääräisesti (Euroopan komissio 2020b).

Tässä muistiossa käsitellään kolmea haastetta, jotka rajoittavat oikeuden tehokasta käyttöä: 20 artiklan rajallista soveltamisalaa, 20 artiklan rajallista oikeusperustaa ja tämän oikeuden tasapainottamista muiden yksilöiden oikeuksien ja vapauksien kanssa.

Yleisen tietosuoja-asetuksen 20 artiklan rajallinen soveltamisala

Yleistä tietosuoja-asetusta sovelletaan henkilötietoihin, jotka on määritelty asetuksen 4 artiklan 1 kohdassa sellaisiksi tiedoiksi, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön, joka voidaan suoraan tai epäsuorasti tunnistaa tunnistetietojen, kuten nimen, sijaintitietojen tai muiden tekijöiden, kuten fyysisten tai psykologisten tekijöiden, perusteella. 29 artiklan mukaisen tietosuojatyöryhmän (WP29) ohjeistus selventää, että henkilötietojen käsitettä tulee tulkita väljästi (29 artiklan mukainen työryhmä 2007).

WP29 luettelee neljä tekijää, joiden perusteella voidaan määrittää, onko jokin tieto henkilötieto vai ei. Näitä ovat:

1. ”mikä tahansa tieto”, jolla tarkoitetaan mitä tahansa yksilöä koskevaa tietoa,
2. ”jotain koskeva”, joka viittaa siihen, että tieto koskee tiettyä henkilöä,
3. ”tunnistettu tai tunnistettavissa oleva”, joka viittaa yksittäiseen henkilöön, joka voidaan tunnistaa suoraan tai epäsuorasti tunnisteiden avulla
4. ”luonnollinen henkilö”, joka viittaa elävään yksilöön.

Yleisen tietosuoja-asetuksen 20 artikla rajaa datan siirrettävyyden oikeuden koskemaan vain rekisteröidyn ”antamia” tietoja. Onkin kiistelty siitä, mitkä tiedot sisältyvät tähän “annetun” datan määritelmään. Sillä tarkoitetaan henkilötietoja, jotka henkilö antaa ”tietoisesti ja aktiivisesti”, ja henkilötietoja, jotka hän tuottaa itse. WP29:n mukaan tämä viittaa myös ”seurantadataan”, jota yritys saa kun rekisteröity käyttää sen palvelua tai laitetta. Tällaista dataa voivat olla esimerkiksi hakuhistoria, verkkoliikennetiedot, paikkatiedot tai puettavan älylaitteen data, kuten vaikkapa laitteen tallentamat syketiedot (29 artiklan mukainen työryhmä 2007).

”Annetun” datan määritelmää voi suhteuttaa ”pääteltyyn” tai ”johdettuun” dataan, jossa on kyse rekisterinpitäjän luomista käyttäjäprofiileista sellaisten tietojen pohjalta, joita henkilöt antavat yritykselle omasta tahdostaan tai jonkin tuotteen tai palvelun käytön kautta (29 artiklan mukainen työryhmä 2017). Näin ollen yksilöillä ei ole oikeutta siirtää käyttäjäprofiilejaan tai sellaisia käyttäytymisanalyyseja, jotka yritys on tehnyt omien algoritmiensa avulla. He voivat kuitenkin pyytää tietoja profiloinnin logiikasta ja henkilötietojen vastaanottajista yleisen tietosuoja-asetuksen 15 artiklan nojalla. Graef et al. (2019) toteavat, että soveltamisalan rajoittaminen ”epäilemättä aiheuttaa rekisteröidyille vaikeuksia” hyödyntää datan siirrettävyyttä, koska on epäselvää, mitä muita tietoja kuin raakadataa oikeus koskee.

Yleisen tietosuoja-asetuksen 20 artiklan rajallinen oikeusperuste

Yksilöiden mahdollisuutta käyttää oikeutta siirtää tiedot järjestelmästä toiseen rajoittaa entisestään se, että yleisen tietosuoja-asetuksen 20 artikla koskee vain sellaisia tilanteita, joissa rekisteröity on antanut rekisterinpitäjälle suostumuksensa datan käsittelyyn tai käsittely perustuu käyttäjän kanssa tehtyyn sopimukseen (yleisen tietosuoja-asetuksen 2 artiklan kohdat 1 ja 2). Näin ollen yksilöt eivät siis voi käyttää oikeutta siirtää tiedot järjestelmästä toiseen henkilötietoja käsitteleviä viranomaisia vastaan. Tämän on esitetty johtuvan siitä, että oikeutta siirtää tiedot järjestelmästä toiseen on pidetty ”taloudellisena oikeutena” eikä yleistä tietosuoja-asetusta annettaessa otettu huomioon sellaista mahdollisuutta, että yksilöt voisivat hyötyä taloudellisesti tietojen siirtämisestä viranomaisilta (De Hert ym. 2018).

Suhde muihin oikeuksiin ja vapauksiin

Koska yksilöiden oikeus siirtää tiedot järjestelmästä toiseen ei ole absoluuttinen oikeus, vastatessaan tietojen siirtopyyntöön yrityksen on arvioitava, voiko pyyntöön vastaaminen loukata muiden oikeuksia tai vapauksia (yleisen tietosuoja-asetuksen 20 artiklan kohta 4). Oletetaan esimerkiksi, että käyttäjä pyytää Facebookilta henkilötietojensa siirtämistä. Tällöin luovutettava tietokokonaisuus ei voi sisältää muiden käyttäjien julkaisuja, vaikka siirtoa pyytänyt käyttäjä olisikin kommentoinut niitä, mikäli tietojen siirtäminen loukkaisi tietojen salassa pidettävyyttä tai tietoihin liittyviä immateriaalioikeuksia.

Liiketoiminnallisesta näkökulmasta tämä rajaus on kuitenkin tervetullut, sillä se rajoittaa ristiriitoja tietojen haltijan immateriaalioikeuksien kanssa, kuten tekijänoikeuksien, liikesalaisuuksien ja sui generis -tietokantaoikeuksien kanssa. Graef et al. (2019) toteavat tämän estävän yrityksen kilpailijoita hyötymästä valmiista käyttäjäprofiileista tai tekemästä käänteistä algoritmia johdettujen tietojen pohjalta, mikäli käyttäjä haluaa siirtää henkilötietoja toiselle palveluntarjoajalle. Vaikka 29 artiklan mukainen tietosuojatyöryhmä muistuttaakin, ettei liiketoiminnallinen riski oikeuta datan siirtopyynnön hylkäämiseen, yrityksen on löydettävä keino tietojen jakamiseen niin, ettei se paljasta liikesalaisuuksia tai luottamuksellisia tietoja (29 artiklan mukainen työryhmä 2017).

Tämä tiivis analyysi osoittaa, että yleisen tietosuoja-asetuksen 20 artiklan mukainen oikeus siirtää tiedot järjestelmästä toiseen on soveltamisalaltaan rajallinen. Solove (2023) huomauttaa, että ”monilla sivustoilla, joilla käyttäjät eniten toivoisivat datan siirtämistä, on merkittäviä rajoituksia sille, kuinka paljon tietoja voidaan siirtää ja kuinka hyödyllistä tietojen siirtäminen tulee olemaan”. Tässä mielessä datan siirrettävyyttä koskeva sääntely kuvastaa niitä haasteita, joita sääntelyviranomaiset kohtaavat uusien, nopeasti kehittyvien teknologioiden yhteydessä. Paljon tulee riippumaan siitä, kuinka hyvin sääntelyviranomaiset ymmärtävät kyseisiä teknologioita ja datan siirrettävyyden mahdollisuuksia.

2.2. Datasäädöksen 4 ja 5 artiklat

Datasäädös pähkinänkuoressa

Mistä datasäädöksessä on kyse? Euroopan komissio julkaisi ehdotuksensa datasäädökseksi vuonna 2022. Säädös on Euroopan datastrategian kulmakiviä ja sen on tarkoitus helpottaa datan jakamista ja datavetoista innovointia Euroopassa. Euroopan parlamentti on hyväksynyt datasäädöksen äänestyksessään marraskuussa 2023 ja se tulee voimaan vuonna 2025. (Euroopan parlamentti 2023a).

Mitä on verkkoon kytkettyjen laitteiden data? Datasäädös luo "yhdenmukaiset säännöt, jotka koskevat tuotteen tai siihen liittyvän palvelun käytön tuloksena tuotetun datan asettamista mainitun tuotteen tai palvelun käyttäjän saataville" (datasäädöksen 1 artiklan 1 kohta). Kytketyt laitteet, joihin viitataan myös nimityksellä esineiden internet (Internet of Things, IoT), tarkoittaa kaikkia sellaisia fyysisiä tuotteita, jotka vastaanottavat, tuottavat tai keräävät dataa ja jotka pystyvät välittämään ja vaihtamaan kyseistä dataa (datasäädöksen johdanto-osan 14 kappale). Säädös sääntelee pääsyä dataan ja datan käyttöä yritysten ja kuluttajien välisissä, yritysten keskinäisissä sekä yritysten ja viranomaisten välisissä suhteissa, mutta mikro- ja pienyritykset eivät kuulu sen soveltamisalaan (datasäädöksen 7 artiklan 1 kohta).

Mitä datasäädöksessä sanotaan datan siirrettävyydestä? Datasäädöksen 4 artiklassa säädetään edellytyksistä, joiden täyttyessä yksittäinen henkilö voi pyytää pääsyä verkkoon kytkettyjen laitteiden ja niihin liittyvien palvelujen tuottamaan dataan ja sen käyttöön. Säädöksen 5 artikla takaa käyttäjille oikeuden jakaa dataa kolmansille osapuolille joko itse tai käyttäen datanhallinta-asetuksessa määriteltyjä datanvälityspalveluja. Esimerkiksi älytermostaattia käyttävä henkilö voi pyytää sähköntoimittajaa jakamaan hänen sähkönkulutusprofiilinsa vertailupalvelulle (Thombal ja Graef 2023).

Valmistajien tulee toimittaa data "ilman aiheetonta viivytystä ... helposti, suojatusti, ymmärrettävässä, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, maksutta ja, tapauksen mukaan ja jos se on teknisesti toteutettavissa, jatkuvasti ja reaaliaikaisesti, myös asettamalla tällaisesta datasta johdetut henkilötiedot rekisteröidyn saataville yleisen tietosuoja-asetuksen (EU) 2016/679 15 artiklan nojalla, yhdessä asianomaisen metadatan kanssa (joka on tarpeen datan tulkitsemiseksi ja käyttämiseksi)" (datasäädöksen 4 artiklan 1 kohta).

Ehdotettu datasäädös on vastaus markkinahäiriöön, joka johtuu siitä, että esineiden internetin IoT-dataa tuottavat tahot eivät saa tietoja käyttöönsä (Euroopan komissio 2022a). Esimerkiksi autonvalmistajat hallitsevat ajoneuvojen dataa ja he ovat etulyöntiasemassa palveluiden ja korjausten tarjoamisessa, koska dataa käsitellään valmistajien kehittämien järjestelmien kautta (Gill ja Metzger 2020).

Ehdotus asettaakin verkkoon kytkettyjen laitteiden valmistajille ja niihin liittyvien palveluiden tarjoajille velvoitteita saattaa data saataville ja siirtää sitä kolmannelle osapuolelle mikäli käyttäjä näin pyytää (datasäädöksen 4 ja 5 artiklat). Datasäädös myös tekee mahdolliseksi jälkimarkkinapalveluiden, korjausten ja muiden lisäpalveluiden kehittämisen, kun dataa jaetaan kolmansille osapuolille. Se myös ehkäisee sellaisia lukkiumatilanteita, joissa käyttäjät karttavat toiselle alustalle siirtymistä, koska se tarkoittaisi kaikkien olemassa olevien yhteyksien, sisältöjen ja datan menettämistä ja näin aiheutuvaa vaivaa (Euroopan komissio 2022b).

Oikeus datan siirtämiseen datasäädöksessä yleiseen tietosuoja-asetukseen verrattuna

Datasäädös laajentaa datan siirrettävyyden soveltamisalaa ja ulottaa sen koskemaan verkkoon kytkettyjen laitteiden käytössä syntynyttä dataa. Verkkoon kytkettyjen laitteiden ollessa kyseessä käyttäjät voivat siirtää henkilötietoja ja muuta dataa niiden käsittelyn oikeusperusteesta riippumatta. Toisin kuin yleisen tietosuoja-asetuksen 20 artikla, datasäädös koskee ”kaikkea dataa”, jota käyttäjä tuottaa käyttäessään tuotteita tai niihin liittyviä palveluja (datasäädöksen 2 artiklan 1 kohta). Säädöksen piiriin kuuluvatkin siis niin henkilötiedot kuin muukin data, kunhan henkilötietojen käsittelylle on olemassa pätevä oikeusperusta. Tämä laaja datan määritelmä kattaa myös datan kaikenlaisesta digitaalisesta varallisuudesta, kuten sovelluksista, virtuaalisista laitteista ja ”virtualisointiteknologioiden ilmentymistä”, metatiedot mukaan lukien (Fernandez 2022).

Siinä missä yleisen tietosuoja-asetuksen 20 artikla on rajattu koskemaan ”yksilön antamaa” dataa, datasäädöksen sovellusalaan sisältyvät puolestaan ”data, joka tuotetaan käyttäjän toiminnan sivutuotteena, kuten diagnostinen data, ja ilman mitään käyttäjän toimintaa, kuten data verkkoon liitetyn tuotteen ympäristöstä tai vuorovaikutuksesta, myös tuotteen ollessa ’valmiustilassa’, ja data, joka tallennetaan tuotteen ollessa sammutettuna” (datasäädöksen johdanto-osan 17 kappale). Euroopan parlamentin hyväksymän kompromissitekstin mukaan 4 artiklan 1 kohta ei kuitenkaan sisällä monimutkaisten algoritmien avulla johdettua tai pääteltyä dataa (Euroopan parlamentti 2023b).

Datan siirtämistä koskevan oikeuden toteutus datasäädöksen ja yleisen tietosuoja-asetuksen avulla

Datasäädöksen 31 artiklan 1 kohta edellyttää EU-jäsenvaltioita nimeämään viranomaisen, joka vastaa säädöksen soveltamisesta ja täytäntöönpanosta. Kukin jäsenvaltio voi itse päättää viranomaisen kokoonpanosta sekä siitä, perustetaanko kokonaan uusi viranomainen tai onko viranomaisia useita. Yksityishenkilö voi valittaa viranomaiselle datasäädöksen rikkomisesta (31 artiklan 3 kohdan b alakohta). Jos asia koskee henkilötietojen käsittelyä, toimivaltainen viranomainen on yleisen tietosuoja-asetuksen mukaisesti kunkin jäsenvaltion asianomainen tietosuojaviranomainen (datasäädöksen 31 asetuksen 2 kohdan a alakohta).

Krämer ym. (2023) kuvaavat datasääntelyä (kuten datasäädöstä ja datanhallinta-asetusta) valvovien uusien viranomaisten perustamista ”hajautetun toimeenpanon malliksi”, johon liittyy sekaannuksen riski. Ei ole selvää, miten eri viranomaiset varmistavat sujuvan yhteistyön välillään niin, että yksilöiden tekemät valitukset pystytään kuulemaan ja käsittelemään nopeasti. Tämä riski korostuu tilanteissa, joissa on epäselvää, koskeeko asia datasäädöksen ja/vai tietosuojaviranomaisen toimialaa.

Datasäädöksen ja yleisen tietosuoja-asetuksen välinen hierarkia

Tombalin ja Graefin (2023) mukaan yksilö voi vedota sekä yleisen tietosuoja-asetuksen 20 artiklaan että datasäädökseen siirtäessään henkilötietoja, jotka on luotu verkkoon kytkettyjen laitteiden käytön avulla. He arvioivat, että ”komissio katsoo, että yleinen tietosuoja-asetus sisältää de minimis -datansiirto-oikeuden, jolla on laaja soveltamisala ja jonka lisäksi voi olla tarkemmin määriteltyjä ja suppeampia mutta mahdollisesti ’vahvempia’ datansiirto-oikeuksia (kuten oikeus päästä esineiden internetin IoT-dataan)”.

Euroopan kuluttajaliitto on kuitenkin huomauttanut, että ehdotetussa datasäädöksessä ei selvästi mainita, mikä lainsäädäntö on ensisijainen ristiriitatapauksissa – toisin kuin esimerkiksi datanhallinta-asetuksen 1 artiklan 3 kohdassa (BEUC 2023). Datasäädöksen 1 artiklan 3 kohdassa kuitenkin todetaan säädöksen täydentävän yleisen tietosuoja-asetuksen 20 artiklaa, kun ”käyttäjät ovat henkilötietojen osalta rekisteröityjä”. Ducuingin (2022) mukaan tämä tarkoittaa, että mikäli yleisen tietosuoja-asetuksen 20 artikla on henkilötietojen siirtämisen kannalta keskeinen säädös, silloin sen sisältö on ristiriidassa ehdotetun datasäädöksen kanssa, koska yleisen tietosuoja-asetuksen mukainen tietojen siirto-oikeus on rajallinen. Hänen johtopäätöksensä on, että datasäädöksen astuttua voimaan yksilöillä on mahdollisuus saada käyttöönsä enemmän dataa (rekisteröidyn ”toimittaman” datan lisäksi) kuin yleisen tietosuoja-asetuksen 20 artiklan nojalla. Yksilöt eivät kuitenkaan edelleenkään voi siirtää käyttäjäprofiilejaan, ja niinpä datasäädöksen 4 ja 5 artiklojen sekä yleisen tietosuoja-asetuksen 20 artiklan suhde jää yhä epäselväksi.

2.3. Eurooppalaisen terveystietoalueen 3 artikla

Euroopan komissio julkaisi vuonna 2022 esityksen eurooppalaisesta terveystietoalueesta (European Health Data Space, EHDS) helpottamaan sähköisten terveystietojen ensisijaista ja toissijaista käyttöä EU:ssa. Ehdotetulla asetuksella vahvistetaan yksilöiden oikeutta datan siirtämiseen terveysalalla auttamalla heitä hallitsemaan sähköisiä terveystietojaan.

Eurooppalaista terveystietoaluetta koskevan asetusehdotuksen johdanto-osan 11 kappaleessa huomioidaan yleisen tietosuoja-asetuksen 20 artiklan olevan puutteellinen terveydenhoitoalan näkökulmasta kahdesta syystä. Ensinnäkin, yksilöillä ei ole oikeutta siirtää diagnoosejaan ja testituloksiaan, koska niitä pidetään pääteltyinä ja johdettuina tietoina, jotka eivät kuulu yleisen tietosuoja-asetuksen 20 artiklan soveltamissalaan. Toisekseen, julkisten viranomaisten (mukaan lukien julkinen terveydenhuolto) keräämät, käsittelemät ja tallentamat henkilötiedot eivät kuulu yleisen tietosuoja-asetuksen 20 artiklan soveltamisalaan.

Eurooppalaisen terveystietoalue-ehdotuksen 3 artiklan 1 kohta antaa yksilöille oikeuden saada omat sähköiset terveystietonsa välittömästi, maksutta ja helposti luettavassa, yhdisteltävässä ja käytettävässä muodossa. Säädöksen 3 artiklan 8 kohta puolestaan antaa yksilöille mahdollisuuden siirtää sähköiset terveystietonsa toiselle palveluntarjoajalle. Samoin kuin tietojen saannin oikeuden kohdalla, myös tietojen siirron tulisi tapahtua välittömästi, maksutta ja esteettä. Säädöksen 3 artiklan 3 kohdan mukaan EU-jäsenvaltiot voivat kuitenkin rajoittaa oikeuden soveltamisalaa yleisen tietosuoja-asetuksen 23 artiklan mukaisesti, jos sen on potilasturvallisuuden ja etiikan kannalta tarpeellista.

Eurooppalainen terveystietoalue kattaa henkilökohtaiset ja muut terveystiedot riippumatta siitä, mikä on henkilötietojen käsittelyn oikeusperusta. Henkilökohtaisiksi sähköisiksi terveystiedoiksi katsotaan yleisessä tietosuoja-asetuksessa määritellyt terveys- ja perimätiedot sekä "terveyden taustatekijöihin liittyvät tiedot tai terveydenhuoltopalvelujen antamisen yhteydessä käsitellyt tiedot, joita käsitellään sähköisessä muodossa" (eurooppalaisen terveystietoalueen 2 artiklan 2 kohdan a alakohta). Eurooppalaisen terveystietoalueen johdanto-osan 5 kappaleessa täsmennetään myös, että soveltamisalaan kuuluvat "päätellyt ja johdetut tiedot, kuten diagnostiikka, tutkimukset ja lääketieteelliset tarkastukset, samoin kuin automaattisilla keinoilla saadut ja kirjatut tiedot".

Pop ja Grant (2023) pitävät yleisen tietosuoja-asetuksen 20 artiklan soveltamisalan laajentamista ehdotetulla EHDS-säädöksellä tervetulleena muutoksena. He kuitenkin epäilevät, edistääkö EHDS arkaluontoisten tietojen laajempaa liikkumista, jos yksilöt voivat siirtää pääteltyjä diagnooseja yhdeltä terveydenhuollon alustalta toiselle alustalle, joka voi edelleen jakaa tietoja kolmansille osapuolille laillisen käsittelyn rajoissa. Tämä voi olla ristiriidassa yleisen tietosuoja-asetuksen tietojen minimoinnin periaatteen kanssa (EDPB-EDPS 2023).

2.4. Digimarkkinasäädös

Euroopan unioni pyrkii hillitsemään suurimpien teknologiatoimittajien merkittävää valtaa vuonna 2022 annetulla digimarkkinasäädöksellä. Säädöksessä käytetään termiä ”portinvartija” viittamaan niin kutsuttuihin ydinalustapalveluihin, kuten verkon hakukoneisiin, sosiaalisen median palveluihin, videonjakopalveluihin ja verkkoselaimiin (digimarkkinasäädöksen 2 artikla).

Digimarkkinasäädöksen nojalla Euroopan komissio voi nimetä ne palvelujentarjoajat, jotka kuuluvat portinvartijoiden piiriin ja joiden on noudatettava säädöksessä määritettyjä velvoitteita (digimarkkinasäädöksen 3 ja 4 artiklat). Näihin velvoitteisiin kuuluvat kielto yhdistellä ydinpalvelun henkilötietoja kolmannen osapuolen palveluihin ja kielto käyttää henkilötietoja ristiin ydinpalveluiden ja muiden palveluiden välillä (digimarkkinasäädöksen 5 artikla). Yksilöt voivat kuitenkin antaa suostumuksensa tietojen yhdistelyyn ja ristiin käytölle (digimarkkinasäädöksen 3 artiklan 1 ja 3 kohdat).

Lisäksi digimarkkinasäädöksen 6 artiklan 9 kohdan portinvartijoiden on helpotettava veloituksetta ”loppukäyttäjän toimittamien tai loppukäyttäjän toiminnassa alustan käytön yhteydessä syntyneiden tietojen” tehokasta siirrettävyyttä. Tämä data tulee olla ”välittömästi ja tosiasiallisesti saatavilla ja käytettävissä loppukäyttäjällä tai loppukäyttäjän valtuuttamalla asiaankuuluvalla kolmannella osapuolella, jolle tiedot siirretään” (digimarkkinasäädöksen johdanto-osan 59 kappale). Portinvartijan tulee siten tarjota tiedonsiirtoon maksutta työkaluja, jotka mahdollistavat jatkuvan ja reaaliaikaisen pääsyn tietoihin. Näihin työkaluihin sisältyvät myös ohjelmointirajapinnat (digimarkkinasäädöksen johdanto-osan 59 kappale). EU katsoo näiden velvoitteiden varmistavan, että portinvartijat eivät rajoita palveluiden vaihtamista tai useamman palvelun käyttämistä. Jos portinvartijat eivät noudata velvoitteita, niille voidaan määrätä sakko, joka voi olla suuruudeltaan enintään 10 prosenttia portinvartijan maailmanlaajuisesta liikevaihdosta (digimarkkinasäädöksen 30 artikla).

2.5. Oikeuksien vertailu

Taulukossa 1 on esitetty yleiskuvaus tässä muistiossa käsitellyistä neljästä instrumentista: yleisen tietosuoja-asetuksen 20 artikla, datasäädösehdotus, ehdotus eurooppalaisesta terveystietoalueesta ja digimarkkinasäädös.

Taulukko 1. Tietojen siirtämisen oikeuden vertailu

	Yleisen tietosuoja-asetuksen artikla 20	**Datasäädös-ehdotus**	**Ehdotus eurooppalaisesta terveystieto-alueesta (EHDS)**	**Digimarkkina-säädös**
Datan tyyppi	Rekisteröidyn antamat henkilötiedot	Henkilötietoja sisältävä ja muu IoT-data, joka on johdettu ja päätelty IoT-data	Henkilötietoja sisältävät terveystiedot sekä muu johdettu, päätelty ja havaittu terveystieto	Käyttäjän antamat tai käytön yhteydessä luodut tiedot
Oikeusperuste	Sopimus ja suostumus	-	-	-
Tekniset vaatimukset	Jäsennelty, yleisesti käytetty ja koneellisesti luettava muoto	Jäsennelty, yleisesti käytetty ja koneellisesti luettava muoto	Sähköinen kopio eurooppalaisessa sähköisen terveyskertomuksen vaihtomuodossa	Jatkuva, reaaliaikainen pääsy käyttäjälle tai hänen valtuutetulle kolmannelle osapuolelle
Pyynnön kohde	Mikä tahansa rekisterinpitäjä tämän alasta riippumatta	Verkkoon kytkettyjen laitteiden valmistajat ja niihin liittyvien palveluiden tarjoajat	Terveydenhuolto- tai hoitoalan yksikkö tai elin tai näillä aloilla tutkimusta tekevä taho (yksityinen tai julkinen toimija)	Portinvartijat

3. Datan siirtämisen oikeuden rajoitukset

Datan siirrettävyyttä koskevaa oikeudellista kehystä ollaan laajentamassa ehdotetun datasäädöksen ja eurooppalaisen terveystietoalueen myötä. Kun ehdotukset on aikanaan hyväksytty, luovat ne kuitenkin sirpaleisen datan siirtämisen oikeuden. Samalla olisi kyettävä ylittämään tekniset ja muut rajoitukset, jotka ovat estäneet yleisen tietosuoja-asetuksen 20 artiklan tehokkaan käytön.

Tässä muistiossa käsitellään neljää rajoitusta: yritysten riittämätöntä oikeuden toimeenpanoa, yksityisyydensuojaan ja tietoturvaan liittyviä riskejä, yhteentoimivuuden puutteita sekä välittäjäpalveluiden roolien epäselvyyttä.

1. Yritysten riittämätön toimeenpano

Tietojen siirrettävyyttä koskevan oikeuden toteutuminen on asetettu kyseenalaiseksi, koska datan siirtämiseen tarkoitettuja välineitä ei ole otettu käyttöön. Esimerkiksi Wong ja Henderson (2019) ovat tutkineet 230 rekisterinpitäjän vastauksia datansiirtopyyntöihin. He keskittyivät erityisesti oikeuteen saada tietoa eivätkä niinkään oikeuteen siirtää sitä. Heidän tutkimustuloksensa osoitti, että pyyntöihin vastaaminen oli hankalaa ja vain noin 75 prosenttia 230 rekisterinpitäjästä toteutti pyynnön. Data myös toimitettiin tutkijoille sellaisissa muodoissa, jotka eivät täyttäneet 20 artiklassa asetettuja teknisiä vaatimuksia, kuten PNG-muotoisina kuvakaappauksina ja PDF-skannauksina, jotka eivät ole vaaditulla tavalla koneluettavia.

Vuonna 2022 julkaistussa toisessa tutkimuksessa puolestaan selvisi, että 160 IoT-laitteen tietosuojaselosteista vain pienessä osassa selitettiin oikeus datan siirtämiseen. Kun tutkijat testasivat joitakin suosittuja laitteita, yksikään niistä ei mahdollistanut tietojen siirtämistä toiseen laitteeseen (Turner et al. 2021). Tutkimus keskittyi Isossa-Britanniassa saataviin IoT-laitteisiin, kuten Garmin Vivosmart 4- ja Fitbit Change 3 -aktivisuusrannekkeisiin sekä Amazon Echo- ja Google Home -älykotilaitteet.

Wong ja Henderson (2019) arvioivat, että yhtäältä se, että datan siirtämisen käytäntöjen ja prosessien toteutuksissa yrityksissä on puutteita, ja toisaalta se, että vain muutamassa oikeustapauksessa on käsitelty datan siirtämiseen liittyviä näkökohtia, ovat merkkejä siitä, että kuluttajien kiinnostus aiheeseen on vähäisestä. Nähtäväksi jää, pystyvätkö datasäädös ja EHDS lisäämään kiinnostusta ja täyttämään ne korkeat odotukset, jotka kohdistuvat datan siirrettävyyteen keinona edistää reilua kilpailua. Kilpailutilanteelle ja lisäpalveluiden markkinoille ei kuitenkaan koidu hyötyä, jos yksilöt eivät käytä tätä oikeuttaan.

2. Yksityisyyteen ja tietoturvaan liittyvät riskit

Vaikka datan siirrettävyys voi olla väline, joka lisää käyttäjien vaikutusmahdollisuuksia ja parantaa heidän mahdollisuuksiaan puolustaa oikeuttaan yksityisyyteen ja tietosuojaansa, se voi myös aiheuttaa horisontaalista epätasapainoa yksityisyyden suojaan nähden. Kun dataa siirretään alustalta toiselle, se irrotetaan asiayhteydestään. Mikäli siirretty data sisältää henkilötietoja, ei ole selvää, sovelletaanko oikeudellisia, teknisiä ja sosiaalisia rajoitteita uuteen alustaan. Datan siirtäminen ei ole oikeutettu peruste henkilötietojen käsittelylle, eikä datan siirtäminen myöskään estä tietojen väärinkäyttöä. (Hondagneu-Messner 2021.)

Yksityisyys on vaarassa myös silloin, jos rekisterinpitäjä tai kolmas osapuoli ei toteuta riittäviä toimenpiteitä tietojen suojaamiseksi siirron aikana (tai datan ollessa tallennettuna). Tätäkin suurempi vaara yksityisyydelle aiheutuu, mikäli yritys myöntää väärälle henkilölle pääsyn dataan (Swire 2020). Voidaankin kysyä, miten henkilöt tunnistetaan datan siirtopyyntöjen yhteydessä. Esimerkiksi yleisessä tietosuoja-asetuksessa ei määritellä vaatimuksia käyttäjien todentamiselle, mutta sen johdanto-osan kappaleessa 57 kuitenkin todetaan, että ”tunnistamiseen olisi sisällytettävä rekisteröidyn digitaalinen tunnistaminen esimerkiksi todentamismekanismin avulla, kuten käyttämällä samoja tunnisteita, joita rekisteröity käyttää kirjautuessaan rekisterinpitäjän tarjoamiin verkkopalveluihin”.

3. Puutteellinen yhteentoimivuus

Yksi syy yleisen tietosuoja-asetuksen artiklan 20 vähäiselle käytölle on yksilöiden saama vähäinen arvo datan siirtämisestä. Arvo kuitenkin kasvaa, jos henkilö pystyy siirtämään tietonsa toiseen palveluun. Palveluiden vaihtaminen vähentää lukkiutumisvaikutuksia ja hyödyttää näin myös kilpailevia yrityksiä. Yrityksillä ei kuitenkaan ole ollut juurikaan kannustimia sallia asiakastietojen saumaton siirto, koska palvelun kannalta on enemmän hyötyä siitä, että käyttäjät pidetään omalla alustalla ja vaikeutetaan palvelujen vaihtamista, mikä lisää käyttäjien pysyvyyttä palvelun parissa (OECD 2021).

Tämän lisäksi yhteentoimivuuden (syntaktiset ja semanttiset) vaatimukset aiheuttavat yrityksille lisää kustannuksia erityisesti siksi, että niiden on varmistettava datan oikea muoto ja tietoturvallinen siirto. Tämän vuoksi on tärkeää helpottaa yhteentoimivuutta ja luoda sille kannustimia, koska ilman sitä datan siirrettävyys ei ole yhtä hyödyllistä. Toistaiseksi yleinen tietosuoja-asetus on kannustanut yrityksiä vaihtamaan tiedostoja yhteensopivissa muodoissa, eikä vaikuta olevan vaatimusta kehittää tiedostomuotoa, joka mahdollistaisi siirron toiselle palveluntarjoajalle, sillä yleisen tietosuoja-asetuksen johdanto-osan kappaleessa 68 todetaan, että siirtämistä edellytetään vain, mikäli se on ”teknisesti toteutettavissa”. (De Hert et al. 2018.).

4. Datanvälityspalveluiden epäselvä rooli

Datanvälityspalvelut voivat paikata yhteentoimivuuden puutteita tarjoamalla yksilöille mahdollisuuden siirtää tietoja toiselle palveluntarjoajalle tarjoamalla pääsyn tietoihin ja niiden siirron välityspalvelun kautta, kuten yksityisten henkilötietojen hallintajärjestelmien (Personal Information Management Systems, PIMS) kautta. Henkilötietojen hallintajärjestelmät voivat auttaa tietojen jatkuvassa siirrossa ja tiedon muuntamisessa eri muotoihin toimien näin ”käyttäjän ainoana yhteyspisteenä tietojenkeruuluvan hallinnassa” (OECD 2021).

Henkilötietojen hallintajärjestelmä voi myös tarjota rahallisen korvauksen dataan pääsyyn järjestämisestä, kun se yhdistelee dataa ja myy pääsyoikeuksia siihen yksilöiden puolesta. Yksi esimerkki tällaisesta palvelusta on mobiilisovellus DIMO, joka myy ajoneuvoihin tallennettua dataa. Toinen esimerkki on italialaisyritys Hoda, joka tarjoaa yksityishenkilöille Weople-sovellusta. Käyttäjä voi sovelluksen avulla yhdistää eri tilejä, kuten Googlen Gmail-tilin ja muita vastaavia, ja siirtää niihin tallennetun datan ”digitaaliseen holviin”. Tämän jälkeen käyttäjä voi ansaita virtuaalivaluuttoja antamalla muille tahoille pääsyoikeuden holviinsa.

Monet PIMS-sovellukset, kuten DIMO ja Weople, ovat yhä varhaisessa vaiheessa toiminta- ja liiketoimintamallinsa kehityksessä. Myös sääntelykehystä kehitetään. Äskettäin hyväksytyn datanhallinta-asetuksen tavoitteena on lisätä luottamusta datanvälitykseen asettamalla rajoituksia välittäjien liiketoimintamalleille ja vaatimalla niitä erottamaan datan jakaminen ydinliiketoiminnastaan, jotta ne pysyisivät neutraaleina ja roolinsa mukaisesti vain saattaisivat datanhaltijan ja dataa tarvitsevan tahon yhteen (datanhallinta-asetuksen 11 artikla). Yhtäältä datanhallinta-asetus on ensimmäinen yritys selkeyttää datanvälityksen oikeudellista asemaa, mutta samalla voidaan kysyä, asettaako se tarpeettomia rajoituksia palveluntarjoajien liiketoiminnan harjoittamisen vapaudelle, joka taataan Euroopan unionin perusoikeuskirjan 16 artiklassa, ja sääteleekö se vielä kypsymätöntä markkinaa (Ducuing 2022).

Selvää ei ole sekään, missä määrin datanvälityspalvelut auttavat yksilöitä saavuttamaan dataa koskevaa autonomiaa ja itsemääräämisoikeuden toteutumista reilussa datataloudessa. Useimmat henkilötietojen hallintajärjestelmät (kuten DIMO) ilmoittavat ”antavansa vallan takaisin” käyttäjille päättää heidän datastaan. Välityspalvelut tukeutuvatkin suostumukseen henkilötietojen käsittelyn oikeusperusteena. Suostumuksen voidaan kuitenkin katsoa de facto heikentävän ”yksityishenkilöiden suojaa, koska rekisteröidyllä ei välttämättä aina ole parhaat mahdolliset resurssit tai osaaminen datan käsittelystä päättämiseen” (Lindroos-Hovinheimo 2022). Tämä korostuu erityisesti ympäristössä, joka hyödyntää ihmisten kognitiivisia vinoutumia ja ohjaa heitä käyttäytymään halutulla tavalla (Mäihänniemi 2022b).

Joissain tapauksissa yksilöitä voidaan myös esimerkiksi pyytää siirtämään henkilötietojaan ilman, että he ymmärtävät seurauksia tai pystyvät

arvioimaan, onko kyseinen yritys tehnyt riittävästi henkilötietojen suojaamiseksi tai tuleeko yritys jakamaan tietoja muille osapuolille. Jos henkilö peruu suostumuksensa ja pyytää tietojensa poistamista, poistavatko ne sekä välittäjä että kolmas osapuoli, jolle data on jaettu?

Suostumuksen käyttöä onkin arvosteltu siitä, että se vastuuttaa heikompaa osapuolta eli käyttäjää sen sijaan, että säädeltäisiin vahvemman osapuolen eli rekisterinpitäjien vastuuta (Mäihänniemi 2022b). Cravo toteaakin varsin vakuuttavasti, että ”jos yksilöt eivät ymmärrä, mihin he antavat suostumuksensa, saattaa datan siirtämisestä saatavan taloudellisen hyödyn hintana olla yksityisyyden menetys” (Cravo 2022).

4. Käyttötapaus: Oikeus datan siirtämiseen metaversumissa

Edellä on tarkasteltu datan siirtämisen oikeuden oikeudellista viitekehystä EU:ssa ja oikeuden täysimääräistä toimeenpanoa rajoittavia tekijöitä. Tässä osiossa tarkastellaan datan siirrettävyyden ja tulevaisuuden teknologioiden välistä suhdetta. Tarkastelun kohteena ovat erityisesti metaversumi ja web 3.0.

Mikä on metaversumi?

Sitra (2023) määrittelee metaversumi(e)n olevan pysyvistä virtuaalitiloista muodostuva kokonaisuus, jossa hyödynnetään hajautettua päätöksentekoa, joka voi toteutua esimerkiksi hajautettujen itsenäisten organisaatioden (decentralised autonomous organisation, DAO) kautta tai käymällä kauppaa kryptovaluutoilla tai digitaalisilla hallintatodistuksilla (non-fungible token, NFT). Yksi esimerkki hajautetusta virtuaalitilasta on Decentraland, jossa käyttäjät ostavat virtuaalista maata käyttäen Ethereum-lohkoketjuun pohjautuvia digitaalisia hallintatodistuksia. Hajautettuun päätöksentekoon perustuvia sovelluksia kutsutaan myös internetin seuraavaksi kehitysvaiheeksi, Web 3.0:ksi (Sitra 2023).

Toinen esimerkki on Mark Zuckerbergin rakentama metaversumi. Zuckerberg brändäsi Facebookin uudelleen vuonna 2021 Metaksi, alleviivaten yhtiön sosiaalisen median metaversumiin tekemiä investointeja (Facebook 2021a). Zuckerberg kuvasi metaversumin käyttökokemusta seuraavasti: ”Voit siirtyä eri kokemusten välillä eri laitteilla – voit käyttää lisätyn todellisuuden laseja ja pysyä läsnä fyysisessä maailmassa, voit käyttää virtuaalisen todellisuuden laseja ja uppoutua virtuaalimaailmaan täysin tai voit käyttää puhelimia ja tietokoneita päästäksesi sisään olemassa olevilta alustoilta” (Facebook 2021b).

Sekä Decentraland että Metan Metaverse kertoivat vuonna 2023 käyttäjien käyttöönoton olleen melko vähäistä (Paul 2023). Taustalla oleva teknologia ja metaversumien idea tarjoavat kuitenkin merkittävän soveltamiskohteen datan siirrettävyydelle.

Miten datan siirrettävyys liittyy metaversumeihin?

Kuten edellä on todettu, datan siirrettävyydellä on kaksi erillistä tavoitetta. Yhtäältä se on keino, jolla yksilöt voivat osallistua datatalouteen tasavertaisemmin ja itsenäisinä toimijoina ja hyötyä datansa potentiaalisesta arvosta. Samalla se on myös perusoikeuksien toteutumisen väline, joka edesauttaa tietosuojaoikeuden toteutumista (yleisen tietosuoja-asetuksen 20 artiklan mukaisesti).

Ensimmäisen tavoitteen osalta kyse on siitä, voivatko yksityishenkilöt hyötyä oikeudesta datan siirtämiseen metaversumeissa ja voiko tämä oikeus auttaa heitä luomaan datallaan arvoa. Yksi esimerkki metaversumiin sijoittuneesta reilun datatalouden kokeilusta oli Sitran ja Kansallisgallerian yhdessä kuratoima ensimmäinen hajautettuun itsenäiseen organisaatioon sijoittunut metaversumitaidenäyttely (Sitra 2023b). Kokeilu toteutettiin Pariisin vuoden 1900 maailmannäyttelyn Suomen paviljongista tehdyssä virtuaalisessa jäljitelmässä, joka oli luotu maailman suurimman hajautetun itsenäisen organisaation Decentralandin alustalle, jossa näytteillä olevat taideteokset voidaan "lyödä" vaihdettaviksi digitaalisiksi hallintatodistuksiksi. Jos käyttäjät joskus haluaisivat esimerkiksi siirtää hallintatodistuksensa Decentralandista kilpailevaan virtuaalimaailmaan, heillä saattaisi olla kiinnostusta siirtää myös heidän muu datansa mukanaan.

Yleisen tietosuoja-asetuksen 20 artiklan mukaan yksilöiden tulee voida siirtää virtuaalitilassa tuottamansa henkilötiedot. Mikäli virtuaalitodellisuuslaitteita, kuten VR-laseja, kuitenkin pidetään verkkoon kytkettyinä laitteina, jotka keräävät, käsittelevät ja lähettävät dataa, ne saattavat kuulua ehdotetun datasäädöksen piiriin. Säädös laajentaakin tietojen siirrettävyyden oikeuden koskemaan myös tällaisilla laitteilla tuotettua dataa, joka on muuta kuin henkilötietoja.

Tällä hetkellä yksilöillä on rajalliset mahdollisuudet siirtyä metaversumien välillä, koska niiden välinen yhteentoimivuus on lähes olematonta jokaisen metaversumin luodessa omat protokollansa. Näin ollen yksilöt eivät pysty hyötymään datastaan tai digitaalisen omaisuutensa (digitaalisten hallintatodistuksien) siirtämisestä toiseen metaversumiin (Euroopan parlamentti 2022).

Voisivatko yksilöt kuitenkin hyötyä datan siirtämisestä ja jos dataa siirretään välityspalvelulle, joka luo lisäpalveluita metaversumeja käytettäessä? Esimerkiksi pankkialalla yksilöt voivat hyötyä heidän pankkitietojaan analysoivista palveluista (Ferretti 2022). VR-lasit mahdollistavat käyttäjän sijainnin, kehon liikkeiden, ilmeiden ja muun biometrisen tiedon tallentamisen, mutta käyttäjä ei välttämättä pysty hyötymään näistä tiedoista palveluntarjoajan vaihdon jälkeen.

Meta on myös tuonut markkinoille omat Meta Quest -nimiset VR-lasinsa, joissa on viisi sisäänpäin suunnattua kameraa, joiden avulla käyttäjien avatarit voivat reaaliajassa ilmehtiä, hymyillä ja iskeä silmää. Myös Applen

uusilla lisätyn todellisuuden Vision Pro -laseilla on vastaavia ominaisuuksia. Voisivatko yksilöt siirtää ja välittää tällaista dataa kolmannelle osapuolelle? Millaista lisäarvoa datanvälityspalvelut voisivat auttaa käyttäjiä saamaan analysoimalla tällaista yksityiskohtaista käyttäytymisdataa? Voisiko välityspalvelu esimerkiksi auttaa käyttäjiä luomaan kuluttajaprofiileja, joilla yksilöt pystyisivät tienaamaan Weoplen kaltaisten sovellusten avulla? Metaversumeissa keskeistä on, että käyttäjä voi hallita luomaansa dataa. Nykyaikaiset VR-lasit esimerkiksi tallentavat tietoja ihmiskasvoista pitkältä ajalta, joten voisiko käyttäjä antaa oman datansa lääketieteellisen tutkimuksen käyttöön? Pitäisikö ja voisivatko yksilöt siirtää nämä tiedot eurooppalaisen terveystietoalueen piirissä?

Näin luotavan arvon vastapainona on kuitenkin fyysisen ja virtuaalisten maailmojen yhdistämisestä aiheutuva ”ennennäkemätön” huoli yksityisyydensuojasta (Nair et al. 2020). Nair et al. (2020) fasilitoivat pienimuotoisen tutkimuksen metaversumin käyttäjien käyttäytymisestä. Tutkimuksessa huomattiin, että käyttäjien oli vaikea ymmärtää tietojen keruun laajuutta ja kuinka tietoja voidaan käyttää mainonnan kohdentamiseen, tunteiden hyväksikäyttöön ja poliittiseen vaikuttamiseen. Tutkijat kyseenalaistivatkin sen, missä olosuhteissa käyttäjät antavat suostumuksensa tietojen käsittelyyn. Voiko olla olemassa vaara, että käyttäjät “houkutellaan” siirtämään tietonsa välityspalveluille, jotka sitten käyttävät niitä pahantahtoisesti? Tutkijoiden löydökset osoittavat, että jopa anonyymeistä profiileista on mahdollista tunnistaa käyttäjä hyvin nopeasti vain muutaman ominaisuuden perusteella (ja mitä pidempään käyttäjä pysyy alustalla, sitä helpompaa hänen tunnistamisensa on).

Yksityisyydensuojaan liittyvät riskit kasautuvat nopeasti metaversumeissa, kun otetaan huomioon, että alustoilla kerätään paljon arkaluontoista tietoa, kuten sukupuoli, seksuaalinen suuntautuminen, etninen tausta, terveystiedot ja vamma. Riskit kasvavat siitä huolimatta, että hajautetut teknologiat antavat yksilöille mahdollisuuksia hallita datavirtoja ja datan käyttöä ”perustuen yksilön vapaaseen valintaan ja itsemääräämisoikeuteen” (Euroopan komissio 2020a). Anidjar et al. (2023) ehdottavat ratkaisuksi ”pakollisia tiedonantovelvoitteita julkistaa sääntelyviranomaisille, miten käyttäjien yksityisyyttä suojataan”, mutta tämä ei sinällään muuttaisi datatalouden peruslogiikkaa.

5. Kuinka oikeutta datan siirtämiseen voidaan parantaa?

Tämän muistion tavoitteena on ollut tarkastella, miten uudet lainsäädäntöehdotukset, kuten datasäädös ja eurooppalainen terveystietoalue, laajentavat oikeutta datan siirtämiseen ja riittääkö tämä varmistamaan, että oikeus saavuttaa tavoitteensa eli käyttäjien vaikutusmahdollisuuksien lisäämisen ja kilpailun parantamisen yksilön näkökulmasta. Analyysi osoittaa, että hajanainen lähestymistapa datan siirrettävyyteen luo aukkoja ja päällekkäisiä oikeuksia dataan. Seuraavassa osiossa tarkastellaan neljää tapaa, joilla datan siirrettävyyden viitekehystä voitaisiin muuttaa, jotta reilumpaa datataloutta voitaisiin edistää Euroopassa.

Vaihtoehto 1: Voisiko tietosuoja-asetuksen 20 artiklan soveltamisalaa laajentaa?

Yleisen tietosuoja-asetuksen 20 artiklan soveltamisala on rajoitettu muun muassa rekisteröidyn ”antamiin” henkilötietoihin. Toistaiseksi artiklan vaikutus reilun datatalouden rakentamiseen onkin ollut varsin vähäinen. Esimerkiksi Gill ja Metzger (2022) toteavat, että artikla 20 rajoittaa yksilöiden päätösvaltaa heidän dataansa, koska heillä ei ole mahdollisuutta hallita dataa, joka on syntynyt heidän toimintansa seurauksena. He katsovatkin, että ”jos tämä oikeus pysyy tehottamana, rekisteröidyillä on vain hyvin rajallinen päätösvalta dataansa, koska he eivät pysty saamaan oikeudenmukaista osuutta arvosta, joka on luotu heidän toimintansa synnyttämästä datasta. Tämä johtaa siihen, ettei yksilön oikeus päättää omista tiedoistaan eli datasuvereniteetti toteudu”.

Ilmiselvä parannus olisi tietosuoja-asetuksen 20 artiklan laajentaminen koskemaan pääteltyä dataa, mikä antaisi yksilöille mahdollisuuden käyttää oikeuttaan riippumatta oikeusperusteesta, jolloin he voisivat vedota tähän oikeuteen myös viranomaisia vastaan.

Vaihtoehto 2: Voisiko yleisen tietosuoja-asetuksen 20 artikla sisältää henkilötiedot ja muita tietoja?

EU on siirtymässä pois henkilötietojen ja muiden tietojen välisestä kahtiajaosta, mikä on nähtävissä myös ehdotetussa datasäädöksessä ja eurooppalaisessa terveystietoalueessa. Käytännössä data-aineistot ovat lähes aina sekalaisia ja sisältävät tietoja kummastakin kategoriasta ja myös henkilötiedon määritelmä on jatkuvassa muutoksessa (ks. esim. Euroopan unionin tuomioistuimen päätökset *Breyer* ja *Nowak*).

Graef (2019) arvioi, että ”koska ‘muu kuin henkilötieto’ -käsite on luonteeltaan avoin, muuttuva ja dynaaminen, on epätodennäköistä, että siitä tulisi hyödyllinen määrittelykriteeri, jonka varaan yritykset voivat rakentaa innovatiivisten tuotteiden syötteitä”. Hän ehdottaakin, että dataan tulisi suhtautua ”kokonaisvaltaisesti” ilman jaottelua henkilötietoihin ja muuhun dataan. Näin ollen yksi mahdollisuus voisikin olla laajentaa 20 artiklan koskemaan muutakin dataa kuin henkilötietoja, jotta voidaan varmistaa oikeuden olevan tehokas myös käytännössä.

Vaihtoehto 3: Olisiko luotava uusi oikeus datan siirrettävyyteen?

Kuten yllä on todettu, oikeus datan siirrettävyyteen painottaa datan hallintaa ja sillä on erilainen taloudellinen tavoite kuin yleisen tietosuoja-asetuksen takaamilla rekisteröityjen oikeuksilla. Jotkut tutkijat ovat jopa väittäneet, että datan siirrettävyys on ”ensimmäinen askel kohti rekisteröityjen” oletusarvoista henkilötietojensa *omistajuutta* (De Hert ym. 2018). Oikeustieteilijät ovat torjuneet ajatuksen datan sääntelemisestä omaisuutena, koska data on mm. kulumatonta ja ehtymätöntä (esim. Van Erp 2021). On kuitenkin mielenkiintoista pohtia, voitaisiinko oikeus datan siirrettävyyteen ”lisätä” EU:n perusoikeuskirjaan yksityisyyden suojan ja tietosuojan rinnalle.

Perusoikeutena oikeus datan siirtämiseen olisi myös linjassa sen ajatuksen kanssa, että yksilöillä on oikeus tuottamansa datan luomaan taloudelliseen hyötyyn. Tätä näkemystä tukevat myös Sitran ”digitaalista valtaa” koskevan selvityksen tulokset, joissa korostui, että yksilöillä ei ole määräysvaltaa heistä kerättyyn dataan ja suuret teknologiajätit, kuten Meta ja Google, pystyvät saamaan huomattavaa taloudellista hyötyä palveluidensa käyttäjien profiloinnista (Sitra 2022a). Selvityksessä suositellaan, että käyttäjien oikeutta heidän ”omaan” dataansa tulisi käsitellä perusoikeutena, jotta voitaisiin ratkoa yksilöiden puutteellisia hallintamahdollisuuksia datataloudessa. Oikeus datan siirtämiseen pitäisi sisällään oikeuden hallita omaa dataa ja oikeuden datasta saatavaan taloudelliseen hyötyyn.

Ehdotuksen toteutuskelpoisuudesta tarvitaan lisätutkimuksia, mutta on selvää, että reilun datatalouden toteutumiseksi yksilöiden on oltava aktiivisia osallistujia eikä vain suojelua tarvitsevia kohteita.

Vaihtoehto 4: Tarvitaanko uusi oikeudellinen instrumentti datan siirrettävyyteen?

Yksi vaihtoehto olisi myös kehittää uutta lainsäädäntöä, joka määrittäisi tarkasti, millaista dataa voidaan siirtää ja jolla olisi riittävän laaja soveltamisala (”kaikki data”, ”kaikilla aloilla”, ”kaikki tuotteet”), jotta yksilöiden vaikutusmahdollisuuksia heidän dataansa voitaisiin parantaa. Tällainen instrumentti voitaisiin sijoittaa kuluttajansuojalakiin ja se voisi ottaa huomioon

yksilöiden erilaiset kognitiiviset kyvyt, kun he tekevät päätöksiä verkossa. Päätöksiin vaikuttaa tapa, jolla digitaalinen ympäristö on suunniteltu hyödyntämään ihmisten kognitiivisia vinoutumia. Kuluttajansuojalaissa yksilöitä pidetään ”heikompana osapuolena” ja heille annetaan enemmän suojaa (Benöhr 2013).

Vaikka ehdotetun sähköisen viestinnän tietosuoja-asetuksen tarkastelu ei kuulunut tämän muistion piiriin, on syytä korostaa, että on olemassa vaara, että yksilöt siirtävät tietämättään edelleen evästeiden kautta tietojaan kolmansille osapuolille ja ilman että he itse hyötyvät yrityksille tuottamastaan arvosta. Siksi sähköisen viestinnän tietosuojaa koskevaa ehdotusta olisi tarkasteltava myös datan siirrettävyyden kannalta.

6. Johtopäätökset

Tämän muistion tavoitteena oli ensinnäkin tarkastella, kuinka uudet lainsäädännölliset ehdotukset, kuten datasäädös ja eurooppalainen terveystietoalue, laajentavat oikeutta datan siirrettävyyteen yleisen tietosuoja-asetuksen 20 artiklan soveltamisalasta, sekä sitä, mitä rajoitteita yksilöiden mahdollisuudella käyttää tuota oikeutta on. Datan siirrettävyyttä koskevan oikeuden laajennetun oikeudellisen viitekehyksen analyysi osoittaa, että vaikka ehdotettu datasäädös ja eurooppalainen terveystietoalue antavat yksilöille uusia oikeuksia siirtää verkkoon kytketyillä laitteilla tuotettuja tietoja ja terveystietoja, näiden oikeuksien soveltaminen pysyy vielä alakohtaisena. Säädökset täydentävät yleisen tietosuoja-asetuksen 20 artiklaa, jonka ansiosta yksilöillä on oikeus siirtää henkilötietojaan kolmansille tahoille, mutta niillä ei voida korjata itse säännöksen rajallista soveltamisalaa.

Ei ole selvää, pystyvätkö yksilöt saavuttamaan datan siirrettävyyden taloudellisen tavoitteen rajallisella alakohtaisella soveltamisalalla. Myös tekniset rajoitteet ovat haaste oikeuden käytölle. Yrityksille tulisikin luoda enemmän kannustimia kehittää yhteentoimivia palveluita. Datanvälityspalvelut, kuten henkilötietojen hallintajärjestelmät, voivat merkittävästi auttaa yksilöitä luomaan arvoa datallaan, mutta tähän liittyy kaksi riskiä.

Ensimmäinen riski on, että EU sääntelee vielä kypsymätöntä markkinaa, jolla datanvälityspalvelut ovat vasta löytämässä liiketoimintamallejaan ja käyttäjiään. Sääntelyn puuttuessa vaarana kuitenkin on, etteivät kuluttajat luota datanvälityspalveluihin ja näin niiden hyöty kuluttajien hyvinvoinnille jää EU:ssa selvittämättä.

Datanvälityspalveluilla voi olla myös merkitystä uusissa teknologisissa kehityssuunnissa, kuten metaversumeissa ja web 3.0:ssa, joiden palveluissa pyritään yhtä lailla houkuttelemaan käyttäjiä ja kehittämään markkinaa. Hajautettu teknologia tarjoaa yksilöille aidon mahdollisuuden saada lisää päätösvaltaa oman datansa hallintaan. Tämä hyöty on kuitenkin punnittava suhteessa riskiin päätösvallan menettämisestä, kun arkaluontoisia tietoja kerätään yhä enemmän virtuaalitodellisuuksissa (esimerkiksi VR-lasien kautta) ja kun toimitaan digitaalisessa ympäristössä, joka on suunniteltu käyttämään käyttäjien kognitiivisia vinoumia hyväksi.

Toisena riskinä on, että painottamalla datanvälityspalvelujen roolia tullaan samalla korostaneeksi entisestään käyttäjien suostumusta datan siirron oikeutuksena. Kysymys kuuluukin, asetetaanko näin yksilöille enemmän vastuuta ymmärtää datan jakamiseen liittyviä riskejä ilman että on asianmukaisia mekanismeja muutoksenhakuun. Haasteita datan väärinkäytön tai puutteellisten datansiirtotoimien oikeussuojatoimille aiheuttaa myös dataa koskevien säädösten (kuten datasäädös, datanhallinta-asetus ja yleinen tietosuoja-asetus) vaatimusten noudattamisesta vastaavien viranomaisten monimutkainen ”hajautettu” rakenne.

Datan siirrettävyydessä onkin pohjimmiltaan kyse siitä, kuinka luodaan reilu datatalous, jossa yksilöt ovat itsenäisiä ja heillä on määräysvaltaa omaan dataansa. Datan siirrettävyyden oikeuden laajentaminen datasäädöksen ja eurooppalaisen terveystietoalueen myötä on askel oikeaan suuntaan, mutta lisätoimia tarvitaan yleisen tietosuoja-asetuksen 20 artiklan rajatun soveltamisalan korjaamiseksi.

Tämän vuoksi muistiossa on käyty läpi hypoteettisia mahdollisuuksia täysimääräiselle datan siirrettävyyden oikeudelle. Esitetystä neljästä vaihtoehdosta kaikkein kunnianhimoisin olisi datan siirrettävyyden oikeuden nostaminen uudeksi perusoikeudeksi yksityisyyden ja tietosuojan rinnalle. Tämä korostaisi yksilöiden taloudellisia ja muita oikeuksia suhteessa heidän dataansa ja heidän oikeuttaan hyötyä digitaalisessa ympäristössä synnyttämästään datasta. Se olisi todellinen askel kohti reilumpaa datataloutta.

Lähteet

EU-lainsäädäntö

Tietokantadirektiivi. Euroopan parlamentin ja neuvoston direktiivi 96/9/EY, annettu 11 päivänä maaliskuuta 1996, tietokantojen oikeudellisesta suojasta, OJ L 77, 27.3.1996.

Datanhallinta-asetus. Euroopan parlamentin ja neuvoston asetus (EU) 2022/868, annettu 30 päivänä toukokuuta 2022, eurooppalaisen datan hallinnoinnista ja asetuksen (EU) 2018/1724 muuttamisesta (datanhallinta-asetus), OJ L 152, 3.6.2022.

Digimarkkinasäädös. Euroopan parlamentin ja neuvoston asetus (EU) 2022/1925, annettu 14 päivänä syyskuuta 2022, kilpailullisista ja oikeudenmukaisista markkinoista digitaalialalla ja direktiivien (EU) 2019/1937 ja (EU) 2020/1828 muuttamisesta (digimarkkinasäädös), OJ L 265, 12.10.2022.

ePrivacy-direktiivi. Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi), OJ L 201, 31.7.2002.

Yleinen tietosuoja-asetus (GDPR). Euroopan parlamentin ja neuvoston asetus (EU) 2016/679, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), EUVL L 119, 4.5.2016.

Euroopan unionin tuomioistuimen tapausoikeus

Peter Nowak vastaan Data Protection Commissioner (C-434/16) [2016] ECLI:EU:C:2017:994

Patrick Breyer vastaan Saksan liittotasavalta (C-582/14) [2014] ECLI:EU:C:2016:779

Toissijaiset lähteet

Anidjar et al. 2023. The Matrix of Privacy: Data Infrastructure in the AI-powered metaverse. Harvard Law & Policy Review, Julkaisematon. Viitattu 10.5.2023.

29 artiklan mukainen työryhmä 2007. Lausunto 4/2007 henkilötietojen käsitteestä. WP 136, 20 kesäkuuta 2007. Viitattu 30.6.2023.

29 artiklan mukainen työryhmä 2014. Lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä. WP 217, 9 huhtikuuta 2014. Viitattu 30.6.2023.

29 artiklan mukainen työryhmä 2017. Guidelines on the right to data portability. WP 242 rev.01, 5 huhtikuuta 2017. Viitattu 30.6.2023.

Euroopan kuluttajaliitto (BEUC) 2021. Recommendations for the trilogue negotiations on the proposed e-Privacy Regulation. BEUC-X-2021-106. Viitattu 16.5.2023.

Euroopan kuluttajaliitto (BEUC) 2022. Giving consumers control of their data - BEUC position paper on the Data Act proposal. BEUC-X-2022-103. Viitattu 10.5.2023.

Benöhr 2023. EU Consumer Law and Human Rights. Oxford University Press, Oxford. Viitattu 30.6.2023.

Colangelo 2022. European Proposal for a Data Act: A First Assessment. CERRE Assessment Paper, Heinäkuu 2022. Viitattu 10.5.2023.

Cravo 2022. How to make data portability right more meaningful for data subjects? European Data Protection Law Review, 8(1), 52–60. Viitattu 30.6.2023.

De Hert et al. 2018. The right to data portability in the GDPR: Towards user-centric interoperability of digital services. Computer Law & Security Review, 34(2), 193-203. Viitattu 30.6.2023.

Ducuing et al. 2022. White Paper on the Data Act Proposal. CiTiP Working Paper 2022. Viitattu 10.5.2023.

EDPB-EDPS 2022. Euroopan tietosuojaneuvoston ja Euroopan tietosuojavaltuutetun yhteinen lausunto 2/2022 ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös). 4.5.2022. Viitattu 10.5.2023.

Euroopan komissio 2017a. Euroopan datavetoisen talouden rakentaminen. COM(2017) 9 final.

Euroopan komissio 2017b. Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus). COM(2017) 10 final.

Euroopan komissio 2020a. Euroopan datastrategia. COM(2020) 66.

Euroopan komissio 2020b. Komission tiedonanto Euroopan parlamentille ja neuvostolle Tietosuojasäännöt kansalaisten vaikutusmahdollisuuksien ja EU:n digitaalisen muutoksen edistäjänä – yleistä tietosuoja-asetusta sovellettu kaksi vuotta. COM(2020) 264 final.

Euroopan komissio 2022a. Ehdotus Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös). COM(2022) 68 final.

Euroopan komissio 2022b. Komission yksiköiden valmisteluasiakirja: Impact assessment report accompanying the document Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act). SWD(2022) 34 final.

Euroopan komissio (2022c). Ehdotus Euroopan parlamentin ja neuvoston asetukseksi eurooppalaisesta terveysdata-avaruudesta. COM/2022/197 final.

Euroopan parlamentti 2023a. Datasäädös: mepit tukevat sääntöjä datan reilulle käytölle ja jakamiselle. Lehdistötiedote, 14.3.2023. Viitattu 10.5.2023.

Euroopan parlamentti 2023b. Euroopan parlamentin tarkistukset 14. maaliskuuta 2023 ehdotukseen Euroopan parlamentin ja neuvoston asetukseksi datan oikeudenmukaista saatavuutta ja käyttöä koskevista yhdenmukaisista säännöistä (datasäädös). COM(2022)0068 – C9-0051/2022 – 2022/0047(COD). P9_TA(2023)0069**.**

Ferretti 2022. A single European data space and data act for the digital single market: on datafication and the viability of a PSD2-like access regime for the platform economy. European journal of legal studies, 14(1), 173-218. Viitattu 10.5.2023.

Graef et al. 2017. Lessons for an Emerging Concept in EU Law. German Law Journal 19 (6), 1359-1398, Tilburg Law School Research Paper No. 2017/22, TILEC Discussion Paper No. 2017-041. Viitattu 10.5.2023.

Graef et al. **2019**. Towards a holistic regulatory approach for the European data economy: why the illusive notion of non-personal data is counterproductive to data innovation. European Law Review 44, 605-21. Viitattu 30.6.2023.

Gill ja Metzger 2022. Data Access through Data Portability – Economic and Legal Analysis of the Applicability of Art. 20 GDPR to the Data Access Problem in the Ecosystem of Connected Cars. European Data Protection Law Review, 3/2022. Viitattu 10.5.2023.

Hondagneu-Messner 2021. Data Portability: A Guide and a Roadmap. Rutgers Computer & Technology Law Journal, 240. Viitattu 10.5.2023.

Krämer et al. 2023. Data Act: Towards a balanced EU data regulation. Centre on Regulation in Europe (CERRE). Viitattu 16.5.2023.

Lindroos-Hovinheimo 2021. Private selves: Legal personhood in European privacy protection. Cambridge University Press, Cambridge.

Meta 2021a. Introducing Meta: A social technology company. 28.10.2021. Viitattu 10.5.2023.

Meta 2021b. Founder's letter. 28.10.2021. Viitattu 10.5.2023.

Mäihänniemi 2022a. Attention being bought and sold by online platforms. User's self-determination in governing their own data as a dimension of consumer welfare in antitrust? EU antitrust: Hot topics and next steps: Proceedings of the International Conference held in Prague on January 24–25. Viitattu 10.5.2023.

Mäihäniemi 2022b. The role of behavioural economics in shaping remedies for Facebook's excessive data gathering. Computer Law & Security Review, 46. Viitattu 30.6.2023.

Nair et al. 2022. Exploring the Unprecedented Privacy Risks of the Metaverse. ArXiv:2207.13176. Viiitattu 10.5.2023

OECD 2021. Data portability, interoperability and digital platform competition. OECD Competition Committee Discussion Paper. Viitattu 10.5.2023.

Pop ja Grant 2023. Data portability in the European Health Data Space: Benefits, Risks, and Challenges. EIPA, 29 March 2023. Viitattu 10.5.2023.

Sitra 2022a. Digivallan jäljillä: Miten datan avulla voidaan vaikuttaa päättäjiin ja ohjata maailmaa. Sitran selvityksiä 215. Viitattu 10.5.2023.

Sitra 2022b. EU-sääntely rakentaa reilumpaa datataloutta: Euroopan viiden datalainsäädäntöehdotuksen tarjoamat mahdollisuudet yrityksille, yksilöille ja julkiselle sektorille. Työpaperi, 7.6.2022. Viitattu 30.6.2023.

Sitra 2023a. Kieli kehittyy: Internetin kolmannen kehitysvaiheen käsitteitä. Viitattu 10.5.2023.

Sitra 2023b. Sitran ja Kansallisgallerian virtuaalinen näyttelykokeilu tarjosi näkymän tulevaisuuden taidekokemukseen. Viitattu 21.6.2023.

Solove 2023. The Limitations of Privacy Rights. Notre Dame Law Review, GWU Legal Studies Research Paper No. 2022-30, GWU Law School Public Law Research Paper No. 2022-30. Viitattu 10.5.2023.

Swire 2020. The portability and other required transfers impact assessment: Assessing Competition, Privacy, cybersecurity, and other considerations. Viitattu 10.5.2023.

Tombal ja Graef 2023. The Regulation of Access to Personal and Non-personal Data in the EU: From Bits and Pieces to a System? TILEC Discussion Paper No. 2022-019. Viitattu 10.5.2023.

Turner et al. 2020. The exercisability of the right to data portability in the emerging internet of things (IOT) environment. New Media & Society, 23(10), 2861–2881. Viitattu 10.5.2023.

Van Erp 2021. Covid-19 apps, Corona vaccination apps and data "ownership". Viitattu 10.5.2023.

Wong ja Henderson 2019. The right to data portability in practice: Exploring the implications of the technologically neutral GDPR. International Data Privacy Law, 9(3), 173–191. Viitattu 30.6.2023.

Kirjoittaja

Sanna Toropainen on väitöskirjatutkija Helsingin yliopiston Legal Tech Labissä. Hänen tutkimuskohteitaan ovat digitaalisten identiteettien oikeudellinen viitekehys ja identiteetteihin liittyvän datan siirrettävyys digitaalisten identiteettilompakoiden avulla. Hänellä on oikeustieteen tutkinto (LLB/LLM) Maastrichtin yliopistosta Alankomaista. Ennen tutkijanuraansa hän oli perustamassa startup-yritystä, jonka tavoitteena oli auttaa yksilöitä ansaitsemaan henkilötiedoillaan. Työskentely tietosuoja- ja kyberturva-asiantuntijana Suomessa ja Belgiassa on tuonut hänelle syvällistä ymmärrystä yksityisyyden suojaan ja tietosuojaan liittyvistä kysymyksistä. Toropainen laati Sitran toimeksiannosta ulkopuolisena asiantuntijana muistion ”Oikeus datan siirtämiseen järjestelmästä toiseen reilussa datataloudessa – Kuinka laajentaa yksilöiden oikeutta hyötyä tietojensa hallinnasta”.

SITRA

SITRAN MUISTIO 25.1.2024
Sitran muistiot ovat tulevaisuustyötämme tukemaan tuotettua tietoa.

ISBN 978-952-347-349-2 (PDF)
www.sitra.fi

SITRA.FI
Itämerenkatu 11–13
PO Box 160
FI-00181 Helsinki, Finland
Tel: +358 294 618 991