Pro Gradu -tutkielma

Anna-Maria Laaksonen

2020

Lappeenrannan-Lahden teknillinen yliopisto LUT

School of Business and Management

Yritysjuridiikka

Anna-Maria Laaksonen

Puettavilla älylaitteilla kerätty terveysdata – oikeudet ja hyödyntäminen

Pro gradu -tutkielma

Tarkastajat

KTT, dosentti Helena Sjögrén

OTT, dosentti Mikko Huuskonen

TIIVISTELMÄ

Tekijä:	Anna-Maria Laaksonen
Tutkielman nimi:	Puettavilla älylaitteilla kerätty terveysdata – oikeudet ja hyödyntäminen
Tiedekunta:	School of Business and Management
Vuosi:	2020
Pro Gradu -tutkielma:	Lappeenrannan-Lahden teknillinen yliopisto LUT
	71 sivua, 1 kuva, 1 liite
Tarkastajat:	KTT, dosentti Helena Sjögrén
	OTT, dosentti Mikko Huuskonen
Hakusanat:	Puettavat älylaitteet, oikeudet terveysdataan, datan omistusoikeus, datan hyödyntäminen

Puettavien älylaitteiden käyttö kuluttajien keskuudessa yleistyy koko ajan ja niillä kerätylle, käyttäjän terveyteen liittyvälle datalle on monia halukkaita hyödyntäjiä. Terveysdataan sisältyvä merkittävä taloudellinen potentiaali ja sen hyödyntäminen pakottavat tarkastelemaan dataan liittyvien oikeuksien hallintaa. Tutkimuksessa selvitettiin puettavilla älylaitteilla kerätyn terveysdatan liittyvien oikeuksien toteutumista nykytilanteessa sekä vaihtoehtoisia datan hallintatapoja. Vaihtoehtoisina malleina tarkasteltiin mahdollista omistusoikeutta terveysdataan sekä ihmiskeskeisiä datan hallintamalleja. Tutkimus toteutettiin lainopillisena kirjallisuustutkimuksena, jonka tuloksia syvennettiin puolistrukturoiduilla asiantuntijoiden teemahaastatteluilla.

Tutkimuksen perusteella terveysdatan nykyiseen, datan kerääjän hallitsemaan tilanteeseen ei ole tarjolla nopeaa ratkaisua. GDPR on selventänyt terveysdataan liittyviä oikeuksia vasta alustavasti, eikä asetus anna työkaluja datan hyödyntämiseen. Vaikka datan omistusoikeutta on esitetty ratkaisuksi datatalouden markkinoiden epäonnistumisiin ja datan hyödyntämisen ulkoisvaikutuksiin, omistusoikeuden käytännön toteuttaminen näyttää todella vaikealta, johtuen datan erityisominaisuuksista oikeuksien kohteena. Datan potentiaalin optimaalinen hyödyntäminen ja siihen sisältyvän arvon tasapainoisempi jakautuminen yhteiskunnassa näyttävät vaativan kuitenkin jonkinlaista selkeämpää viitekehystä oikeuksien hallintaan.

Kerätyn datan tehokas hyödyntäminen ja yksilön oikeuksien vahvistaminen näyttävät olevan jossain määrin ristiriitaisia tavoitteita. Myöskään ihmiskeskeiset datan hallintamallit eivät ole helppo ratkaisu intressien yhteensovittamiseen. Ihmiskeskeisissä malleissa nähdään kuitenkin potentiaalia tulla taloudellisesti perustelluksi vaihtoehdoksi nykyiselle datan kerääjien hallitsemalle ja läpinäkymättömälle datan markkinalle, jos ne keräävät tarpeeksi poliittista ja yhteiskunnallista tukea. Ennen kuin terveysdatan oikeuksien nykyistä tilannetta muuttaa disruptio, sääntely tai datan oikeuksiin liittyvät ennakkotapaukset, terveysdatan tosiasiallinen hallinta pysyy sen kerääjällä ja puettavien älylaitteiden käyttäjän oikeudet terveysdataan ovat tietosuojalainsäädännön ja käyttäjän oman aktiivisuuden varassa.

ABSTRACT

Author:	Anna-Maria Laaksonen
Title:	The Rights and Use of Health Data Collected by Wearables
Faculty:	School of Business and Management
Year:	2020
Master's Thesis:	Lappeenranta-Lahti University of Technology LUT
	71 pages, 1 figure, 1 appendix
Examiners:	D.Sc. (Econ. and Bus. Adm.), Docent Helena Sjögren
	LL.D., Docent Mikko Huuskonen
Keywords:	Wearables, rights to health data, data ownership, data utilization

Wearable smart devices are becoming increasingly popular among consumers, and there is considerable interest in utilizing the collected health data in several fields. The data carries so much financial potential, that the legal aspects of data rights cannot be ignored. This study is focused on the legal and practical implementation of these rights in the case of wearable technologies. In addition to current practices, the study considers personal ownership to health data and human centric management models. Research methods include legal literature survey and semi-structured interviews of data management professionals.

The results show that there is no easy solution to the current state of affairs, controlled by data collector. GDPR has provided only introductory, yet to be tested, framework for individual rights and show little to no potential for utilization of health data collected by wearables. Data ownership has been suggested and considered as a solution to market failures and externalities of data economy. The practical implementation of data ownership, however, has turned out to be challenging. This is due to the specific characteristics of data as the object of legal ownership.

The optimal utilization of health data and equitable distribution of its associated value calls for a transparent and unambiguous framework for the management of data rights. Human centric data management models have been proposed to reconcile the conflicting interests of data subjects and data users. Human centric models show some potential as the alternative for current practices, dictated by the data collector. This, however, necessitates that the revised approach attracts sufficient political and societal support. Until a new paradigm for data rights and utilization emerges, de facto control to health data is with the data collector and user's rights to their health data remain limited, dependent on data privacy laws and individual awareness.

Sisällysluettelo

Lainsäädäntö

Kuluttajansuojalaki 38/1978 (KSL)
Laki varallisuusoikeudellisista oikeustoimista 13.6.1929/228 (OikTL)
Liikesalaisuuslaki 595/2018
Tekijänoikeuslaki 8.7.1961/404
Tietosuojalaki 5.12.2018/1050
Laki sosiaali- ja terveystietojen toissijaisesta käytöstä 552/2019 (toisiolaki)

Lainsäädäntö (EU)

Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoitu toisinto 2016. 2012/C 326/01 (EU:n perussopimus)

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 (tietosuoja-asetus, GDPR)

Hallituksen esitykset

Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi, HE 300/2018 (toisiolaki)

Direktiivit

Euroopan parlamentin ja neuvoston direktiivi tietyistä digitaalisen sisällön ja digitaalisten palvelujen toimittamista koskeviin sopimuksiin liittyvistä seikoista 2019/770 (digitaalisen sisällön direktiivi)

Euroopan parlamentin ja neuvoston direktiivi 96/9/EY, annettu 11 päivänä maaliskuuta 1996, tietokantojen oikeudellisesta suojasta (tietokantadirektiivi)

Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943, annettu 8 päivänä kesäkuuta 2016, julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta (liikesalaisuusdirektiivi)

1 Johdanto

1.1 Tutkimuksen taustaa ja motivointi

Oma hyvinvointi ja terveys kiinnostavat ihmisiä koko ajan enemmän ja niiden mittaamiseen soveltuvien puettavien älylaitteiden markkina kasvaa nopeasti. Jo joka kolmas suomalainen käyttää jonkinlaista hyvinvointia ja terveyttä mittaavaa älylaitetta (Terveystalo 2018). Maailmalla käytössä olevien laitteiden määrä yli tuplaantunut kolmessa vuodessa ja arvioidaan ylittävän miljardin laitteen rajan vuoteen 2022 mennessä (Statista 2020).

Puettava älylaite on käytännössä pieni tietokone, joka mittaa, kerää ja analysoi tietoa käyttäjästään (Holst 2020). Käyttäessään puettavaa teknologiaa, kuten älykelloa, kuluttaja jakaa yksityisten yritysten kanssa reaaliaikaisesti henkilökohtaiseen terveydentilaansa liittyviä tietoja, joihin on aikaisemmin päässyt käsiksi korkeintaan terveydenhuoltohenkilöstö. Siinä missä jo perinteisten älylaitteiden kuten kännyköiden yksityisyydestä on oltu huolissaan, puettava teknologia on usein kokoaikaisesti fyysisesti kiinni henkilössä, mitaten monia fysiologia toimintoja ja keräten hyvin paljon tietoa käyttäjästään ja tämän elintavoista. Hyödyntämismahdollisuuksia datalle syntyy laitteiden yleistyttyä koko ajan lisää. Puettavalla älylaitteella voi olla jopa mahdollista diagnosoida käyttäjän virustartunta ajankohtaisessa COVID19-pandemiassa (Savonen 2020).

Puettavan teknologian hyödyntämisestä odotetaan suuria säästöjä ja toiminnan tehostumista monilta eri aloilta (Manyika et al. 2015, 2-3). Kuluttajille tutuin käyttökohde puettaville älylaitteille on oman terveyden ja hyvinvoinnin mittaaminen. Terveysdatan keräämisen ja hyödyntämisen arvioidaan muuttavan terveydenhuollon toimintatapaa ja mahdollistavan siirtymisen kohti sairauksien ehkäisyä ja hyvinvoinnin edistämistä (Kääriä 2018). Laitteiden käytöstä saatava taloudellinen hyöty kroonisten sairauksien hoidossa arvioidaan olevan sadoista miljardeista biljoonaan dollariin vuosittain (Manyika et al. 2015, 8). Yksistään kuluttajien käyttämien hyvinvointia mittaavien älylaitteiden tuomat terveyshyödyt parempana tuottavuutena arvioidaan olevan 600 miljardia vuodessa (Manyika et al. 2015, 45).

Puettavien älylaitteiden ja palvelujen käyttö kuitenkin edellyttää kuluttajien luottamusta tietojensa suojaamiseen ja yksityisyyteen sekä siihen, ettei niitä väärinkäytetä. Viranomaiset pyrkivät suojaamaan kuluttajia ja pysymään teknologisen kehityksen mukana lakimuutoksilla kuten vuonna 2018 voimaan tulleella EU:n tietosuoja-asetuksella, jonka tarkoitus on antaa yksityisille ihmisille

paremmat mahdollisuudet hallita omia henkilötietojaan. Koko ajan muuttuvan teknologian maailmassa lait tulevat kuitenkin aina hiukan jäljessä, eikä niitä ei voida tehdä kaikkia tilanteita kattaviksi.

Yhdistelemällä tietoja eri laitteista ja lähteistä yrityksillä voi olla näennäisesti rajattomat mahdollisuudet selvittää käyttäjän terveyttä, elintapoja ja reaktioita. Tämä on avannut aivan uuden luokan mahdollisuudet kuluttajan tietojen hyödyntämiseen ja esimerkiksi yksilölliseen markkinointiin. Samalla mahdollisuus ja riski yksilön tietojen väärinkäyttöön lisääntyy.

Esimerkiksi teknologiajätti Googlella on oma puettavien älylaitteiden käyttöjärjestelmä WearOS, maailman käytetyin hakukone ja tytäryhtiönsä kautta Britannian julkisen terveydenhuoltojärjestelmän tietoja potilaista. Tytäryhtiö on luvannut olla yhdistämättä tietoja Google-tileihin, mutta myöhempien yritysjärjestelyjen myötä tämä on mahdollista. Asiantuntijat varoittavat terveystietojen päätyvän helposti odottamattomiin kohteisiin. (Ovaskainen 2018).

Terveyteen liittyvä data on arvokasta monille muillekin kuin puettavan älylaitteen käyttäjälle ja siihen haluavat päästä käsiksi niin yritykset, viranomaiset kuin tutkijatkin. Myös mainostajat ja vakuutusyhtiöt ovat luonnollisesti kiinnostuneita kuluttajien terveyteen liittyvästä datasta. Valtio on pyrkinyt jo vuosia määrätietoisesti edistämään terveystiedon hyödyntämistä ja siihen perustuvaa liiketoimintaa, sekä poistamaan hyödyntämistä hidastavia lainsäädännöllisiä esteitä (Valtioneuvosto 2017).

Viranomaiset kannustavat kuluttajia lataamaan oman puettavien älylaitteilla kerätyn datansa viranomaisen palveluissa kuten Kanta.fi:ssä hoidon laadun parantamiseksi, vaikka tiedon hyväksikäyttö asiakkaan hoidossa odottaakin vielä uuden asiakastietolain voimaantuloa (Kanta-palvelut 2019). Tietojen luovuttamisen viranomaiselle ja edelleen viranomaiselta eteenpäin luvataan auttavan yksilöllisemmän ja tehokkaamman hoidon kehityksessä. Tavoitteena on myös houkutella uuden terveystiedon ekosysteemin perässä Suomeen ulkomaista innovaatiotoimintaa ja tutkimusryhmiä. Viranomaiset vakuuttavat kuitenkin yksilön tietosuojan ja yksityisyyden säilyvän. (Valkama 2019)

Tiedon omistajuus ja käyttöoikeus nousevat keskeisiksi kysymyksiksi kun tiedolle on monta halukasta hyödyntäjää. Datan hyväksikäytön ja myynnin markkinat kehittyvät koko ajan. Erilaisilla älylaitteilla kerätyn big data -markkinan arvo kasvaa 36 % vuosivauhtia ja sen ennustetaan ylittävän

10 miljardin raja vuoteen 2021 mennessä (Western Digital 2020). Laskentajärjestelmien kehitys tekee myös datasta koko ajan arvokkaamman resurssin, koska analysoinnin myötä siitä saadaan koko ajan nopeammin ja tarkempaa tietoa (Dynes 2018).

Myös laitteen käyttäjällä voi olla syytä hyödyntää tai kaupallistaa oma terveysdata. Vaikka peruskäyttäjien mahdollisuuteen myydä omaa dataansa suhtaudutaan vielä epäillen (Garcia Martinez 2019), joissain tapauksissa puettavien laitteiden käyttäjät kuten urheilijat ovat jo voineet hyötyä taloudellisesti omien tietojensa jakamisesta. Esimerkiksi amerikkalaisen jalkapalloliigan NFL:n urheilijoilla on ollut mahdollisuus myydä omaa biometristä dataansa yhteistyössä aktiivisuusrannekevalmistajan ja oman urheiluliittonsa kanssa (Boyd 2018).

1.2 Muutokset lainsäädännössä

Terveystietojen hallintaan liittyvät säädökset ovat olleet viime vuodet muutoksessa. Monet lait ovat muuttuneet niin tietosuojan kuin yksilön henkilötietojen hallinnan osalta. Uuden asiakastietolain (Hallituksen esitys eduskunnalle laiksi sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä sekä eräiksi siihen liittyviksi laeiksi, HE 300/2018) pitäisi tulla voimaan kesäkuussa 2020. Lain on tarkoitus helpottaa asiakkaan tietojen siirtymistä eri terveyspalvelutuottajien välillä sekä asiakkaan omien puettavalla laitteella kerättyjen hyvinvointitietojen hyödyntämistä hoidossa (Komulainen 2020, 6). Samalla uusi laki mahdollistaa uusien biopankki- ja genomilakien säätämisen.

EU:n tietosuoja-asetus (Euroopan parlamentin ja neuvoston asetus 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta, GDPR) tuli voimaan toukokuussa 2018. Lain tarkoitus on parantaa yksilön mahdollisuuksia hallita ja suojata omia tietojaan. Samalla sen tarkoitus on maksimoida digitaalitalouden kasvupotentiaali Euroopassa (EU COM 2015, 4). Toisiolaki eli laki sosiaali- ja terveystietojen toissijaisesta käytöstä (552/2019) tuli voimaan huhtikuussa 2019. Toisiolaki mahdollistaa uuden viranomaisen, vuoden 2020 alussa toimintansa aloittaneen FinDatan, välittää suomalaisten terveystietoja tutkijoille ja muille kiinnostuneille (Valkama 2019). Nämä toimet ovat määrätietoisia askelia valtion pyrkimyksessä tehdä terveystoimialasta ja lääketieteellisestä tutkimuksesta uusi talouden veturi. (HUS 2016; STM 2016)

Digitaalisen sisällön direktiivi (Euroopan parlamentin ja neuvoston direktiivi tietyistä digitaalisen sisällön ja digitaalisten palvelujen toimittamista koskeviin sopimuksiin liittyvistä seikoista, 2019/770) tuli voimaan 2019 ja sitä pitäisi soveltaa kansallisesti kahden vuoden sisällä, mutta valmistelu on kesken. Direktiivin tarkoituksena on tehdä digitaalisten tuotteiden ja palveluiden ostamisesta helpompaa ja turvallisempaa kuluttajille ja toimittamisesta helpompaa yrityksille, ja tätä kautta edistää eurooppalaista digitaalitaloutta ja talouskasvua (Digitaalisen sisällön direktiivi johdanto-osa 1). Direktiivissä (johdanto-osa 24) myös parannetaan jossain määrin niiden kuluttajien asemaa, jotka saavat digitaalisia palveluita tai tuotteita henkilötietojensa luovuttamista vastaan.

1.3 Tutkimuksen tavoite ja tutkimuskysymykset

Terveysdatan arvon optimaalinen hyödyntäminen yhteiskunnallisella tasolla vaatii sitä, että osapuolet tietävät tarkasti omat oikeutensa ja velvollisuutensa sekä tiedon hallintaan liittyvät riskit, ja voivat luottaa lain tulkintaan. Jos tiedon omistajuus on epäselvä, käyttäjät voivat vältellä teknologian käyttöä ja palveluntarjoaja tai muu datan ekosysteemi tiedon hyödyntämistä. Myös datan myynnin ja muun kaupallistamisen kynnys nousee, jos omistusoikeuden tila on epäselvä. Näissä tilanteissa yhteiskunta menettää osan puettavan teknologian taloudellisesta potentiaalista.

Tutkimuksen tavoitteena on selventää puettavalla teknologialla kerätyn terveysdatan oikeuksien jakautumista ja toteutumista *nykytilanteessa*, sekä tarkastella nykytilanteeseen nähden kahta muuta datan hallintamallia. Tutkimuksessa selvitetään miten datan mahdollinen *omistusoikeus* tai *ihmiskeskeiset datan hallintamallit* soveltuisivat terveysdatan oikeuksien hallintaan. Tutkimuksessa tarkastellaan erityisesti oikeuksien jakautumista käyttäjän ja laitteen valmistajan tai palveluntarjoajan välillä. Tutkimuksessa pyritään vastaavaan seuraaviin kysymyksiin:

- Miten puettavalla teknologialla kerätyn terveysdatan oikeudet jakautuvat laitteen käyttäjän ja palveluntarjoajan välillä tällä hetkellä?
- Onko puettavalla teknologialla kerättyyn terveysdataan mahdollista luoda lainsäädännön kautta omistusoikeus ja millaisen oikeudellisen viitekehyksen kautta se olisi mahdollista?
- Millaisina datan oikeuksien hallinnan asiantuntijat näkevät terveysdatan oikeuksien jakautumisen nykytilanteessa sekä oikeuksien kehityksen tulevaisuudessa?
- Miten käyttäjän terveysdatan erilaiset hallintamuodot vaikuttavat tai vaikuttaisivat yksilön oikeuksiin, yritysten toimintamahdollisuuksiin ja yhteiskunnalliseen etuun?

1.4 Tutkimuksen rajaukset ja perustelut

Tässä tutkimuksessa tarkastellaan kuluttajille suunnattuja, puettavia älylaitteita, joiden on tarkoitus olla lähes kokoaikaisesti käyttäjässä kiinni ja kerätä yksilöön liittyvää tietoa. Vaikka puettavat älylaitteet kuten älykellot keräävät käyttäjän terveyteen liittyvää tietoa, ne tulee erottaa *lääkinnällisistä laitteista*, joita säädellään erillisellä lainsäädännöllä (e.g. Laki terveydenhuollon laitteista ja tarvikkeista, 24.6.2010/629) ja joiden markkinointia ja turvallisuutta valvovat viranomaiset kuten Fimea ja Valvira.

Puettavien älylaitteiden käyttäjät yleensä joutuvat hyväksymään käyttöoikeussopimuksen ennen laitteen käyttöä. Näin ollen tutkimus rajataan sopimuksenalaiseen tiedon keräämiseen, erotuksena tiedosta, jota puettavat laitteet saattavat kerätä ympäristöstään ilman sopimusta tai suostumusta. Tarkastelussa sivutaan kuitenkin myös käyttäjän oikeuksia dataan suhteessa kolmansiin osapuoliin, joihin hänellä ei ole sopimussuhdetta.

Puettavien älylaitteiden keräämä data on valittu tutkimuksen kohteeksi, koska se on yksi tietosuoja-asetuksen arkaluontoisia henkilötietoryhmiä, joiden kerääminen on lähtökohtaisesti tietosuoja-asetuksessa (GDPR) kielletty, mutta jota kuitenkin rutiininomaisesti kerätään yksilöiltä koko ajan esimerkiksi älykellojen kautta sopimus- ja suostumusperusteisesti. Sen voi nähdä olevan yleisimpiä arkaluonteisen datan muotoja, johon yritykset pääsevät hyvin helposti käsiksi suoraan, toisin kuin esimerkiksi genomitieto, jota hallitaan yleensä välioperaattorin, kuten biopankin kautta, joka on ensisijaisesti vastuussa tiedon kohteen tietosuojasta ja anonymisoinnista. Arkaluonteisen datan keräämisessä voi nähdä olevan lähtökohtaisesti suuremmat riskit kuin esimerkiksi auton tietojärjestelmän keräämässä datassa, koska puettava laite on usein kokoaikaisesti käyttäjän vartalolla ja pystyy keräämään käyttäjän terveyteen liittyvää dataa ja johtaa siitä edelleen arkaluonteista informaatiota, jonka lopulliset käyttömahdollisuudet ja -kohteet voivat jäädä tietosuoja-asetuksen suomista oikeuksista huolimatta käyttäjältä piiloon.

Tutkimuksessa tarkastellaan kuluttajien vapaaehtoisesti käyttämiä puettavia laitteita ja niiden dataa, joten ulkopuolelle jäävät myös ammattikäyttöön tarkoitetut laitteet, kuten teollisuuden ja muiden alojen puettavat laitteet, joiden käyttämiseen voidaan sitoutua työsopimuksessa tai joiden käyttöön voidaan muuten velvoittaa. Datan oikeuksien määräytymiseen voi vaikuttaa myös muut sopimussuhteet, kuten urheilijan sopimus seuraansa tai sponsoriinsa.

Datan hallinta Euroopassa on muuttunut tietosuoja-asetuksen voimaantultua 2018. Tämä vaikuttaa kaikkiin EU:n alueen kuluttajiin ja EU:n kansalaisille laitteita ja palveluita tarjoaviin yrityksiin. Tutkimuksessa selvitetään terveysdatan omistajuuden nykytilaa Suomessa ja EU:ssa ja siksi pois rajautuvat muiden oikeusjärjestelmien tulkinnat, muutoin kuin satunnaisten vertailujen osalta.

Tutkimuksessa käytetään tietosuojalain (5.12.2018/1050) käsitteisiin verraten määritelmiä puettavan älylaitteen *käyttäjä* (rekisteröity, datasubjekti) ja *palveluntarjoaja* (rekisterinpitäjä, henkilötietojen käsittelijä). Palveluntarjoajalla tarkoitetaan datan kerääjää, jonka kautta data päätyy ekosysteemiin ja muille datan hyödyntäjille. Useimmiten palveluntarjoaja on sama kuin laitteen valmistaja.

Nykytilanteen kanssa vaihtoehtoisiksi hallintamalleiksi on valittu mahdollinen datan omistusoikeus, koska sitä on nostettu eurooppalaisessa tieteellisessä keskustelussa (e.g. Purtova 2017, Janeček 2018, Trakman 2019, Stepanov 2020) ja ihmiskeskeiset mallit, koska ne ovat sekä kotimaisella poliittisella agendalla (Valtioneuvosto 2018; LVM 2020, 3) että Euroopan komission helmikuussa 2020 julkaistussa Datastrategiassa (EU COM 2020b, 10).

1.5 Tutkimusmenetelmät

Tutkimuksessa yhdistetään lainopillinen kirjallisuustutkimus ja laadullinen haastattelututkimus. Ensimmäisessä osiossa tehdään aiheeseen liittyvä kirjallisuustutkimus ja selvitetään, miten voimassa oleva laki säätelee datan oikeuksien määräytymistä ja miten datan oikeuksien hallinta on tulkittu kirjallisuudessa. Lähteinä käytetään pääasiassa kotimaista ja EU-tasoista lainsäädäntömateriaalia sekä aiheeseen liittyviä tieteellisiä julkaisuja. Aihetta käsitellään sopimusoikeudellisesta, varallisuusoikeudellisesta, immateriaalioikeudellisesta, henkilötietojen suojan näkökulmasta sekä datan hyödyntämisen näkökulmasta. Immateriaalioikeus on osa varallisuusoikeutta, mutta perusteidensa puolesta muusta perinteisestä varallisuusoikeudesta siinä määrin erilainen osa, että se on syytä käsitellä omana lukunaan. Kirjallisuustutkimuksen perusteella arvioidaan terveysdatan oikeuksien jakautuminen nykytilanteessa käyttäjän ja palveluntarjoajan välillä, omistusoikeuden potentiaalia datan hallintamallina sekä kartoitetaan terveysdatan oikeuksien hallinnan haasteita.

Tutkimuksen empiirisessä osioissa haastateltiin kuutta datan oikeuksien hallinnan asiantuntijaa puolistrukturoiduissa teemahaastatteluissa perustuen ensimmäisen osan kirjallisuustutkimukseen. Haastattelut on valittu menetelmäksi, koska datan omistusoikeuksiin liittyvää tieteellistä kirjallisuutta

ja tutkimusta on suomeksi vähän ja haastatteluilla voidaan saada ajankohtaista tietoa datan oikeuksista, joihin liittyvä teknologinen ulottuvuus muuttuu nopeasti. Puolistrukturoitu teemahaastattelu on valittu aineiston keruun menetelmäksi sen joustavuuden takia, ja koska valittavien haastateltavien voidaan asiantuntemuksensa perusteella odottaa tuntevan käsiteltävän teeman aihepiirin ja sen käsitteet (Tuomi & Sarajärvi 2002, 79). Teemaan liittyviä kysymyksiä voidaan näin käsitellä joustavasti haastateltavan erityisasiantuntemuksen aluetta myötäillen.

Haastateltavat on valittu heidän asiantuntemuksensa ja erityisosaamisensa perusteella, pyrkien saamaan mahdollisimman laaja ja kattava kuva eri datan hallinnan erityisalueiden näkökulmista sekä tavoittamaan asiantuntijoiden ajankohtainen ja mahdollisesti *hiljainen* tieto datan oikeuksien nykytilanteesta ja arvioita datan hallinnan tulevaisuudesta. Haastateltavien valinta on tehty osin eliittiotannalla ja osin lumipallo-otannalla. Eliittiotannassa haastateltavat valitaan sen perusteella, keneltä on arvioitu saatavan parhaiten tietoa tutkittavaan aiheeseen ja ilmiöön (Tuomi & Sarajärvi 2002, 88). Lumipallo-otantaa on käytetty valitsemalla asiantuntijoiden itsensä suosittelemia henkilöitä (Tuomi & Sarajärvi 2002, 88). Haastateltavia voidaan pitää asiantuntijataustansa puolesta ns. eliittihaastateltavina, jotka tuntevat aihealueen vähintään osittain haastattelijaa paremmin ja pystyvät näin hahmottamaan käsitteet ja kysymyksenasettelut kriittisesti (Gillham 2005, 54). Tämän vuoksi on perusteltua, että asiantuntijat voivat halutessaan ohjata teemahaastattelussa keskustelua näkemyksensä mukaisesti relevanttiin suuntaan (Gillham 2005, 54). Haastateltavien pienen ja spesifin joukon aiheuttamaa mahdollista tulosten vääristyneisyyden riskiä on pyritty minimoidaan aineistotriangulaatiolla eli vertaamalla haastatteluaineistoa muista lähteistä saatavaan tietoon (Eskola & Suoranta 1999, 69).

1.6 Keskeiset käsitteet ja ilmiöt

1.6.1 Puettava laitteet ja teknologia

Puettaville älylaitteille (engl. *wearables, wearable smart devices*) ei ole yhtä vakiintunutta määritelmää, mutta niitä voidaan kuvailla puettaviksi tietokoneiksi tai älysensoreiksi, jotka ovat yhteydessä verkkoon tietojen vaihtoa varten. Yritykset, asevoimat ja terveydenhuolto ovat käyttäneet laitteita jo pitkään, mutta kuluttajien suosioon ne ovat nousseet vasta viime vuosina. Suosituimpia laitteita kuluttajien keskuudessa ovat tällä hetkellä erilaiset älykellot, hyvinvointimittarit ja aktiivisuusrannekkeet. Korvalla pidettävien puettavien laitteiden ennustetaan lisäävän voimakkaasti suosiotaan tulevina vuosina. (Holst 2020) Puettavat älylaitteet voivat olla myös kypäriä, älylaseja,

kuulokkeita, kenkiä, vaatteita, implantteja, laastareita ja piilolinssejä (UIC). Kauffman ja Soares (2018, 516) listaavat puettavien älylaitteiden määritteleviä ominaisuuksia: ne ovat kiinni käyttäjässä, yksilöllisessä käytössä, käyttäjän mukana liikkuvia, koko ajan mittaavia, ympäristöstään tietoisia sekä tekevät itsenäisesti päätöksiä ja suosituksia keräämiensä tietojen pohjalta.

1.6.2 Kerättävä data

Puettavien älylaitteiden käyttöönotto vaatii useimmiten alkutietojen kuten iän, sukupuolen ja painon merkitsemistä käyttäjäprofiiliin (Jülicher & Delisle 2018, 84). Laite mittaa ja kerää tietoa käyttäjänsä elintavoista ja seuraa elintoimintoja kuten sydämen sykettä ja rytmiä, liikkeitä, hengitystä, lämpötilaa, hikoilua, unen laatua, happisaturaatiota ja kalorien kulutusta (UIC). Näiden arvojen perusteella voidaan tehdä arvioita ja ennusteita esimerkiksi käyttäjän stressistä, diabetesriskistä ja hedelmällisyydestä (Silbert 2019). Tietojen keräämiseen liittyy myös laitteeseen ja sen käyttöön liittyvää *metadataa*, kuten laitteen valmistaja, mallin ja sarjanumeron sekä internetyhteyden tiedot (Julicher & Delisle 2018, 84). Tässä tutkimuksessa käytetään käsitettä terveysdata tarkoittamaan kaikkea puettavan älylaitteen keräämää tietoa, joka liittyy käyttäjän terveyteen ja fysiologiaan.

Puhuttaessa puettavan älylaitteen käyttäjän datasta ja käyttöoikeudesta siihen, on tärkeää määritellä myös *henkilötieto* käsitteenä. EU:n tietosuoja-asetus (GDPR) muutti Suomenkin lakia henkilötietojen määrittelyn ja hallinnan osalta. Sen mukaan henkilötietoja ovat tiedot, joiden perusteella luonnollinen henkilö voidaan tunnistaa suoraan tai välillisesti esimerkiksi yhdistelemällä tietoja, jotka johtavat tunnistamiseen (GDPR johdanto-osa 26). Puettavan laitteen käyttäjälle tällaisia ovat esimerkiksi nimi, sijantitiedot tai muut käyttäjälle tunnusomaiset fyysiset, fysiologiset, geneettiset, psyykkiset tai sosiaaliset tekijät (GDPR 4 artikla 1). Tunnistettavuuden määrittelyssä tulisi ottaa huomioon kaikki keinot, joita rekisterinpitäjä tai muu henkilö voisi *kohtuullisen todennäköisesti* käyttää henkilön tunnistamiseen (GDPR johdanto-osa 26). Asetuksessa huomautetaan, että suoja ei ole absoluuttinen ja että sitä tulisi soveltaa suhteellisuusperiaatteen mukaisesti huomioiden henkilötietojen suojan suhde muuhun yhteiskuntaan ja muihin perusoikeuksiin (GDPR johdanto-osa 4).

Tämän perustella voidaan tulkita kaiken käyttäjää koskevan tiedon puettavalla älylaitteella olevan henkilötietoa, koska niin palveluntarjoaja rekisteripitäjänä kuin kuka tahansa laitteella kerättyyn dataan käsiksi pääsevä henkilö voisi tunnistaa käyttäjän jo pelkästään monien käyttöehtosopimusten vaatimilla aidoilla henkilötiedoilla (Paul & Irvine 2014, 5). Myös laitteeseen ja verkkoyhteyteen

liittyvä metadata on henkilötietoa, koska sillä on yhteys käyttäjään ja sen kautta on mahdollista tunnistaa käyttäjä (Julicher & Delisle 2018, 84). Käyttäjän terveyttä koskeva tieto on *arkaluonteista* tietoa eli yksi *erityisistä henkilötietoryhmistä*, jonka käsittely on lähtökohtaisesti kiellettyä ja vaatii erityiset olosuhteet, tässä tapauksessa yleensä käyttäjän nimenomaisen suostumuksen (GDPR 9 artikla). Tietosuoja-asetuksen (GDPR johdanto-osa 15) määritelmän mukaan terveystietoja ovat ”*luonnollisen henkilön fyysiseen tai psyykkiseen terveyteen liittyvät henkilötiedot, mukaan lukien tiedot terveyspalvelujen tarjoamisesta, jotka ilmaisevat hänen terveydentilansa*”. Asetuksessa (GDPR johdanto-osa 35) myöhemmin vielä määritellään suoja kattamaan niin entiset, nykyiset kuin tulevatkin fyysiseen ja henkiseen terveyteen liittyvät tiedot, jotka on saatu *”kehon osan tai kehosta peräisin olevan aineen testaamisesta tai tutkimisesta […], kuten geneettiset tiedot ja biologiset näytteet, sekä kaikki tiedot esimerkiksi sairauksista, vammoista, sairauden riskistä, esitiedoista tai annetuista hoidoista sekä tieto rekisteröidyn fyysisestä tai lääketieteellisestä tilanteesta*”, riippumatta siitä mistä tiedot ovat peräisin. Tämä kattaa myös puettavalla laitteella kerätyn datan.

Toisaalta tietosuoja-asetus ei koske anonyymiä, anonymisoitua tai pseudonymisoitua tietoa. Anonymisointi tarkoittaa tarkoittaa, että henkilötietoa on käsitelty niin, että yksilöä ei voida enää tunnistaa. Pseudonymisointi tarkoittaa tietojen käsittelyä niin, että tunnistaminen on mahdollista vain lisätietojen avulla. (GDPR johdanto-osa 26) Useat asiantuntijat ovat esittäneet epäilyjä onko tietojen tehokas anonymisointi edes mahdollista, esimerkiksi Koronacki et al. (2010, 49) varoittavat, että tällä hetkellä anonyymi tieto voidaan mahdollisesti tulevaisuudessa palauttaa tunnistettavaan muotoon uusista lähteistä saatavalla tiedolla. Tämä korostaa tarvetta määritellä tiedon omistajuus kestävällä ja oikeudenmukaisella tavalla eri osapuolten kannalta.

1.6.3 IoT

IoT, Internet of Things eli suomeksi *esineiden internet* on järjestelmä, missä arkipäiväiset esineet kuten jääkaapit ja televisiot ovat yhteydessä internetiin, keräävät tietoa ympäristöstään ja kommunikoivat keskenään. Esineitä voidaan etähallita käyttöliittymän tai toisen älylaitteen kautta ja ne ovat usein yksilöllisesti tunnistettavia ja paikannettavia. (Mattern & Floerkemeier 2010, 242, 244) Yhteys internetiin tuo palveluntarjoajan ulottuville valtavan määrän mahdollisuuksia käyttää, tehostaa ja kehittää palvelua laitteen keräämän datan pohjalta sekä käyttäjille mahdollisuuden hyötyä datan sovelluksista. Esineiden etähallinnalla voidaan tehostaa terveydenhuoltoa ja hoivapalveluita, optimoida kodin laitteiden käyttöä ja turvallisuutta sekä edistää niin yhteiskunnan, ympäristön kuin

yritystenkin resurssien optimaalista ja turvallista käyttöä. (McKean 2014, 167-168) Puettava teknologia ja älylaitteet ovat osa esineiden internetiä.

1.6.4 Big Data

Big data eli massadata tarkoittaa suurta määrää tietoa, jota *esineiden internetin* laitteet keräävät, analysoivat ja tallentavat koko ajan. Yritykset ja muut organisaatiot hyödyntävät dataa esimerkiksi asiakkaiden käyttäytymisen analysoinnissa ja pyrkivät saamaan kilpailuetua sekä tehostamaan toimintojaan big datasta johdetulla ymmärryksellä. (Poikola et al. 2018, 61;73) Big Dataa kuvataan usein 3V:n mallilla, jossa kirjaimet tarkoittavat *volyymia* (volume), *vauhtia* (velocity) ja *variaatiota* (variety). *Volyymi* viittaa datan eksponentiaalisesti kasvavaan määrään ja *vauhti* datan kerääntymisen kiihtyvään nopeuteen ja haasteisiin, joita datamassan käsittely ja tehokas hyödyntäminen aiheuttaa käytännössä. *Variaatio* tarkoittaa datan lähteiden ja datan tyyppien kasvavaa ja koko ajan monipuolistuvaa määrää. Data ei ole sinällään eikä kenen tahansa käytössä arvokasta vaan sen arvo syntyy sen muokkaamisessa ja analysoinnissa sekä oikeassa sovelluskohteessa ja oikean hyödyntäjän hallussa. (Alanko & Salo 2013, 3-4)

1.6.5 Ekosysteemi

Esineiden internetin *ekosysteemi* viittaa laitteisiin ja palveluihin liittyviin koko toimijoiden joukkoon, kuten laitteen, ohjelmiston ja sensorien valmistajat sekä data-analytiikkayritykset, muut palveluntuottajat ja loppukäyttäjät (EU COM 2016, 22). Kokonaisuuden toimimiseksi käyttäjän dataa jaetaan ekosysteemin eri toimijoille ja vastaavasti käyttäjä voi käyttää GDPR:n antamia oikeuksiaan kaikkia hänen dataansa käsitelleitä kohtaan (Kauffman & Soares 2018, 530).

1.6.6 Quantified Self -ilmiö

Quantified Self eli *itsensä mittaaminen* on Kaliforniasta, Yhdysvalloista 2000-luvulla lähtenyt liike ja ilmiö, jossa mitataan omaa kehoa, sen toimintoja ja suorituskykyä pyrkimyksenä lisätä ymmärrystä oman kehon toiminnasta ja elintapojen vaikutuksista siihen sekä optimoida omaa terveydentilaa mitatun tiedon avulla (Kurppa 2017). Quantified Self -käsitteen toi julkiseen keskusteluun Wired-lehden toimittaja vuonna 2007. Puettavilla mittareilla voidaan mitata, optimoida ja verrata muihin omaa terveyttä ja tehokkuutta (Benvie 2013, 280). Mittaamisen kautta voi myös ennakoida tulevia ongelmia ja hakea motivaatiota muutoksiin (Kurppa 2017). Laitteilla mitataan unta ja sen laatua, mielialaa, fyysistä kuntoa, ravintoa ja sen laatua sekä henkistä suorituskykyä (Benvie 2013, 281-283).

Biohacking eli *biohakkerointi* on osa samaa ilmiötä, mutta biohakkerit menevät vielä pidemmälle kokeillessaan erilaisia uusia tieteellisiä tai perinteisiä vanhoja, terveyttä väitetysti edistäviä, menetelmiä. Sekä itsensä mittaaminen että biohakkerointi voidaan nähdä osana terveydenhuollon muutosta, jossa lääketieteelliset laitteet tulevan teknologisen kehityksen ja halpenemisen myötä yhä useamman saataville. Kuluttaja voi näin seurata, mitata ja edistää omaa terveyttään itsenäisesti. (Kurppa 2017) Quantified Self -ilmiössä sanotaan näkyvän individualistinen ihmiskäsitys ja ajatus siitä, että yksilön terveys on suoraa seuraus hänen omista valinnoistaan ja elämäntavoistaan (Venhe 2020).

1.6.7 Dataetiikka

Dataetiikka on etiikan suhteellisen uusi osa-alue, joka tutkii ja arvioi dataan liittyviä moraalisia ongelmia kuten sen keräämisen, jakamisen ja hyödyntämisen oikeutusta sekä algoritmeihin ja tekoälyyn liittyviä käytäntöjä ja niiden vastuullisuutta. Data-etiikan tavoitteena on luoda moraalisesti kestäviä ratkaisuja perusteltujen käytäntöjen ja arvojen pohjalta. (Floridi & Taddeo 2016, 1) Erityisesti big dataan liittyvää etiikkaa (Big Data Ethics) on käsitelty ja tutkittu viime vuosina paljon. Big Dataan liittyviä moraalisia ongelmia ovat esimerkiksi datan kerääjän mahdollisuus kerätä dataan kohteen tietämättä, yksilön identifiointi anonyymistä tiedosta sekä big datan käyttö yksilöön vaikuttamiseen ja manipulointiin. (Herschel & Miori 2017, 1-2)

1.6.8 MyData

MyData on käyttäjäkeskeinen lähestymistapa henkilötietojen käsittelyyn, jossa halutaan parantaa yksilön oikeuksia oman henkilötietonsa keräämisessä ja hyödyntämisessä. MyData on kansainvälinen ilmiö, joka lähti Suomessa kehittymään näkyvämmin vuonna 2014 tehdystä liikenne- ja viestintäministeriön selvityksestä, jossa haluttiin luoda suuntaviivat ihmiskeskeisen datatalouden pohjaksi. (Kailio 2018) MyData Global on liikettä edustava kansainvälinen yleishyödyllinen organisaatio, joka on perustettu ajamaan liikkeen ideaa yksilön itsemääräämisoikeudesta omien henkilötietojensa käyttöön ja hallintaan. Omadata-liike arvostelee teknologiajättien tapaa vaatia käyttöoikeutta käyttäjän tietoihin palvelun käyttöä vastaan. MyDatan tavoitteena on varmistaa, että palvelujen käyttöehdot ovat käyttäjille tarpeeksi selkeitä ja ymmärrettäviä. (Hukkanen 2018) Omadata-liike haluaa yhdistää datan optimaalisen hyödyntämisen mahdollisimman korkeaan yksityisyydensuojaan (Poikola 2020).

Valtio ja viranomaiset ovat olleet mukana kehittämässä ja edistämässä Omadataa ilmiönä ja se on ollut osana kahden viimeisen hallituksen hallitusohjelmaa (Erkinheimo 2019). Monet suomalaiset ja kansainväliset yritykset sekä organisaatiot kuten Posti, Yle, VTT, Futurice ja Demos Helsinki ovat jäseninä MyData Global-organisaatiossa (MyData 2018). Tietosuojavaltuutettu on puoltanut MyDataa periaatteena terveyssovellusten suunnittelussa (Aarnio 2020). Teknologioita ja datan ekosysteemejä, joissa johtoajatuksena on MyDatan tai vastaavien käyttäjäkeskeisten liikkeiden periaatteet, kutsutaan nimellä PIMS eli *personal information management systems* (EDPS 2016, 3).

1.6.9 IHAN-hanke

IHAN-hanke on Sitran (Suomen itsenäisyyden juhlarahasto) vetämä projekti, jossa pyritään rakentamaan ”*reilun datatalouden perustuksia ja luodaan valtioiden rajat ylittävät pelisäännöt ja ratkaisut datan jakamiseen ja hyödyntämiseen*”. Hankkeen tavoitteena on saada ihmiskeskeinen datan hyödyntäminen Euroopan tasoiseksi standardiksi, jossa edistetään samanaikaisesti niin käyttäjien hallintaa omaan dataansa kuin sen tehokasta hyödyntämistäkin. Sitran julkaisemassa, päivittyvässä IHAN-blueprint-dokumentissa määritellään reilun datatalouden vaatimuksia dataa käyttävälle ekosysteemille (Sitra 2020) Eurooppalainen standardisointijärjestö (European Committee for Standardization) julkaisi IHAN-hankkeen määrittelyt reilulle datataloudelle keväällä 2020 omana asiakirjanaan, mitä pidetään ensimmäisenä askeleena viralliselle standardille (Suomalainen 2020). IHAN-hankkeeseen sisältyy reilun datatalouden periaatteisiin nojaavia, henkilötiedon käyttöön perustuvia pilottihankkeita, kuten varusmiesten vapaaehtoinen liikunta- ja hyvinvointidatan hyödyntäminen kuntotalkoissa. Hankkeesta saatuja kokemuksia ja testattua mallia pyritään soveltamaan hyvinvointidatan hyödyntämiseen muillakin aloilla kuten terveydenhuollossa ja työhyvinvoinnissa. (Suomalainen 2019)

Seuraavissa luvuissa käydään läpi puettavilla laitteilla kerätyn terveysdatan hallinnan nykytila sekä mahdollisuudet ja kehykset datan oikeuksien hallitsemiseksi omistusoikeudella. Datan oikeuksia käydään läpi sopimusoikeuden, varallisuusoikeuden – erityisesti immateriaalioikeuden – sekä henkilötietojen suojan näkökulmasta. Luvussa käydään läpi terveysdatan erityispiirteitä hallinnan kohteena sekä näiden erityispiirteiden tuomia haasteita datan oikeuksien määrittelylle.

2 Sopimusoikeudellinen näkökulma

2.1 Käyttöehtosopimus

Puettavien älylaitteiden markkinoita ja datan keräämistä säätelevä lainsäädäntö pohjautuu tällä hetkellä toisistaan irrallisiin säädöksiin kuten tietosuoja-asetukseen (GDPR) ja sopimusoikeuteen (OikTL, Laki varallisuusoikeudellisista oikeustoimista 13.6.1929/228) joten kokonaiskuva ja normien soveltuvuus on epäselvää. Lainsäädännön hajanaisuus on antanut yrityksille mahdollisuuden luoda itse omat sääntönsä ja datan hallinta perustuu tällä hetkellä yritysten itse laatimien vakioehtoisiin sopimuksiin. (Tarkela 2016, 71) Sopimukset ovatkin tällä hetkellä yleisin tapa säännellä dataa älylaitteiden maailmassa (Kauffman & Soares 2018, 526). Itsenäisyys sopimusten laatimisessa mahdollistaa yritysten luoda itselleen mahdollisimman edulliset ja joustavat oikeudet käyttäjän dataan ja sen hyödyntämiseen (Tarkela 2016, 71). Yritykset pyrkivät maksimoimaan sopimusten kattamat oikeudet itselleen, vaikka ne eivät olisi perusteltuja tai todellisuudessa toimeenpantavissa (Banerjee et al. 2018, 54).

Alkaessaan käyttämään puettavaa älylaitetta, käyttäjä joutuu yleensä hyväksymään käyttöoikeus- eli lisenssisopimuksen. Käsitteet lisenssi, lisenssisopimus ja käyttöoikeussopimus tarkoittavat käytännössä samaa asiaa ja lisenssiä voidaan kutsua myös hyödyntämisoikeudeksi tietoon (Takki & Halonen 2017, 198;62). Puettavan älylaitteen palveluntarjoajan on varmistuttava käyttöehtosopimuksella siitä, että käyttäjästä kerättävä data on sopimuksenalaista ja palveluntarjoaja saa datan hyödyntämiseen mahdollisimman laajan luvan (Tarkela 2016, 71). Toisaalta tietosuoja-asetuksen käyttäjälle tuoma oikeus *tulla unohdetuksi* voidaan nähdä rajaavan tätä lupaa ja luovan käytännössä tilanteen, jossa *käyttäjä* antaa *palveluntarjoajalle* käyttöoikeuden omiin tietoihinsa ja samalla pidättää oikeuden lopettaa tämä käyttöoikeus (Kauffman & Soares 2018, 531). Kuitenkin datan muokkaaminen kuten anonymisointi ja analysointi vähentävät GDPR:n tuomien oikeuksien, kuten unohdetuksi tulemisen oikeuden merkitystä (Kauffman & Soares 2018, 531). Oikeuksilla ei ole enää käytännön merkitystä sen jälkeen, kun dataa on hyödynnetty yksilön profilointiin ja jaettu ekosysteemissä (Kauffman & Soares 2018, 531).

Tai (2018, 9) huomauttaa artikkelissaan datan omistajuudesta ja kuluttajansuojasta, että vaikka käyttöoikeussopimuksissa kuluttajille vakuutetaan heidän omistavan oman tietonsa, todellisuudessa käyttöoikeus on palvelun tarjoajalla, jolla on sopimuksen mukaan pysyvä käyttöoikeus kuluttajan tietoihin ja oikeus hyödyntää niitä taloudellisesti. Vaikka käyttäjällä olisi omistusoikeus

henkilötietoihinsa, häntä koskevaa tietoa on muokkaamisen jälkeen mahdotonta poistaa tai vaatia poistamaan tietokannasta (Tai 2018, 9). Kauffman ja Soares (2018, 532) katsovat, että vaikka GDPR:n tarkoitus ja oikeudet suunnattiin suojaamaan yksilön henkilötietoja ja oikeuksien on nähty muodostavan jopa omistusoikeuksien kaltaista *näennäisomaisuutta* (Purtova 2017, 66) käyttäjälle*,* käytännössä se on kuitenkin johtanut yksilön oikeuksien heikkenemiseen.

Käyttöehtosopimuksella perusteella palveluntarjoaja antaa käyttöoikeuden palveluun ja saa samalla oikeuden hyödyntää käyttäjän henkilö- ja muuta tietoa. Monien muiden tietoa keräävien palveluiden kuten Facebookin tai Twitterin käytöstä poiketen, puettavan teknologian käyttäjä maksaa fyysisestä tuotteesta eli älylaitteesta. On epäselvää maksaako käyttäjä samalla myös itse ohjelman eli esimerkiksi hyvinvointisovelluksen ja siihen liittyvien palvelujen käytöstä vai maksaako hän itse palvelun käytöstä omilla *henkilötiedoillaan.*

Uudessa digitaalisen sisällön direktiivissä (Euroopan parlamentin ja neuvoston direktiivi tietyistä digitaalisen sisällön ja digitaalisten palvelujen toimittamista koskeviin sopimuksiin liittyvistä seikoista, 2019/770) tunnustetaan sopimusperusteinen tietojen luovuttaminen vaihtoehtoiseksi tavaksi maksaa palvelusta (johdanto-osa kohta 24). Direktiivissä asetetaan palvelusta kauppahinnan maksanut joissain tilanteissa eri asemaan kuin käyttäjä, joka on maksanut luovuttamalla tietojaan, koska hinnanalennus ei luonnollisesti jälkimmäisessä tilanteessa onnistu. Näin tietojaan luovuttanut voi esimerkiksi purkaa sopimuksen jo vähäisen virheen johdosta (johdanto-osa kohta 67), toisin kuin kauppahinnan maksanut.

Direktiivissä huomautetaan, että henkilötietojen suoja on silti perusoikeus eikä henkilötietoja voida pitää hyödykkeenä. (johdanto-osa kohta 24) Kuitenkin esimerkiksi Malgieri & Custersin (2018, 291) mielestä henkilötiedot ovat EU:n lainsäädännössä koko ajan enemmän kaupallistettavia varallisuuden kohteita. Heidän mukaansa palveluntarjoajien pitäisi jo nykylainsäädännön puitteissa ilmoittaa käyttäjälle jos ja kun hän saa tuotteita tai palveluja vastapalveluksena omien henkilötietojensa luovuttamisesta (Malgieri & Custers 2018, 302). He katsovat, että informaatiovelvollisuus pitäisi kuitenkin lisätä virallisesti tietosuoja-asetukseen, jotta käyttäjät olisivat tietoisempia henkilötietojensa käyttämisestä vaihdannan kohteina ja niiden taloudellisesta arvosta.

Jos henkilötietojen luovuttamisella voi kuitenkin tietyssä mielessä ”maksaa” palvelusta, onko puettavan älylaitteen käyttäjä maksanut palvelusta ostaessaan laitetta vai onko laitteen hinta valmistuskustannuksiin nähden halpa, koska valmistaja tai palveluntarjoaja tietää saavansa arvokasta

dataa ”kaupan päälle”? Pitäisikö valmistajan ja palveluntarjoajan tarjota myös kalliimpaa palvelupakettia, jonka kautta henkilötietoja ei voisi hyödyntää edes anonymisoituina? Koska laitteen käytön aloittaminen vaatii käyttöehtosopimuksen hyväksymisen, käyttäjälle jää mahdollisuuksiksi vain antaa suostumus henkilötietojensa käyttöön tai olla ottamatta laitetta käyttöön.

Henkilötietojen luovutus maksuna palvelusta henkilötiedoillaan ei kuitenkaan ole tietosuoja-asetuksen vaatima *vapaaehtoinen* suostumus henkilötietojen käytölle, jos palvelun saaminen riippuu suostumuksen antamisesta (Malgieri & Custers 2018, 291). Tietosuoja-asetuksessa mainittu vaatimus henkilötietojen käsittelyn minimoinnista (GDPR 2 luku 5 artikla) estää palveluntarjoajia laittamasta palvelun kannalta epäolennaisten henkilötietojen luovuttamista ehdoksi palvelun tarjoamiselle (Malgieri & Custers 2018, 291).

2.2 Käyttäjän kuluttajansuoja

Tässä tutkimuksessa käsiteltävät kuluttajien käyttämät puettavat älylaitteet ja niihin liittyvät palvelut hankitaan yksityiskäyttöön ja luonnollisille henkilöille ja ovat siten kuluttajansuojalain (KSL 38/1978) alaisia. Laki suojaa kuluttajaa sopimuksen heikompana osapuolena. Tämä tuo pakottavaa sääntelyä, josta ei voi sopimuksella poiketa kuluttajan vahingoksi. Käyttöehtosopimukseen voitaisiin näin soveltaa esimerkiksi kohtuuttomien ehtojen kieltoa (KSL 3 luku, 1 §), epäselvän ehdon tulkintaa kuluttajan eduksi kun sopimus laadittu ilman kuluttajan myötävaikutusta (KSL 4 luku, 3 §) ja EU:n ulkopuolisen valtion lainvalinnan syrjäyttämistä kun viittaus olisi kuluttajan vahingoksi (KSL 5 luku, 5 §). Kuluttajan on kuitenkin vaikea arvioida ehtojen kohtuullisuutta kun datan käsittely, prosessointi ja siirtyminen kolmansille sen keräämisen jälkeen ei ole läpinäkyvää (Tarkela 2016, 72).

Kuluttajan täytyy pystyä myös käytännössä tutustumaan ehtoihin, eikä kuluttaja-asiakas voi tehokkaasti sitoutua sopimukseen pelkällä palvelun käyttöönotolla, vaan vakiomuotoiset ehdot on aktiivisesti hyväksyttävä. Käyttäjällä on myös oikeus nostaa kanne palveluntarjoajaa vastaan ja ehdoista riippumatta käydä oikeutta paikallisessa alioikeudessaan. (Honkinen et al. 2016, 7.2.2) Massalisensoinnissa on yleistä, että käyttäjä sitoutuu ehtoihin avaamalla pakkauksen (shrink-wrap) tai hyväksymällä ehdot klikkauksella (click-wrap). Suomessa ja muissa Pohjoismaissa tällaisiin sopimusehtoihin on suhtauduttu varauksellisesti, ja sitoakseen kuluttajaa ne eivät ainakaan saa sisältää *yllättäviä* tai *ankaria* ehtoja. (Harenko et al. 2016, 107).

2.3 Sitoutuminen sopimukseen ja suostumus

Yrityksen intressi dataan riippuu siitä, onko se liiketoiminnan kannalta keskeinen resurssi. Puettavan teknologian palveluntarjoajalle ja samalla koko ekosysteemille data on arvokas resurssi, jonka hallinta ja hyödyntämismahdollisuus on elintärkeää ja sopimustekniikkaan voi tämän vuoksi ajatella panostettavan tavallista enemmän. Tämän johdosta käyttöehtosopimukseen sitoutuneen kuluttajan voi arvioida olevan erityisen heikko osapuoli sopimustasapainon kannalta.

Tietosuoja-asetuksen (GDPR) 4 artiklan kohdassa 11 on määritelty, että suostumuksen henkilötietojen käyttöön olisi oltava *vapaaehtoinen*, *yksilöity*, *tietoinen* ja *yksiselitteinen*. Suostumuksesta on kuitenkin väitetty tulleen käytännössä pelkkä sisällötön rituaali ilman käytännön merkitystä (Sankari & Wiberg 2019, 345-346). On kyseenalaista voiko käyttäjän odottaa perehtyvän monikymmensivuisiin käyttöehtoihin ja tekevän aidosti *tietoisen* päätöksen antaessaan suostumuksen henkilötietojensa käyttöön ja toteuttavatko monimutkaiset ja vaikeaselkoiset ehdot GDPR:n vaatimuksia tietojen *läpinäkyvyydestä, käyttötarkoitussidonnaisuudesta* ja *tietojen keräämisen minimoinnista* (GDPR 2 luku artikla 5 a; b; c) (Jülicher & Delisle 2018, 86). Tietojen keräämisen minimointi tarkoittaa käytännössä sitä, että palveluntarjoaja ei saa kerätä käyttäjästä dataa, mikä ei ole *olennaista ja tarpeellista* suhteessa palvelun toteuttamiseen (GDPR 2 luku 5 artikla c). Tämä tarkoittaa käänteisesti sitä, että kaikkeen palvelun tai tuotteen tarjoamisen kannalta *ei-olennaisen* ja *ei-tarpeellisen* datan keräämiseen ja käyttöön pitää pyytää käyttäjältä suostumus ja datan käyttötavat pitää kertoa selkeästi käyttäjälle.

Uusi digitaalisen sisällön direktiivi muuttaa tilannetta siltä osin, että jos käyttäjä on ”maksanut” jostain palvelusta antamalla vaihdannassa henkilötietojaan, hänestä voidaan kerätä myös muita kuin palvelun kannalta kuin välttämättömiä tietoja (Malgieri & Custers 2018, 293). Käyttäjän on vaikeaa ellei mahdotonta arvioida mikä on välttämätöntä dataa. Asia jää siis käytännössä palveluntarjoajan harkinnan varaan. Myös Purtova (2017, 72) on arvostellut suostumusta ja sen roolia tietosuojakäytännöissä. Hänen mukaansa on kohtuutonta odottaa käyttäjän lukevan ja ymmärtävän kaiken ehdoissa kerrotun ja suostumuksen todelliset vaikutukset käytännössä omien henkilötietojensa hyödyntämisessä.

Euroopan komission selvityksessä (EU COM 2018, 366-367) datan omistusoikeudesta käsitellään erikseen puettavien älylaitteiden keräämää dataa ja sen hyödyntämistä. Sen perusteella osa palveluntarjoajista myy kerättyä terveysdataa käyttäjän antaman alkuperäisen suostumuksen

perusteella kolmansille osapuolille kuten tutkimukseen ja vakuutusyhtiöille. Selvityksessä korostetaan käyttöehtojen läpinäkyvyyden ja selkeyden tärkeyttä käyttäjän etujen suojelemiseksi.

3 Varallisuusoikeudellinen näkökulma

3.1 Argumentteja omistusoikeudesta – puolesta ja vastaan

Siinä missä sopimusoikeus joustaa melko helposti reaalimaailman muutoksiin ja sopimusosapuolten tarkoituksiin, varallisuusoikeuteen on perinteisesti ollut vaikea tuoda uusia omaisuusryhmiä (van Erp 2017, 256). Varallisuusoikeutta ei ole EU:n tasolla harmonisoitu ja eri maiden kansallisten lakien erityispiirteet heijastuvat näin myös datan omistusoikeuden määrittelyyn, kun data kuitenkin liikkuu vapaasti rajojen yli. Kansallisissa oikeusistuimissa on jo jouduttu ottamaan kantaa esimerkiksi siihen, onko data vahingonkorvauslain perusteella *oikeushyvä* ja voiko sitä käyttää panttauksen kohteena. (Kauffman & Soares 2018, 522-523) Ottaen huomioon datan merkityksen digitaalitalouden resurssina, dataan liittyvien konfliktien ja paineen sen oikeudellisesta määrittelystä voi odottaa vain lisääntyvän.

Datan omistusoikeudesta käydään koko ajan keskustelua puolesta ja vastaan. EU:n lainsäädännössä ei tunnusteta omistusoikeutta dataan ja suurin osa tutkijoista ja asiantuntijoista suhtautuu omistusoikeuteen varauksella muun muassa tiedon datan ihmisoikeuskytköksen ja vapaan liikkuvuuden periaatteen perusteella (Janeček 2018, 1040-1043). On väitetty, lähinnä yritysmaailman näkökulmasta, että eksklusiiviset oikeudet dataan aiheuttaisivat häiriötä nykyisellä toimivalla markkinalla rajoittamalla yritysten toimintaa ja luomalla kilpailua haittaavia rakenteita (Drexl et al. 2016, 2-3). Toisaalta koko keskustelun datan omistusoikeudesta voi katsoa lähteneen saksalaisen autoteollisuuden tarpeesta määritellä autojen keräämän, arvokkaan datan oikeuksien hallinta (Hugenholtz 2017, 65). Yritysten näkökulmasta tärkeä aineeton omaisuus, kuten profilointialgoritmit, on kuitenkin suojattu liikesalaisuuksina, joten välitöntä tarvetta datan omistusoikeuden sääntelylle yleisesti ei ole (Malgieri & Custers 2018, 289). Datan omistusoikeuksien määrittelemättömyyden pelätään kuitenkin hidastavan ja haittaavan EU:n digitaalisen talouden kasvua ja kehitystä kokonaisuutena (Stepanov 2019, 3). On esitetty, että yksilöiden ja yhteiskunnan etu vaatii omistusoikeuden määrittelemistä laissa jo dataan liittyvän suuren taloudellisen arvon ja sen oikeudenmukaisemman jakautumisen vuoksi (Purtova 2017, 77). Datan omistusoikeuden säätämisen on esitetty lisäävän yksilön mahdollisuutta hallita omia henkilötietojaan ja yksilönsuojaansa sekä rajaavan datan kerääjien ”*de facto omistusoikeuden kaltaista hallintaa*” yksilön henkilötietoihin (Purtova 2017, 77).

Tärkeimpiä argumentteja datan omistusoikeudelle ovat markkinoiden epäonnistuminen ja datan hyödyntämisen ulkoisvaikutukset yhteiskunnan ja yksilön näkökulmasta. Datatalouden kehitys perustuu keskittymiselle, tehostamiselle ja työvoiman tarpeen vähenemiselle, mikä voi johtaa dataan liittyvän arvon epätasaiseen jakautumiseen ja tuloerojen kasvuun. Ilmiötä on vaikea hallita yhteiskunnallisesti verotuksen kautta, koska datan luoma arvo ei välttämättä näy taseessa. (Tarkela 2016, 73) Yhteiskunnallisesta ja kilpailuoikeudellisesta näkökulmasta on myös huolestuttavaa, että suuret yritykset kuten Google hallitsevat datan markkinaa ja monopolisoivat dataa muiden osapuolten, kuten käyttäjien ja pienempien yritysten kustannuksella (Purtova 2017, 71). Datan markkinoilla on ensimmäisen tai ensimmäisten toimijoiden etu, eli jos yritys saa suuren markkinaosuuden tai määrävään markkina-aseman, se on toimijalle merkittävä vahvuus ja se pystyy siitä koituvilla eduilla sen usein myös pitkäaikaisesti säilyttämään (Kuoppamäki 2018, 271). Suurilla toimijoilla on siis mahdollisuus estää pienempien markkinoille tulo hallitsemallaan suurella tietomäärällä, jonka perusteella he voivat hyötyä paitsi käyttäjistä myös dataa tarvitsevista pienemmistä yrityksistä, joita molempia ryhmiä suuri toimija voi hyväksikäyttää omien, ylivoimaisten algoritmiensa kehityksessä (Kuoppamäki 2018, 271).

Globaalin digitalouden vuoksi keskustelu datan omistusoikeudesta on myös osa geopolitiikkaa (Singh &Vipra, 54). Euroopan viimeaikaisten datan oikeuksiin liittyvien lakihankkeiden taustalla on sanottu olevan pelko eurooppalaisten toimijoiden jäämisestä yhdysvaltalaisten yritysten armoille, sekä yritys parantaa oman alueen yritysten markkinavoimaa näitä kohtaan (Hugenholtz 2017, 65). On väitetty, että Yhdysvallat yrittää ajaa vapaakauppasopimuksilla datan vapaata liikkuvuutta ja estää keskustelua datan omistusoikeuksista, koska se kyseenalaistaisi yhdysvaltalaisten yritysten vapaan ja itsevaltaisen toiminnan datan markkinoilla (Singh & Vipra 2019, 54). Ilman selvää viitekehystä datan taloudelliselle hyödyntämiselle datan oikeudet ovat käytännössä sen kerääjällä, ja myös EU ja sen kansalaiset uhkaavat jäädä Kiinan ja Yhdysvaltojen suurien digiyritysten vapaasti hyödynnettäväksi resurssiksi (Singh & Vipra 2019, 54-55).

Datan kerääjä pystyy kontrolloimaan datan jalostusta ja keräämään siitä tulevan hyödyn. Datan omistusoikeuden määrittelyn puolesta puhuu siihen sisältyvän taloudellisen arvon lisäksi myös sen potentiaali *yhteiskunnallisen vallan välineenä.* (Tarkela 2016, 69) Henkilöistä kerätyn taustadatan avulla voidaan vaikuttaa ja manipuloida yksilöitä ja ryhmiä (Singh & Vipra 2019, 55). Tämän voi huomata esimerkiksi taannoisesta Cambridge Analytica-skandaalista, jossa sosiaalisesta mediasta saaduilla tiedoilla pystyttiin vaikuttamaan äänestäjiin ja vaalien lopputuloksiin (Isaak & Hanna

2018), 2). Datalla ja sen keräämisellä voi myös ottaa kantaa mitkä asiat ovat tarkastelun arvoisia ja ohjata yhteiskunnallista keskustelua. (Tarkela 2016, 69)

Thouvenin et al. (2017, 136-137) kuitenkin katsovat, että markkinat eivät ole laajassa mittakaavassa epäonnistuneet ja varoittavat tekemästä laaja-alaisia ratkaisuja, jotka toisivat uusia ongelmia, vaan heidän mielestään pitäisi keskittyä tekemään täsmäsääntelyä havaittuihin ongelmiin. Myös Drexl (2018, 2) katsoo, että dataan ei pitäisi säätää omistusoikeutta, vaan pelkästään alakohtaisia datan käyttöoikeuksia.

Tietosuoja-asetuksen voimaantulon jälkeen voi huomata EU:n lainsäädännön keskittyneen enemmän datan omistusoikeuteen vapaan liikkuvuuden välineenä kuin dataan liittyvien oikeuksien suojaamiseen tai määrittelyyn (Tai 2018, 10). Euroopan komission selvityksen (EU COM 2018, 78) mukaan datan omistusoikeuden määrittelemättömyys aiheuttaa suurimmalle osalle yrityksistä epävarmuutta datan käytöstä ja nostaa kynnystä jakaa dataa muille yrityksille, mikä hidastaa eurooppalaisen datatalouden kehitystä. Yrityksille keskeinen tavoite ei kuitenkaan ole omistusoikeus, vaan pääsy dataan ja oikeus käyttää sitä (EU COM 2018, 224). Näiden lisäksi datan kopiointi on nähty tärkeänä dataan liittyvänä oikeutena (Thouvenin et al. 2017, 137).

Yritysten välisten suhteiden näkökulmasta datan hallinnointi sopimusehtojen kautta on edullisempi vaihtoehto, koska sopimusrikkomukselle on matalampi todistuskynnys kuin aineettomien oikeuksien loukkaukselle (Kauffman & Soares 2018, 526). Toisaalta ekosysteemin erilaisten ristikkäisten sopimusten hierarkia tekee kokonaishahmottamisen vaikeaksi ja pakottava lainsäädäntö sopimusehdot alisteiseksi (Kauffman & Soares 2018, 526). Tämän perusteella voi yhteenvetona todeta, että intressit datan omistussuhteiden kodifioimiseen ovat eri toimijoilla erilaiset: yritysmaailmassa omistusoikeuden toivotaan selkeyttävän yritysten välisten suhteita datan hyödyntäjinä, viranomaisten huolena on datatalouden ja kilpailun esteet ja käyttäjän näkökulmasta keskeistä on varmistaa omien henkilötietojen hyödyntämisen kontrollointi.

Omistusoikeuden kodifioimisen esteenä on kuitenkin vielä niin kansallisia kuin EU:n laajuisia esteitä. Tarkelan (2016, 81) mukaan datan omistusoikeuden säätämisen haasteena on pystyä liittämään se käsitteellisesti ja sisällöllisesti osaksi paitsi varallisuusoikeutta myös muita oikeusjärjestelmän osia, kuten perusoikeuksia ja velvoiteoikeutta. Hänen mukaansa kytkennän tekeminen mihinkään olemassa olevaan järjestelmään ei ole helppoa. Myös Thouvenin et al. (2017, 137) ovat varoittaneet samoista integraation haasteista. Janeček (2018, 1049) katsoo, että suurimpia esteitä datan

omistusoikeuden säätämiselle ainakaan ylhäältä, lainsäätäjän tavoitteista käsin (*top-down*) on EU:n oma perussopimus (Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoitu toisinto 2016. 2012/C 326/01), joka nykyisellään estää puuttumisen jäsenvaltioiden omistusoikeusjärjestelmiin. Hänen mukaansa (Janeček 2018, 1050) ainoa varteenotettava viitekehys datan omistusoikeudelle olisi rinnastaa se aineettomiin oikeuksiin, mutta huomauttaa samalla että EU (EU COM 2017a, artikla 345) on nimenomaan halunnut välttää säätämästä dataan oikeuksia, joita voitaisiin pitää ”super-IPR”:nä. Koska varallisuusoikeutta ei ole EU:n sisällä harmonisoitu eikä datan omistusoikeutta määritelty, omistusoikeuden säätäminen vaatisi joko uuden lain tai olemassa olevan lain muuttamisen soveltumaan datan erityispiirteisiin (Kauffman & Soares 2018, 523).

3.2 Data omistusoikeuden kohteena

Lähtökohta datan omistusoikeutta käsittelevissä lähteissä on useimmiten se, että tietoa tai dataa *ei voi omistaa* (e.g. Takki & Halonen 2017, 62; Valkjärvi 2017, 130) eikä sitä pitäisi monopolisoida omistusoikeudella, viitaten perusoikeuksiin, tiedon vapaaseen liikkuvuuteen ja merkitykseen yhteiskunnan resurssina. Dataan liittyy kuitenkin jo tällä hetkellä rajoituksia ja yksinoikeuksia. Omistusoikeuden kaltaisina oikeuksina voidaan pitää esimerkiksi pääsyä dataan, oikeutta rajata pääsyä muilta ja oikeuttaa poistaa data (Zhang 2018, 319). Asiantuntijoiden mielipiteet datan omistusoikeuden toteutuskelpoisuudesta ja muodoista vaihtelevat sen mukaan, mitä monitahoisempana resurssina he näkevät sen käsitteellisesti.

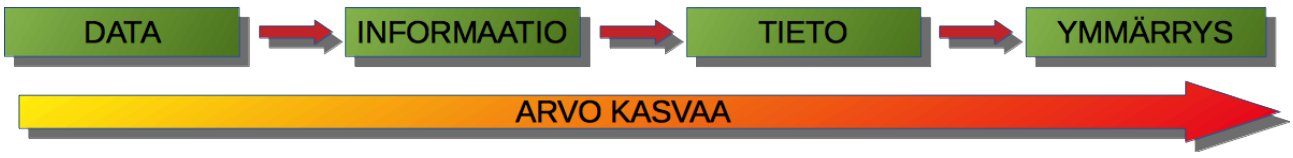
Omistusoikeuden kohteelta yleensä vaaditaan, että se on *kilpaileva*, *pois-sulkeva* ja *niukka* hyödyke (Malgieri 2016, 6). Data ei ole esineoikeudellisten omistuksen kohteiden kanssa samalla tavalla *kilpaileva* tai *niukka* hyödyke, että yhden omistuskappale olisi pois muilta tai estäisi muita nauttimasta samasta hyödykkeestä, tai ainakaan sen kopioista, jotka ovat käytännössä ilmaiseksi ja välittömästi luotavissa (Kauffman & Soares 2018, 521). Digitaloudessa datan arvo voi käyttäytyä kriittisen massan vuoksi jopa päinvastoin eli data on sitä arvokkaampaa mitä enemmän ja mitä laajemmalle sitä jaetaan (Singh & Vipra 2019, 57). Data on kuitenkin konkreettisessa muodossa *tiedostona* kilpaileva ja poissulkeva hyödyke, koska sen voi kadottaa tai sen hyödyntäminen voidaan estää (Tai 2017, 4-5).

Datan erityispiirteitä ja samalla ongelmia sen omistusoikeuden määrittelyn kannalta ovat sen vaikea määriteltävyys, dynaaminen luonne ja helppo kopioitavuus. Data ja informaatio sekoitetaan helposti käsitteinä, mikä vaikeuttaa yhteismitallista keskustelua datan omistusoikeudesta (Janeček 2018,

1042). Käsitteet ”data”, ”tieto” ja ”informaatio” eivät ole vakiintuneita sen enempää suomen kuin englannin kielessäkään ja niitä käytetään toisensa kanssa ristiin eri tieteenaloilla. Tämä tekee oikeuksien määrittelyn vaikeaksi, koska käsitteiden eri merkityksillä on erilaiset vaikutukset sen sisältämiin oikeuksiin. (Tarkela 2016, 67-68). Kirjallisuudessa yleensä asetetaan data yleisemmäksi, epävarmemmaksi *raaka-aineeksi*, josta joko saadaan tai ei saada arvokasta *informaatiota* (Tarkela 2016, 67). Datan arvon määrittelee sen *jatkojalostettavuus* ja *muokattavuus*. (Tarkela 2016, 68) Yhden määritelmän mukaan data muuttuu informaatioksi, kun ihminen antaa sille jonkun merkityksen (Alanko & Salo 2013, 7).

3.2.1 Informaation eri tasot

Tärkeä kysymys datan oikeuksia määriteltäessä on se, *minkä tasoiseen* dataan halutaan myöntää omistusoikeus. Informaatio voidaan ryhmitellä neljään hierarkiseen tasoon. Alin taso on informaation *rakenteellinen* taso eli fyysinen kuljetin kuten informaatio kirjana tai älylaittella. Toinen taso on *syntaktinen* eli informaatio merkkien tasolla, kuten kirjaimet tekstissä tai ohjelmiston koodi. Kolmas taso on *semanttinen* taso, joka sisältää informaation sisällön ja merkityksen, eli esimerkiksi puettavan älylaitteen palaute käyttäjälle. (Zech 2015, 3) Semanttisen tason yläpuolella voidaan vielä katsoa olevan *pragmaattinen* taso eli semanttinen ymmärrys käytännön hyödyllisenä sovelluksena (Thouvenin et al. 2017, 121). Saman asian voi esittää myös *datan arvoketjuna*:



Kuva 1. Datan arvoketju

Data on käyttäjästä kerättyä raaka-aineen tasoista informaatiota eli *raakadataa,* josta analysoidaan jonkin tulkinnan sisältävää informaatiota, joka vastaanottajan tulkinnan kautta muuttuu tiedoksi (Takki & Halonen 2017, 59-60). Datan hyödynnettävän arvon on olevan katsottu olevan semanttisella tasolla eli informaatiossa (ja siitä ylöspäin) ja informaation hyödyntämisen rajaaminen omistusoikeudella on sitä haitallisempaa yhteiskunnalle mitä korkeamman tason informaatiosta on kyse. (Zech 2015, 5-6) Syntaktisen ja semanttisen tiedon tasojen raja on kuitenkin häilyvä (Thouvenin et al. 2017, 135). Yleinen mielipide on, että semanttisen tason dataa ei pitäisi altistaa omistusoikeuden riskeille (e.g. Janeček 2018, 1042; Van Erp 2017, 244) toisaalta semanttisen tason dataa suojataan jo

esimerkiksi tietosuojalailla ja liikesalaisuuksien suojalla (Drexl 2017, 263). Drexlin (2017, 263) mielestä asia pitäisi ratkaista lailla, joka ottaisi tosiasiat huomioon tapauskohtaisesti ja kehottaa ottamaan mallia liikesalaisuuksien suojan mallista.

3.2.2 Datan anonymisointi

Datan rajaaminen henkilötiedoksi tai ei-henkilötiedoksi on vaikeaa ja raja on häilyvä. Tietosuoja-asetuksessa (GDPR) pseudonymisoidut eli jollain lisätiedolla tunnistettavan ihmisen tiedot ovat henkilötietoa ja GDPR:n antamien oikeuksien alaisia, mutta palveluntarjoajan *anonymisoimiin* tietoihin käyttäjä ei enää pysty käyttämään oikeuksiaan tai estämään käyttöä. Asetuksessa määritellään tunnistettavuuden rajaksi (GDPR johdanto-osa kohta 26) keinot, joita *joku* voi *kohtuullisen todennäköisesti* odottaa käyttävän henkilön tunnistamiseen. Henkilö on siis tunnistettavissa ja data on henkilötietoa, jos *joku* pystyy *laillisin* keinoin tunnistamaan henkilön datasta (Kauffman & Soares 2018, 528). Kohtuullisia keinoja tarkennetaan (GDPR johdanto-osa kohta 26): *"...olisi otettava huomioon kaikki objektiiviset tekijät, kuten tunnistamisesta aiheutuvat kulut ja tunnistamiseen tarvittava aika sekä käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys.* ".

Anonymisoidusta datasta henkilöiden tunnistaminen on kuitenkin ollut jo pitkään yleisesti tunnustettu ilmiö ja se tulee teknologian kehittyessä ja kerätyn datamäärän kasvaessa vain yleistymään (Purtova 2018, 7). Big data-analytiikan ja algoritmien kehitys sekä tekoälyn itsenäisyys ja läpinäkymättömyys tietomassan analysoinnin myötä muuttaa koko ajan datan luonnetta eikä muutosta välttämättä huomaa edes datan hallinnoija, tiedon kohteesta (datasubjekti) puhumattakaan. (Purtova 2017, 73;75-76) Sama data voi olosuhteista ja ajankohdasta riippuen olla molempia ja yhteyden vahvuus yksilöön voi muuttua asteittain koko ajan datan analysoinnin myötä (Purtova 2017, 77). Käytännössä siis henkilötiedon ja anonymisoidun tiedon erottaa vain aika ja resurssit prosessoida suuri määrä dataa ja anonymisoinnin voi katsoa käytännössä vähentävän käyttäjän oikeuksia omiin henkilötietoihinsa ja niiden hyödynnettävyyteen. Tämä on vakava heikkous edetenkin *erityisten henkilötietoryhmien* kuten terveyteen liittyvän datan suhteen. Henkilötiedon ja anonyymin tiedon rajan häilyvyys tekee omistusoikeuksien määrittelystä, hallinnoinnista ja täytäntöönpanosta vaikeaa (Purtova 2017, 75).

Komissio on huomauttanut tiedonannossaan (EU COM 2017b, 10), että käytännössä yrityksissä käsiteltävissä aineistoissa on yhtä aikaa molempia, niin henkilötietoa sisältävää kuin siihen

liittymätöntä dataa. Janeček (2018, 1043-1044) on esittänyt henkilötiedon käsitteelle tarkempaa erittelyä. Hän katsoo, että *luontainen* henkilötieto kuten ihmisen DNA täytyy jättää omistusoikeuden ulkopuolelle jo eettisistä ja ihmisoikeudellisista syistä, koska se liittyy yksilön identiteettiin, joka ei ole luovutettavissa. Toisaalta kaikki henkilötieto ei ole kuitenkaan *luontaisesti* tai lähtökohtaisesti henkilötietoa, vaikka se liittyisikin henkilöön vaan *ulkoista* henkilötietoa kuten IP-osoite. Omistusoikeus voitaisiin näin myöntää *vain* dataan, joka on henkilötietoa vain *ulkoisesti.* (Janeček 2018, 1043-1044) Malgieri ja Comandé (2017, 238; 244) katsovat, että tietosuoja-asetuksen määritelmä terveyttä koskeville tiedoille on liian epämääräinen, koska puettavien älylaitteiden käyttäjiltä kerätään niin suoraan terveyteen liittyvää dataa kuten sykettä ja kehon lämpöä kuin myös tällaisista suureista johdettua pääteltyä ja ennustavaa dataa, kuten sairastumisriskiä tai hedelmällisyyttä. Heidän (Malgieri & Comandé 2017, 232) mukaansa jälkimmäisten ryhmien data on kaikkein arkaluontoisinta ja silti tietosuoja-asetuksen antamien oikeuksien, kuten oikeus siirtää tietoja, ulkopuolella. On esitetty, että tietosuoja-asetuksen määrittelemille arkaluonteisille tiedoille eli *erityisille henkilötietoryhmille* kuten käyttäjän terveystiedoille pitäisi säätää muita henkilötietoja parempi suoja esimerkiksi immateriaalioikeuksien kautta (Trakman et al. 2019, 937; 957).

Henkilötiedon määrittely teknologisessa mielessä voi kuitenkin osoittautua vielä haasteellisemmaksi kuin yleisesti käsitteenä (Janeček 2018, 1046; 1051). Jotta yksilön henkilötietoon liittyvän datan omistusoikeus voitaisiin säätää, se pitäisi pystyä yksilöimään ja erottamaan muusta data-aineksesta (Van Erp 2017, 250-251) Data ei kuitenkaan ole esineoikeuden kohteeksi vaadittavalla tavalla *pysyvä* tai *yksilöitävä, ja* datan hyödyntäjien tavoitteena on nimenomaan poistaa datalta sen yksilöitävyys ja saada anonymisoinnin kautta mahdollisimman laajan hyödyntämisoikeus. Datan kytkemisessä esineoikeuksiin pitäisi silloin ottaa huomioon myös datan, joka *ei* sisällä henkilötietoa, hyödyntämisen logiikka ja muodot. (Tarkela 2016, 89-90) On myös esitetty, että *de lege ferenda* henkilötietoa ja ei-henkilötietoa ei edes pitäisi enää erotella tai säätää niitä koskevia tyyppikohtaisia sääntöjä, koska se vähentäisi lakien käytännön merkitystä ja niiden vaikutusta tavoitteisiin (Drexl 2018, 5-6).

3.2.3 Data ja kuljetin

Data ja fyysinen esine, jolla se on tallennettuna, nähdään varallisuusoikeuden näkökulmasta eri tavoin ja niihin voi kohdistua eri oikeudet. On epäselvää, voidaanko fyysisen esineen omistaja nähdä myös datan omistajana eli onko data erottamaton osa sen kuljetinta kuten älylaitetta. (Van Erp 2017, 251) Thouvenin et al. mielestä fyysisen esineen omistajaa ei voida lähtökohtaisesti ohittaa punnittaessa

datan omistajaa (Thouvenin et al. 2017, 135). Tätä voisi verrata pilvipalveluun ja sen asiakkaaseen. Pilvipalvelun asiakas omistaa pilveen tallentamansa datan, ellei sopimusehdoissa ole muuta sovittu ja muuta indikoiva ehto voitaisiin nähdä kohtuuttomana asiakkaan asemaa arvioitaessa. Toisaalta, muuttaako asiaa se, jos palvelu on asiakkaalle ilmainen? Koska esimerkiksi liikesalaisuuksien suoja vaatii, että suojan haltija on pyrkinyt estämään liikesalaisuuden paljastumisen ulkopuolisille, haltija voisi saada omistusoikeuden kaltaisen oikeuden dataan estämällä muiden pääsyn dataa sisältävään esineeseen kuten kovalevyyn (Zhang 2018, 306). Palveluntarjoajalla on data hallinnassaan, joten se pystyisi myös estämään pääsyn siihen ja tätä kautta saamaan eksklusiivisen oikeuden dataan.

3.2.4 Datan arvo

Omistusoikeudettoman datan liikkuessa vapaasti maiden välillä dataan liittyvät oikeudet ovat käytännössä sen kerääjällä (Singh & Vipra 2019, 53). Nykytilanteessa datan kerääjällä eli tässä tapauksessa palveluntarjoajalla on oikeus hyödyntää keräämäänsä dataa ja saada sen sisältämän tai siitä jalostetun taloudellisen arvon, jos data on kerätty tietosuojalainsäädännön määräysten mukaisesti (Singh & Vipra 2019, 56). Tämä tarkoittaa suostumuksen kysymisen lisäksi useimmiten henkilötietojen anonymisointia, jonka jälkeen tietojen hyödyntämiselle ei ole juuri rajoituksia eikä datasubjekti eli käyttäjä pysty enää seuraamaan datan käyttöä tai vaatimaan sen suhteen oikeuksiaan (Singh & Vipra 2019, 2). Malgieri & Custersin (2018, 290) mielestä nykyinen datatalouden käyttäjien ja palveluntarjoajien välinen tiedon epäsymmetria on vakava haitta käyttäjille ja he ehdottavat ratkaisuksi lakia, joka velvoittaisi palveluntarjoajat kertomaan selvästi käyttäjille heidän henkilötietojensa taloudellinen arvo. Tämä edistäisi heidän mukaansa käyttäjien aktiivista roolia datatalouden aktiivisina omien tiedollisten ja taloudellisten etujensa suojelijoina, nykyisen passiivisen, hyödynnettävän sivuroolin sijaan (Malgieri & Custers 2018, 290).

3.3 Omistusoikeuden määrittely

3.3.1 Omistusoikeuden sisältö

Omistusoikeuden katsotaan esineoikeudessa muodostuvan kolmesta elementistä eli omistajan hallintaoikeudesta, omistajan kompetenssista ja omistajan nauttimasta dynaamisesta suojasta (Mikkola 2017, 24). Näistä hallintaoikeus eli staattinen oikeus on primäärioikeus, joka takaa omistajalle oikeuden käyttää omistuksen kohdetta muiden häiritsemättä tai estämättä (Kaisto & Lohi 2013, 64-65). Omistajan kompetenssi on hallintaan nähden sekundäärinen oikeus ja tarkoittaa

omistajan kelpoisuutta määrätä omistuksen kohteesta eli siirtää esimerkiksi siirtää omistusoikeus toiselle henkilölle tai antaa kohde perintönä (Kaisto & Lohi 2013, 65-66). Omistusoikeuden siirtyminen toimijalta toiselle ei liity yksittäiseen hetkeen tai tapahtumaan vaan määritellään olosuhteiden ja oikeusasemien summana tai tapahtumien sarjana (Kaisto & Lohi 2013, 173).

Dynaaminen suoja taas tarkoittaa omistajan suojaa sivullisilta ja omistajan oikeuksiin nähden ristiriitaisilta, mutta alisteisilta oikeuksilta (Kaisto & Lohi 2013, 65). Dynaamista suojaa saisi siis henkilö, jonka oikeus dataan määriteltäisiin tärkeimmäksi tai voittavaksi oikeudeksi oikeuksien kollisioissa. Omistusoikeuden sisältö määräytyy kuitenkin kohteen tarkoituksen ja luonteen (Kaisto & Lohi 2013, 65), tässä tapauksessa datan käytön ja ominaisuuksien perusteella. Yhden määritelmän mukaan omistusoikeus ”*ilmentää tietynlaista esineen tosiasialliseen käyttöön ja hallintaan liittyvää oikeusasemaa*” (Kaisto & Tepora 2012, 243). Joissain tilanteissa kohteen luonteesta riippuen voidaan puhua ennemmin omistajan *oikeusasemasta* kuin *omistusoikeudesta* (Kaisto & Lohi 2013, 241). Aineettomien oikeuksien ollessa kyseessä onkin ennemmin käytetty nimityksiä kuten *tekijä, keksijä* ja *oikeuden haltija*. Johdonmukaisuuden vuoksi tässä tutkimuksessa käytetään kuitenkin käsitettä *omistusoikeus* ja *omistaja*.

Datan omistusoikeuden mallia voidaan lähteä määrittelemään kahdesta eri lähtökohdasta eli paradigmaattisen oikeuskäsityksen tai tyyppitapausajattelun kautta. Paradigmaattisessa oikeuskäsityksessä luodaan kokonaisvaltainen lainopillinen malli, tässä tapauksessa datan omistusoikeuden malli, jonka pohjalta pyritään antamaan ratkaisuja käytännön ongelmiin ja tapauksiin (*top-down*). Tyyppitapausmalli lähtee liikkeelle toisesta päästä eli käytännössä esiintyneistä tilanteita ryhmitellään tyyppitapauksiksi ja niistä johdetaan normeja (*bottom-up*). (Norrgård 2008, 215) Tiedon omistajuuteen suhtaudutaan sekä poliittisesti että asiantuntijoiden keskuudessa osin torjuvasti, minkä vuoksi omistajuus luo itse itseään käytännön tarpeiden pohjalta eli *bottom-up* (Janeček 2018, 1044). Tätä käytännön luomaa omistusoikeutta dataan on kirjallisuudessa kutsuttu *näennäisomaisuudeksi* (e.g. Malgieri 2016, 13; Purtova 2017, 66).

Top-down- lähestymistavan näkökulmasta omistusoikeutta ei ole olemassa ennen kuin se luodaan oikeudellisena instituutiona, kun taas bottom-up-lähestymistavan näkökulmasta omistusoikeuden kodifiointi vain vahvistaa olemassa olevan asetelman (Janeček 2018, 1044). Tämän voisi nähdä EU:n lainsäädännön näkökulmasta kahdeksi vaihtoehdoksi: odotetaanko datan omistusoikeuden teknologista ja omistusoikeudellista ”kypsymistä” käytännön kautta ja säädetään laki vakiinnuttamaan *de facto* omistusoikeus kun tilanne on tarpeeksi ”kypsä” (*bottom-up*) vai luodaanko

omistusoikeuden instituutio – melko epävakaassa ja koko ajan kehittyvässä tilanteessa – jonka toivotaan ohjaavan yhteiskunnallista ja teknologista kehitystä (*top-down*). Teknologian nopean kehityksen vuoksi voi olla vaikea arvioida oikeaa hetkeä säätää uutta lakia kummankaan lähestymistavan kautta. Kehitys tuskin tulee tulevaisuudessakaan hidastumaan.

Janečekin (2018, 1050) mukaan datan luonne resurssina, sen omistusoikeus ja omistusoikeuden perustelut pohjaavat arvoihin kuten ihmisoikeudet ja yksityisyys, ja siksi omistusoikeutta ei pitäisi säätää ylhäältä käsin (*top-down*) vaan käytännön muovaamien käsitteiden ja ongelmien pohjalta (*bottom-up*). Toisaalta tämän lähestymistavan heikkoutena on riski, että käytäntö muovautuu joidenkin yksilöiden, ryhmien ja yritysten kannalta epäeettisesti ja kilpailun kannalta kyseenlaiseksi (Janeček 2018, 1051). Drexlin (2018, 32) voi tulkita kannattavan samaa lähestymistapaa. Hänen mukaansa datan omistusoikeus olisi häiriö datan vapaaseen liikkuvuuteen ja toisi yhteiskunnallisia haittoja, joten muutokselle pitäisi olla vahvat perustelut (Drexl 2018, 32). Valitun lähestymistavan pitäisi kattaa neljä omistusoikeuden tavoitetta: kontrolli, suoja, arvonmääritys ja allokaatio (Janeček 2018, 1044).

Janeček (2018, 1041) viittaa säädösoikeuden (civil law) ja tapaoikeuden (common law) eroihin omistusoikeuden määrittelyssä. Säädöslaissa omistusoikeus perustuu *numerus clausus*- periaatteelle (tyyppipakkoperiaate), joka rajoittaa omistusoikeuden vain niihin kohteisiin ja tyyppeihin mitkä laissa on määritelty. Common law-maissa omistusoikeus nähdään monimutkaisemmin joukkona tai *kimppuna* oikeuksia, joita voi olla vaihteleva määrä ja ne voivat päteä yhtä (*in personam*) tai kaikkia (*in rem*) kohtaan (Janeček 2018, 1041). Maissa, jossa oikeusjärjestelmä perustuu säädösoikeuteen, kuten Suomessa, omistusoikeus sisältää kaikki laissa omistuksen kohteeseen säädetyt oikeudet (*numerus clausus*) ja oikeus on pätevä kaikkia kohtaan (*erga omnes*) (Janeček 2018, 1041). Datan omistusoikeuden määrittely *erga omnes*-oikeutena vaatii lisäksi, että oikeudet ovat laissa määriteltyjä (*numerus clausus*) ja ne ovat kaikille julkisia ja läpinäkyviä. Ulkopuolistenkin pitäisi pystyä jotenkin varmistumaan tiettyyn kohteeseen liittyvistä oikeuksista ja näiden vaikutuksista. (Van Erp 2017, 239).

Käytännössä *numerus clausus*-periaatteesta seuraa, että omistusoikeutta dataan ei voida säätää Suomen varallisuuslain perusteella osittaisena, ns. *oikeuksien kimppuna*. Vaikka Iso-Britannia common law-maana on eronnut EU:sta, Irlanti on edelleen common law-jäsenvaltio (Osborne Clarke LLP 2016, 82). Koska kuitenkin ylivoimaisesti suurimman osan EU-jäsenmaiden oikeusjärjestyksistä perustuu säädösoikeuteen, mahdollinen datan omistusoikeus tulisi perustumaan

numerus clausus-periaatteelle eikä common law-maiden tapaan dataan liittyviin oikeuksiin erillisinä, mukautettavana oikeuksien joukkona. Van Erp (2017, 254) viittaa Luxemburgin lakiin ja oikeustapaukseen (Your Response Ltd. v. Datateam Business Media.), jonka myötä säädettiin lakiin oikeus saada maksukyvyttömän hallussa olevasta tavaroista oma aineeton omaisuus, jos se oli *erotettavissa* maksukyvyttömän omaisuudesta. Hänen mielestään tapaus on osoitus säädösoikeusjärjestelmän muutoksesta ja digitaalisen omaisuuden hyväksymisestä osaksi varallisuusoikeuden *numerus clausus*-ryhmää (Van Erp 2017, 254-255).

Van Erp (2017, 238-239) katsoo eurooppalaisen varallisuusoikeuden kehityksen kansallishenkisen, nurkkakuntaisen ja putkinäköisen historian olevan syynä omistusoikeuden joustamattomuudelle. Hänen mukaansa immateriaalioikeus piti tästä syystä säätää omaksi oikeudenalakseen, koska aineettomat teokset eivät soveltuneet esineoikeuden ahtaaseen muottiin, mutta immateriaalioikeuden säätämisessä tehtiin sama virhe, eikä otettu huomioon immateriaalioikeuden yhteyksiä oikeusjärjestelmän muihin aloihin. Kotimaisessa tutkimuksessa esimerkiksi Tarkela (2016, 83) on vaatinut kokonaisvaltaista hahmottamista ja integraatiota datan omistusoikeuden lisäämisessä osaksi oikeusjärjestelmää, jos sellaiseen päädytään. Hän huomauttaa, että esimerkiksi digitaalisten teosten liittäminen osaksi tekijänoikeutta oli monelta kannalta välttämätöntä, mutta vaillinainen ja kapea kytkentä muuhun oikeusjärjestelmään on tuonut konflikteja suhteessa muun muassa sananvapauteen (Tarkela 2016, 84). Van Erpin (2017, 245-246) mielestä varallisuusoikeuden historian painolasti nykyteknologiaan sopimattomine käsitteineen vaikeuttaa tämän hetken ongelmien ratkaisemista.

Omistusoikeuden voidaan katsoa syntyvän lain takaamilla *erga omnes*-oikeuksilla, jotka antavat johonkin resurssiin hallinnan ja suojan (Janeček 2018, 1042). Purtovan (2017, 66;70) mukaan tietosuoja-asetus (GDPR) on jo tuonut de facto omistusoikeuden kaltaisen oikeuden yksilölle henkilötietoihinsa esimerkiksi oikeudella siirtää tietojaan järjestelmästä toiseen, vaikkakaan asetuksessa ei oteta kantaa omistusoikeuden keskeiseen ominaisuuteen eli eksklusiivisuuteen, oikeuteen sulkea muut pois. Myös Malgierin (2016, 8) mielestä käyttäjällä on jo omistusoikeuden kaltaisia oikeuksia omiin henkilötietoihinsa. Se, että omistusoikeus on *erga omnes*-oikeutena pätevä kaikkia kohtaan, tekee siitä vahvemman omitusoikeuden määrittäjän kuin rajattujen osapuolten välinen sopimus (Kauffman & Soares 2018, 522). Tämän perusteella erityisesti käyttäjä hyötyisi datan omistusoikeuden säätämisestä, koska sopimusoikeudellisesti datan kerääjä on itse laatimiensa sopimusten vuoksi jo lähtökohtaisesti vahva osapuoli.

Omistusoikeus voidaan määritellä myös *nominalismin* tai *essentialismin* kautta (Duch-Brown et al. 2017, 13). Duch-Brown et al. (2017, 13) katsovat, että datataloudessa datan omistusoikeus määritellään *essentialismin* kautta eli jos käytännössä joku pystyy määräämään omistuksen kohteesta, taho on datan todellinen omistaja – verrattuna *nominalismiin*, jossa oikeusjärjestelmä määrittelee oikeuden kohteen ja omistajan.

3.3.2 Omistusoikeuden allokaatio

Kysymys omistusoikeuden *omistajasta* on kahden perusoikeuden törmäyskohta. Ihmisoikeuksiin kuuluvan yksityiselämän suojan (Suomen perustuslaki, PL 731/1999, luku 2, 10 §) pohjalta voisi argumentoida omistusoikeuden kuuluvan datasubjektille (käyttäjä), omistusoikeuden suojan (PL luku 2, 15 §) perustella taas omistusoikeus pitäisi määritellä puolueettomasti. (Janeček 2018, 1047) Toisaalta henkilötiedon omistusoikeus ja itsemääräämisoikeus dataan on sanottu olevan ristiriidassa perusoikeuksien luovuttamattomuuden kanssa (Janeček 2018, 1045) Voiko joku *omistaa* jotain mistä ei voi perusoikeuksien valossa luopua? Janeček (2018, 1045) huomauttaa GDPR:n ja älylaitteiden teknologisten ominaisuuksien, kuten prosessiin sisältävän automaattisen kopioinnin, jo tällä hetkellä rajoittavan henkilötietojen täydellistä hallintaa.

Omistusoikeuden säätämisessä on haasteena tehdä henkilötiedon ja ei-henkilötiedon välinen rajanveto ja määritellä milloin data liittyy datasubjektiin, tässä tilanteessa käyttäjään, niin oleellisesti, että hänelle voidaan myöntää omistusoikeus dataan (Purtova 2017, 64). Tarkela (2016, 74-75) luo analogian ihmisperäisestä datasta ihmisperäisen kudosnäytteen omistajuudesta käytyyn keskusteluun. Datan ja kudosnäytteen voi molempien katsoa olevan välinearvoisia raaka-aineita, joista jalostetaan todellisen arvon sisältävä *informaatio.* Hän huomauttaa, että oikeus informaation hyödyntämiseen kaupallisesti ja tutkimukseen onkin ehkä tärkeämpää ja arvokkaampaa kuin raaka-aineen, kuten datan tai kudosnäytteen fyysinen tai oikeudellinen hallinta. Molempien hyödyntäminen perustuu yksilöltä saatuun *suostumukseen,* mutta sääntely ei ota huomioon jatkojalostukseen perustuvaa arvonlisäystä ja sen epätasaista jakautumista. (Tarkela 2016, 74-76)

Voi kysyä, onko suostumus yleensäkään toimiva malli yksilön terveyteen liittyvän datan käsittelyyn kun sen analysointi ja datan kulku toimijoiden välillä ei ole läpinäkyvää. Käyttäjä ei pysty nykyisen sääntelyn oloissa saamaan osaansa oman terveysdatansa tuottamasta taloudellisesta hyödystä, kun arvonlisäys tapahtuu hänen ulottumattomissa ja hänen tietämättään. Tästä voi luoda vertailun julkisten organisaatioiden biopankkien (tai FinDatan) toimintalogiikkaan MyData-hengessä: jos

käyttäjä pystyisi hallinnoimaan suostumusperusteisesti omien henkilötietojensa käyttöä tietojen välittäjän kautta ja valitsemaan omien tietojensa käyttömahdollisuudet (e.g. tutkimus, kaupallinen) sekä halutessaan peruuttamaan käyttöoikeuden tietoihinsa, malli mahdollistaisi tietojen luotettavan anonymisoinnin, valikoivan luovuttamisen sekä datan hyödyntämisestä kertyvän taloudellisen arvon tasaisemman jakautumisen. Tarkelan (2016, 104) mukaan henkilötiedon häivyttäminen datasta esimerkiksi anonymisoinnilla heikentää nykytilanteessa suostumusperusteisen datan omistusoikeuden hallinnan tehokkuutta, eikä hän näe todennäköisenä, että suuret yritykset suostuisivat näiden datan muokkaamistapojen rajoituksiin.

Asetelma olisi kuitenkin toinen, jos yritykset saisivat oikeudet datan käyttöön vain välittäjän kautta ja muokkaamista ja hyödyntämistä hallitsisi käyttäjä. Tämä toki tarkoittaisi käytännössä nykymuotoisen käyttösopimuspohjaisen datan käytön lopettamista ja se vaatisi uuden lain tai tietosuoja-asetuksen muokkaamista terveystiedon osalta. Toisaalta ei ole itsestäänselvyys kuuluuko edes osa arvonlisäyksestä käyttäjälle, kun varsinaisen datan jalostuksen tekee joku muu.

Datan ihmisperäisyyden merkityksen voidaan katsoa vähenevän sitä mukaa kun muiden datan hyödyntäjien tekemät panostukset ja jatkojalostus lisäävät datan taloudellista arvoa, ja erottavat *datan* ja siitä jalostetun *informaation* kehityksen (Tarkela 2016, 77). On kuitenkin vaikea määritellä ajankohtaa tai taitekohtaa, missä yksilön oikeus terveyttään koskevaan dataan ei olisi enää relevantti (Tarkela 2016, 77) Anonymisoinnin voi katsoa tietosuojalainsäädännön perusteella jollain tavalla olevan tällainen muutos. On kuitenkin kiistanalaista voiko henkilötietoa edes *omistaa* siinä mielessä, että oikeudet siihen voisi luovuttaa, esimerkiksi myydä, ja jos voisi, *kenelle* ne voisi myöntää (Janeček 2018, 1045-1047). Janečekin (2018, 1047) mielestä *luontaisen* (intrinsic) henkilötiedon omistajuutta ei voi ihmisoikeuksien näkökulmasta oletusarvoisesti myöntää kenellekään muulle kuin käyttäjälle, kun taas datan joka on henkilötietoa vain *ulkoisesti,* kuten käyttäjän metatiedot, ei pitäisi häneen mukaansa ei pitäisi lähtökohtaisesti allokoida käyttäjälle vaan omistajuus ratkaista tasapuolisen arvioinnin kautta.

4 Immateriaalioikeudellinen näkökulma

4.1 Omistusoikeus aineettomaan omaisuuteen

Immateriaalioikeuksien, kuten muidenkin lakiin perustuvien oikeuksien, vahvuus datan omistuksen määrittelyssä verrattuna sopimusehtoihin on niiden pätevyys suhteessa myös sopimuksen

ulkopuolisiin (Takki & Halonen 2017, 67). Datan omistusoikeuden määrittelyä immateriaalioikeuden kautta puoltaa lisäksi se, että teknologisen kehityksen myötä immateriaalioikeudessa on aiemminkin jouduttu ratkaisemaan uusien omaisuusryhmien kytkeminen osaksi järjestelmää ja sen käsitteistö on muotoutunut abstrakteihin kohteisiin. Myös suojattavien kohteiden rajanvedon epämääräisyys on immateriaalioikeudessa tuttu ongelma. (Tarkela 2016, 81-82 92). Komissio on kuitenkin vuoden 2017 tiedonannossaan (EU COM 2017b, 10) linjannut, että raakadataan, jota esimerkiksi puettavan teknologian keräämä datakin on ennen käsittelyä, ”*ei sovelleta teollis- ja tekijänoikeuksia, koska sen ei katsota syntyneen henkisen työn tuloksena ja/tai olevan millään tavalla omaperäistä*”. Immateriaalioikeudessa oikeuksien myöntäminen siten perustellaan sen luomiseen tai keräämiseen tehdyllä inhimmillisellä tai taloudellisella panoksella (Tarkela 2016, 93). Tarkelan (2016, 95-96) mukaan immateriaalioikeuden käsitteet ja logiikka eivät sovellu datan omistusoikeuden kehikoksi, koska datan ominaisuudet eivät vastaa tekijänoikeuden lähtökohtia kuten luovaa panosta tai oikeuden kohteen pysyvyyttä. Immateriaalioikeuden kautta kuitenkin suojellaan jo nykyisin dataa joissakin muodoissa kuten tietokantoina ja liikesalaisuuksina. On esitetty, että datan omistusoikeuden voisikin Suomessa toteuttaa lähinnä tietokantasuojan tai liikesalaisuuksien suojan avulla (Takki & Halonen 2017, 63). Seuraavassa käydään läpi eräitä suojamalleja mahdollisina muotoina käyttäjän datan suojaamiseen nykyisessä tai mahdollisessa tulevaisuuden lainsäädännössä.

4.2 Tekijänoikeus

Tekijänoikeus perustuu lähtökohdalle, että oikeudenhaltijalla eli *tekijällä* on etuoikeus ja yksinoikeus päättää teoksen hyödyntämisestä (Oesch 2008, 4) Koska datan kerääminen ei vaadi kuitenkaan tekijänoikeudelle keskeistä luovaa panosta, sitä ei voida lähtökohtaisesti pitää *teoksena* (Kauffman & Soares 2018, 524). Tekijänoikeuslakiin (8.7.1961/404) kuitenkin sisältyy myös erityinen suoja *luetteloille ja tietokannoille*, joka eroaa muista tekijänoikeuden kohteista siinä, että suojaa annetaan tehdyn työn, käytetyn ajan sekä taloudellisten panostusten perusteella (Sorvari 2007, 56).

Kuten muutkaan immateriaalioikeudet, tekijänoikeus ei suojaa informaatiota itsessään vaan päinvastoin pyrkii edistämään informaation leviämistä ja hyödyntämistä (Drexl 2018, 3;32). Oesch (2008, 7-8) on huomauttanut, että tekijänoikeuden *tekijän* määrittely on tullut digiaikana vaikeammaksi ja kahtiajako *käyttäjään* ja *oikeudenhaltijaan* on muuttunut perinteisestä. Sama taho voi vastaanottaa, jalostaa, linkittää ja olla samalla luovan tekijän roolissa. (Oesch 2008, 7-8) Käyttäjän kannalta omistusoikeuden vaikeutena on hänestä kerätyn muokkaamattoman raakadatan keskeneräinen luonne. Raakadataan ei sinällään voida antaa omistusoikeutta (EU COM 2017b, 10)

ja palveluntarjoajan jalostuksen myötä arvokkaampi ja anonymisoitu data ei taas ole enää aukottomasti yhdistettävissä käyttäjään eikä tietosuojalainsäädännön perustella edes käyttäjän henkilötietona oikeuden kohde. Palvelutarjoajalle sen sijaan on useita vaihtoehtoja millä omistusoikeuden säätäminen käyttäjän dataan voisi olla mahdollista.

4.2.1 Tietokantasuoja ja *sui generis -oikeus*

Tietokannat ovat Big Datan aikakaudella merkittävässä roolissa niin teknisesti tietomäärän hallinnoinnissa kuin sen kaupallisessa hyödyntämisessäkin (Valkjärvi 2017, 129). Sähköisen tietokannan voi suojata joko tekijänoikeudella tai *sui generis* -oikeudella tai molemmilla. Tekijänoikeudella voi suojata tietokannan rakenteen ja *sui generis* -suojalla sen sisällön. Eri suojille on erilaiset vaatimukset mutta jos tietokanta täyttää nämä, se voidaan suojata molemmilla oikeuksilla. (EU 2020) Tietokannan rakenteen suojaaminen tekijänoikeudella vaatisi sen aineiston valinnassa ja järjestämisessä näkyvän tekijän *omaperäinen henkinen luomus* (Tietokantadirektiivi 96/9/EY, johdanto-osa kohdat 15 ja 16). Sähköinen henkilötietoja sisältävä tietokanta on useimmiten ominaisuuksiltaan sopiva täyttämään molempien suojien vaatimukset (Valkjärvi 2017, 150. Koska datan kerääminen ei vaadi kuitenkaan tekijänoikeudelle keskeistä luovaa panosta, sitä ei voida lähtökohtaisesti pitää teoksena (Kauffman & Soares 2018, 524). Tämän vuoksi mahdollisuudeksi jää vain *sui generis* -suoja, jonka vaatimukset on määritelty tekijänoikeuslain 5 luku 49 §:ssä:

> *Sillä, joka on valmistanut*
>
> *1) luettelon, taulukon, ohjelman tai muun sellaisen työn, jossa on yhdisteltynä suuri määrä tietoja, taikka*
>
> *2) tietokannan, jonka sisällön kerääminen, varmistaminen tai esittäminen on edellyttänyt huomattavaa panostusta,*
>
> *on yksinomainen oikeus määrätä työn koko sisällöstä tai sen laadullisesti tai määrällisesti arvioiden olennaisesta osasta valmistamalla siitä kappaleita ja saattamalla se yleisön saataviin.*

Sui generis -tietokantasuoja antaa siis yksinoikeuden määrätä tietokannasta, jonka kerääminen, varmistaminen ja esittäminen on edellyttänyt *huomauttavaa panostusta*. Suoja ei koske yksittäistä tietoa tai pientä kokonaisuutta ja se on voimassa 15 vuotta (Takki & Halonen 2017, 64). *Sui generis* -suoja tai käyttöehdot eivät kuitenkaan voi estää tietokannan laillisia käyttäjiä kopioimasta ja uudelleen käyttämästä tietokannasta osia, jotka eivät ole sisällön laadullisesti tai määrällisesti arvioiden olennaisia (EU 2020; Tekijänoikeuslaki 5 luku 49 §). *Sui generis* -tietokantasuojaa

kuitenkaan tuskin sovellettaisiin niin, että käyttäjä saisi suojaa omalle henkilötiedolleen koska käyttäjän on vaikeaa ellei mahdotonta näyttää tehneensä *huomattavan panostuksen* datan keräämiseen, joten suojasta on nykyisellään taloudellista hyötyä ainoastaan datan kerääjälle eli palveluntarjoajalle (Kauffman & Soares 2018, 525-526), Käyttäjältä kerätty raakadata ei tavoittaisi suojan vaatimuksia pienenä osana kokonaisuudesta siltäkään osin, että se on ennen muokkaamista järjestymätöntä datamassaa (Banterle 2018, 5).

Tietokantasuojan voi nähdä lainsäätäjän antamana myönnytyksenä henkilötietojen taloudelliseen hyödyntämiseen (Valkjärvi 2017, 152). Vaikka tietokannan suojassa ovat vastakkain palveluntarjoajan taloudellinen intressi ja käyttäjän yksityisyys ja tiedollinen itsemääräämisoikeus, molempien pitkälti yhteisenä tavoitteena on henkilötietojen suojaaminen ja salaaminen (Valkjärvi 2017, 150-151). Käyttäjän kannalta heikkous on siitä, että palveluntarjoaja hyödyntää tietoja lopulta suhteessa kolmansiin osapuoliin, mitä käyttäjälle ei ole aikaisemmin mainitun anonymisoinnin jälkeen mahdollisuutta vastustaa. Henkilötietojen suoja kuitenkin rajoittaa tietokannan hyödyntämistä siinä mielessä, että sen keräämisessä on noudatettava tietosuojalain ja -asetuksen säännöksiä, muuten se ei saa tekijänoikeudellista suojaa (Valkjärvi 2017, 152). Jos siis osoitettaisiin esimerkiksi ennakkotapauksena, että käyttäjää ei ole informoitu tarpeeksi henkilötietojen käyttötavoista ennen suostumusta tai että henkilötietoja olisi käytetty muuten käyttöehtosopimuksen vastaisesti, palveluntarjoajan keräämä tietokanta ei saisi tekijänoikeudellista tietokantasuojaa.

Tietokantasuoja on kuitenkin törmännyt käytännön vaikeuksiin sitä kautta, että suojatuksi tarkoitettu panostus, tietokanta itsessään, ei ole usein välttämättä tärkein taloudellisen arvon lähde vaan tietokannan muodostuksen yhteydessä syntynyt sivutuote (Tarkela 2016, 94). Tarkelan (2016, 95) mukaan tietokanta ei sovi datan omistusoikeuden välineeksi, koska yleinen datamassa ei vertaudu tietokannan ominaisuuksiin epäkoherenttina kokonaisuutena. *Sui generis*-tietokantasuoja ei ole muutenkaan ollut niin tiedeyhteisön kuin myöskään Euroopan Komission itsensä näkökulmasta onnistunut suojamuotona ja jopa sen kumoamista harkitaan (Hugenholtz 2017,76-77). Tarkelan (2016, 94) mukaan EU:n tuomioistuimen oikeustapaukset aiheesta kuvaavat datan määritelmällistä vaikeutta. Tietokantasuojan on sanottu olevan varoittava esimerkki siitä, mitä tapahtuu jos datan vaikutuksia yhteiskunnallisia vaikutuksia ei arvioida kokonaisvaltaisesti lakeja säädettäessä (Drexl 2018, 3)

4.2.2 Liikesalaisuuksien suoja

Liikesalaisuuslaki (595/2018) tuli voimaan vuonna 2018 ja perustuu EU:n liikesalaisuusdirektiiville (Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/943, annettu 8 päivänä kesäkuuta 2016, julkistamattoman taitotiedon ja liiketoimintatiedon (liikesalaisuuksien) suojaamisesta laittomalta hankinnalta, käytöltä ja ilmaisemiselta), jolla on tarkoitus harmonisoida eri jäsenmaiden vaihtelevia lainsäädäntöjä sekä tuoda liikesalaisuuksien suojaa lähemmäs muita aineettomia oikeuksia (Vapaavuori 2019, 23). Liikesalaisuuksien suoja koskee arvokasta tietoa, joka ei ole *kokonaisuutena* tai *osiensa täsmällisenä kokoonpanona tai yhdistelmänä* asiaan perehtyneen henkilön tiedossa tai helposti saatavissa. (Liikesalaisuuslaki 2 § 1 a,b). Tämän lisäksi liikesalaisuuden oikeudellisen haltijan edellytetään *ryhtyneen kohtuullisiin toimenpiteisiin* liikesalaisuuden suojaamiseksi eli käytännössä tehneen esimerkiksi salassapitosopimuksia liikesalaisuuden varjelemiseksi (2 §, 1 c). Tietoon liittyvä arvo ja kilpailuetu syntyy siitä, että se ei ole muiden, tai ainakaan kaikkien kilpailijoiden tiedossa (Vapaavuori 2019, 23). Toisin kuin muut immateriaalioikeudet, liikesalaisuuksien suoja ei anna *yksinoikeutta*, vaan ainoastaan estää liikesalaisuuden kohteena olevan tiedon *oikeudettoman* siirtymisen muille osapuolille väärinkäytösten kautta mutta sen vahvuus on joustavuudessa eli siinä, että suojan kohde voi olla lähes mikä tahansa arvokas ja yleisesti tuntematon tieto (Vapaavuori 2019, 37; Liikesalaisuuslaki 3 §). Liikesalaisuuksien suojan rajat ovat kuitenkin käytännössä tulleet vasta oikeuskäytännön kautta selkeämmiksi (Oesch 2017, 13) Liikesalaisuuksien suoja ei siis anna *omistusoikeutta* liikesalaisuuksiin (Stepanov 2019, 72). Jos joku saa saman tiedon haltuunsa laillisin keinoin, esimerkiksi itsenäisesti keksimällä tai luomalla, mikään ei estä häntä hyödyntämästä tai paljastamasta samaa tietoa (Liikesalaisuuslaki 3 §). Oikeudettomasti tiedon hankkinut ei saa kuitenkaan paljastaa liikesalaisuutta muille (4 §). Liikesalaisuuden julkinen paljastuminen päättää sen suojan (Drexl 2018, 56). Koska dataa on kuitenkin käytännössä jaettava ekosysteemissä monen toimijan kesken, salassapidon pyrkimystä tai *kohtuullisia toimenpiteitä* voi olla vaikea todistaa (Banterle 2018, 7).

Liikesalaisuuksien suojan vahvuus on sen soveltuminen monenlaisiin, niin pieniin kuin suuriinkin, datakokonaisuuksiin eikä sen kohteilta vaadita luovuutta, teoskynnyksen ylittämistä, henkisen tai taloudellisen panostuksen osoittamista tai tietyntyyppistä dataa (Banterle 2018, 7). Yritykset käyttävät liikesalaisuuksien suojaa jo esimerkiksi asiakastietojensa ja profilointialgoritmiensa suojaamiseen (Malgieri & Custers 2018, 289). Malgieri (2016, 2) on ehdottanut liikesalaisuuksien suojan soveltamista myös yksilöiden henkilötietojen hallintaan, tietosuoja-asetuksen täydentäjänä.

4.3 Datan tuottajaoikeus

Datan tuottajaoikeutta (vapaasti suomennettu, data producer's right) on pohdittu mahdollisena ratkaisuna tarpeeseen määritellä datan omistusoikeus. Ehdotus perustuu komission valmisteluasiakirjassa (EU COM 2017a, 30) mainittuihin vaihtoehtoihin, joilla haluttiin edistää ei-henkilötiedon ja anonymisoidun henkilötiedon saatavuutta ja jakamista sekä suojata investointeja ja vapaata kilpailua. Vaikka ehdotus käsittelee vain anonymisoitua henkilötietoa, oikeus koskisi edellä mainitusta anonymisoinnin ongelmista johtuen mahdollisesti myös puettavan teknologian käyttäjien dataa ja oikeuksia sen hyödyntämiseen.

Vaihtoehtoina on oikeus joko kaikkia kohtaan pätevänä *in rem*-oikeutena, jonka voisi nähdä vastaavan omistusoikeutta tai ryhmänä puolustavia oikeuksia, jotka vastaisivat datan hallussapitoa/hallintaa ja antaisivat datan lailliselle *haltijalle* mahdollisuuden kieltää datan hyödyntäminen ja väärinkäyttö. Oikeus koskisi vain datan koodia, ei sitä koskevaa informaatiota eikä olisi varsinaisesti omistusoikeus vaan käyttöoikeus. (Stepanov 2019, 74) Tekijänoikeuden panostuksen palkitsemisen logiikan mukaan oikeuden haltija olisi datan kerääjä tai laitteen valmistaja. Oikeuden haltijaa voi olla kuitenkin vaikea määrittää ekosysteemissä ja oikeus voitaisiin myöntää myös ryhmälle (Stepanov 2019, 74-75). Hugenholtzin (2017, 76) mukaan tuottajaoikeus koneen tuottamaan dataan veisi pohjan perinteiseltä vapaan tiedon lähtökohdalta ja toisi monia uusia ongelmia olemassa olevien immateriaalioikeuksien kuten tekijänoikeuden ja tietokantasuojan tulkintojen kanssa. Hänen mielestä tärkeämpää olisi keskittyä edistämään big datan tuomaa yhteiskunnallista hyödyntämistä varmistamalla datan vapaa liikkuvuus.

5 Henkilötietolainsäädännön näkökulma

5.1 Omistusoikeus henkilötietojen suojan välineenä

Omistusoikeuden myöntämistä henkilötietoon on esitetty tavaksi toteuttaa ja vahvistaa tietosuojaa sekä yksilöön liittyvän tiedon itsemääräämisoikeutta. Omistusoikeus pätevänä kaikkia muita kohtaan (*erga omnes*) antaisi yksilölle tehokkaan tavan hallita henkilötietojaan, toisin kuin esimerkiksi sopimus tai lisenssi, joka sitoo vain sen osapuolia (Purtova 2017, 67). Tämä ominaisuus on hyödyllistä erityisesti nykyisessä teknologisessa tilanteessa, kun data voi olla missä tahansa kohtaa datan hyödyntämisen ekosysteemiä ja arvoketjua. (Purtova 2017, 67-68)

Datan omistusoikeus ja tietosuoja voidaan nähdä myös vastakkaisina ilmiöinä. Janeček (2018, 1043) vertaa yksityisyydensuojan ja omistussuoja kannattajien näkemyksien eroja *muna-kana*- dilemmaan. Vaarantaisiko datan muut poissulkeva omistusoikeus tieto/yksityisyydensuojan vai omistusoikeuden suojan puuttuminen tieto/yksityisyydensuojan? Omistusoikeuden kannattajat haluaisivat hyödyntää ”munan” arvon ja luoda sen hallinnalle viitekehyksen, yksityisyydensuojan kannattajat taas suojata ”kanan” yksityisyyden.

Henkilötietojen ja yksityisyydensuoja on keskeinen osa keskustelua datan omistusoikeudesta, koska käyttäjän kontrolli omiin henkilötietoihin on edellytys oman identiteetin suojelemiseen ja oikeusturvaan ja sitä kautta puoltaa datan omistusoikeuden myöntämistä yksilölle hänen omiin henkilötietoihinsa. Henkilötietojen suoja liittyy myös monella tavalla yksilön taloudellisten oikeuksien ja tasa-arvon toteutumiseen. Yksilö voi yritysten profiloimana kuluttajana toisaalta hyötyä henkilötietojen jakamisesta, jos pystyy osoittamaan olevansa toivottu ja edullinen asiakas, mutta myös kärsiä taloudellisesti ei-toivottuna ja ei-kannattavana asiakkaana (Duch-Brown et al. 2017, 31).

On esitetty, että henkilötietojen suojaan liittyviin oikeuksiin pitäisi liittää dataan liittyvät taloudelliset omistusoikeudet, koska GDPR ei ota niihin tällä hetkellä kantaa (Singh & Vipra 2019, 2). Kuitenkin Duch-Brown et al. (2017, 15) mukaan tietosuoja-asetukseen ei tarkoituksella sisällytetty datan myytäviä oikeuksia, koska yksityisyydensuoja on perusoikeus eikä sitä voi tehokkaasti luovuttaa. Thouvenin et al. (2017, 135) varoittavat nykyisen tietosuoja-asetuksen ja mahdollisen datan omistusoikeuden olevan ristiriitaiset keskenään. Heidän mukaansa konflikti vaatisi GDPR:n muuttamista ja he ehdottavat ratkaisuksi GDPR:n osittaista korvaamista datan omistusoikeuksilla. GDPR:ssä määritelty henkilötiedon käsite kuitenkin rajaa mahdollisuutta saada taloudellisia oikeuksia dataan tietosuojan kautta, koska yritykset anonymisoivat tiedot ennen jalostamista, ja

vaikka tiedot eivät olekaan edellä käsitellyistä syistä absoluuttisesti tai lopullisesti anonyymejä, tietosuoja-asetus ei anna käyttäjälle oikeuksia dataan, jonka ei katsota olevan enää henkilötietoa (Drexl 2018, 33). GDPR:n on sanottu jopa antaneen datan todellisen omistusoikeuden käytännössä datan kerääjälle. Tämän sanotaan johtuvan siitä, että GDPR:ssä käyttäjälle määriteltyjen oikeuksien ulkopuolelle jäävät *residuaalioikeudet* eli oikeudet, joita ei ole muuten määrätty kenellekään muulle taholle ja jotka käytännössä näin jäävät datan kerääjälle eli palveluntarjoajalle. (Duch-Brown et al. 2017, 17) Tämä tarkoittaisi käytännössä, että kuluttajan oikeuksien laajuus riippuu siitä, kuinka paljon hän käyttää tietosuoja-asetuksen tuomia oikeuksiaan.

Omistusoikeuteen on nähty kuuluvan aktiivisia ja passiivia oikeuksia. Henkilötietojen suojeleminen omistusoikeuden kautta on passiivinen oikeus. (Janeček 2018, 1045). Omistusoikeuden vaatima läpinäkyvyys ja oikeuksien julkisuus on ongelma erityisesti henkilötietojen suojan kannalta koska älylaitteen käyttäjä ei voi vaatia suojaa tai omistusoikeutta henkilötiedolleen, jos hän ei ole tietoihin datan olemassaolosta. Omistusoikeuden aktiivinen oikeus eli oikeus säilyttää ja esimerkiksi hyödyntää sen sijaan ei tarvitse olla ilmeinen tai läpinäkyvä muille kuin oikeuden omistajalle. (Janeček 2018, 104)

Käyttäjien yksityisyyttä voidaan kuitenkin suojata oikeuksien kautta vain tiettyyn pisteeseen asti, jos käyttäjä ei itse ole kiinnostunut sen suojaamisesta. Jos käyttäjä on valmis luopumaan osasta yksityisyyttään saamaansa palvelua tai informaatiota vastaan, suostumus viittaa käyttäjän kokevan saavansa vaihtokaupassa enemmän takaisin (Duch-Brown et al 2017, 15). Käyttäjät vaikuttavat kuitenkin toimivan hetken mielijohteen tai esimerkiksi mukavuuden perusteella, koska vaikka käyttäjä sanoisi pitävänsä tietosuojaa ja yksityisyytensä suojelemista tärkeänä, käytännössä henkilötietoja luovutetaan hyvin helposti. Tätä kutsutaan *yksityisyysparadoksiksi*. (Duch-Brown et al. 2017, 34)

5.2 Datan verkostovaikutukset ja kollektiiviset oikeudet

Henkilötiedon määrittelyssä täytyy ottaa huomioon, että henkilötieto liittyy enää harvoin vain yhteen yksilöön (Purtova 2017, 73). Yksilön antama suostumus henkilötietojensa ja erityisesti terveyteen liittyvien tietojensa (erityinen henkilötietoryhmä) kuten geneettisen tiedon käsittelyyn, vaikuttaa myös muihin yksilöihin. Tätä kutsutaan tiedon *verkostovaikutuksiksi* ja ilmiö voi vaikeuttaa todellisen omistusoikeuden ja kontrollin saamista omiin henkilötietoihin. (Purtova 2017, 64, 73) Verkostovaikutuksien myötä henkilötiedosta voi nähdä seuraavan myös vastuuta samalla tapaa kuin

vaikka auton omistaja vastaa autonsa aiheuttamista vahingoista (Janeček 2018, 1044). Puettavan älylaitteen käyttäjälle tämä voisi näyttäytyä esimerkiksi käyttäjästä kerättynä terveyteen liittyvänä tietona, joka big data-analytiikan myötä paljastaisi käyttäjän periytyvän sairauden ja sitä kautta informaatiota myös ylös- ja alaspäin sukupolvissa.

Ongelmaan on esitetty ratkaisuksi datan omistusoikeuden kollektiivista järjestämistä, jossa datan omistusoikeuksia hallittaisiin hajautetusti, kuten monia muitakin jakamistaloudessa olevia hyödykkeitä nykyään (Singh & Vipra 2019, 1). Puettavien laitteiden käyttäjille kollektiivinen omistusoikeus voisi tarkoittaa esimerkiksi käyttäjäyhteisöä MyData-idean pohjalta. Singh & Vipra (2019, 2;4) katsovat, että yhteisöllinen omistus on tulevaisuudessa relevantimpi tapa järjestää oikeudet, koska datan fokus siirtyy tulevaisuudessa yhä enemmän yksilön henkilötiedoista yhteisöä koskeviin tietoihin kuten älykaupunkien keräämään dataan, mutta myös siksi, että yksilön mahdollisuudet hyödyntää dataan liittyviä oikeuksia eivät ole osoittautuneet toimiviksi. Myös Thouvenin et al. (2017, 137) mielestä datan omistajan määrittely on niin vaikeaa, että parempi ratkaisu olisi määritellä omistus kollektiivisena. Jotta omistusoikeus voitaisiin myöntää ryhmälle ja oikeuksia hyödyntää, ryhmän pitäisi olla määriteltävissä ja melko pysyvä (Purtova 2017, 78). Datan prosessoinnin läpinäkymättömyys ja verkostovaikutukset tekevät omistusoikeuden säätämisestä vaikeaa, koska omistusoikeus vahvana oikeutena kaikkia muita vastaan vaatii oikeuksien julkistamista, jotta kaikki voivat tietää kuka omistaa ja mitä (Purtova 2017, 73-74). Lisähaasteensa tuo verkostovaikutusten muuttuminen aikaa myöten ja vaikutusten alaisen ryhmän määrittely, joka on vaikeaa samalla tavalla kuin datan määrittely yksilöä koskevaksi (Purtova 2017, 77).

Janečekin (2018, 1045) mukaan keskustelussa pitäisi erottaa datan suoja omistusoikeuden kohteena ja data henkilökohtaisen informaation ja persoonallisuusoikeuksien välineenä. Tietosuojalainsäädännön taustalla on yksityisyydensuojan intressit ja myös Drexlin (2018, 3) mielestä sen pohjalta tai sen perusteella ei voida rakentaa datan omistusoikeuden sääntöjä.

6 Datan hallinnan asiantuntijanäkökulma

6.1 Asiantuntijahaastattelut

Terveysdatan oikeuksien nykytilannetta ja erilaisia hallintamallien mahdollisuuksia tarkasteltiin puolistrukturoiduissa teemahaastatteluissa, joissa haastateltiin kuutta datan hallinnan ja oikeuksien asiantuntijaa eri erityisaloilta. Haastatteluissa käytiin läpi puettavilla laitteilla kerätyn terveysdatan oikeuksien hallintaa nykytilanteessa sekä kahta mahdollista vaihtoehtoista hallintamallia: omistusoikeutta ja ihmiskeskeisiä datan hallintamalleja. Haastattelujen teemoina olivat mallien vaikutukset yksilön oikeuksiin, yritysten toimintaympäristöön sekä yhteiskunnalliseen etuun ja oikeudenmukaisuuteen. Haastatteluissa käytiin läpi puettavilla älylaitteilla kerätyn terveysdatan oikeuksien

- nykytilannetta eli oikeuksien hallintaa käyttöehtosopimuksilla ja suostumusperusteisesti, perustuen edellä luvuissa 1-5 läpikäytyihin lakeihin, säädöksiin ja kirjallisuuteen
- hallintaa mahdollisen omistusoikeuden kautta, perustuen edellä läpikäytyyn tieteelliseen keskusteluun sekä lakeihin ja säädöksiin
- hallintaa ihmiskeskeisten hallintamallien kautta, käyttäen esimerkkeinä MyData-ideaa ja Sitran IHAN-standardihanketta
- datan hallinnan tulevaisuuden näkymiä

Haastattelut olivat noin tunnin pituisia ja ne tallennettiin sanelimelle, mihin oli kysytty haastateltavilta lupa. Haastattelut litteroitiin kokonaisuudessaan ja puhekielisinä. Litteroinnista jätetiin pois vain toistettuja täytesanoja. Haastateltavien sitaateista kaikki täytesanat on kuitenkin jätetty pois, koska tutkimuksen fokuksessa eivät ole haastateltavat yksityishenkilöinä ja persoonina, vaan heidän asiantuntijaroolinsa ja -näkemyksensä, joihin ne eivät tuo lisäarvoa. Sitaateista on voitu jättää myös pidempiä osia pois, jotta esitys olisi mahdollisimman tiivis. Editoinnissa on pyritty kuitenkin säilyttämään haastateltavan sanoman ydin. Yksi haastattelu tehtiin ja myös litteroitiin englanniksi. Suomennokset on tehty vasta kirjoitusvaiheessa.

6.1.1 Tutkimusmenetelmän valinta

Haastattelut ovat valittu menetelmäksi, koska datan omistusoikeuksiin liittyvää tieteellistä kirjallisuutta ja tutkimusta on suomeksi vähän ja haastatteluilla voidaan saada ajankohtaista tietoa datan oikeuksista, joihin liittyvä teknologinen ulottuvuus muuttuu nopeasti. Tieteelliset julkaisut

seuraavat jopa vasta vuosien päästä siitä, kun aihe on ollut tutkijalla työstettävänä, eikä kaikki käytännön tieto tai ns. hiljainen tieto edes välity julkaisuissa tai yleensä päädy julkiseksi (Gillham 2005, 56-57). Puolistrukturoitu teemahaastattelu on valittu aineiston keruun menetelmäksi sen joustavuuden takia, ja koska valittavien haastateltavien voidaan asiantuntemuksensa perusteella odottaa tuntevan käsiteltävän teeman aihepiirin ja sen käsitteet (Tuomi & Sarajärvi 2002, 79). Teemaan liittyviä kysymyksiä voidaan näin käsitellä joustavasti haastateltavan erityisasiantuntemuksen aluetta myötäillen. Haastateltavia voidaan pitää asiantuntijataustansa puolesta ns. eliittihaastateltavina, jotka tuntevat aihealueen vähintään osittain haastattelijaa paremmin, ja pystyvät näin hahmottamaan käsitteet ja kysymyksenasettelut kriittisesti (Gillham 2005, 54). Tämän vuoksi on perusteltua, että asiantuntijat voivat halutessaan ohjata keskustelua näkemyksensä mukaisesti relevanttiin suuntaan (Gillham 2005, 54).

Haastateltaviksi on valittu datan hallinnan asiantuntijoita eri erityisalueilta, jotta kuva datan oikeuksien hallinnan nykytilasta ja arvio datan oikeuksien kehityksestä olisi mahdollisimman monipuolinen ja kattava. Haastateltavien valinta on tehty osin eliittiotannalla ja osin lumipallo-otannalla. Eliittiotannassa haastateltavat valitaan sen perusteella, keneltä on arvioitu saatavan parhaiten tietoa tutkittavaan aiheeseen ja ilmiöön (Tuomi & Sarajärvi 2002, 88). Lumipallo-otantaa on käytetty valitsemalla asiantuntijoiden itsensä suosittelemia henkilöitä (Tuomi & Sarajärvi 2002, 88). Muutaman kerran suositeltiin samoja henkilöitä, joita oli jo suunniteltu tai kysytty haastateltaviksi, minkä voi nähdä viittaavan pieneen määrään spesifin alueen – datan oikeuksien hallinnan – asiantuntijoita. Osa haastateltavista on organisaatioidensa puolesta joidenkin ryhmien edunvalvojia, mutta eri näkökulmien kattamiseksi tämä on tutkimuksen kannalta tarkoituksenmukaista. Haastattelussa täytyy ottaa huomioon, että jonkin ryhmän edustajana identifioidun asiantuntijahaastateltavan mielipiteet, varomattomat lausumat tai haastattelijan väärinymmärrykset voivat johtaa ongelmiin (Gillham 2005, 55). Toisaalta tiettyjä tahoja tai organisaatioita edustavien eliittihaastateltavien tulkinnassa täytyy ottaa huomioon haastateltavan motiivit heidän sanomansa tai mahdollisten pidättyvien kannanottojen takana (Gillham 2005, 58). Tämän vaikutusta pyritään vähentämään aineistotriangulaatiolla eli vertaamalla aineistoa muista lähteistä saatavaan tietoon, mikä lisää tulosten luotettavuutta (Eskola & Suoranta 1999, 69).

6.1.2 Tutkimuksen toteutus ja analyysi

Kaikilta haastateltavilta on kysytty lupa ja he ovat suostuneet nimensä julkaisuun. Haastattelut tehtiin touko-kesäkuussa 2020 puhelu- tai videopuheluyhteydellä. Haastateltaville lähetettiin ennen

haastattelua kysymysrunko, jossa määriteltiin tutkimuksen lähtökohdat, tärkeimmät määritelmät ja kysymyslista. Listan kysymykset vaihtelivat henkilöstä ja haastattelusta toiseen jonkin verran, koska oleelliset näkökulmat tarkentuivat haastatteluiden myötä, ja niissä pyrittiin käymään läpi haastateltavan erikoisosaamisalaa. Mainitut teemat eli datan eri hallintamallien vaikutukset

- yksilön oikeuksiin
- yritysten toimintaympäristöön ja vapaaseen kilpailuun sekä
- yhteiskunnalliseen etuun ja oikeudenmukaisuuteen

pysyivät joka haastatteluissa samana ja niitä käsiteltiin joka haastattelussa. Kaikkia listan kysymyksiä ei ehditty käymään läpi kaikissa haastatteluissa. Haastatteluiden kysymyksissä pyrittiin käymään läpi edellä luvuissa 1-5 esiin nousseita ongelmia ja havaintoja. Haastatteluajan rajallisuuden vuoksi useimmissa haastatteluissa painottui kaksi ensimmäistä teemaa.

Koska tietosuoja ja siihen liittyvä lainsäädäntö on keskeinen osa puettavien älylaitteiden käyttäjän oikeuksia, tietosuojavaltuutettu Reijo Aarniota pyydettiin haastateltavaksi vastaamaan kysymyksiin käyttäjän oikeuksien ja tietosuojan näkökulmasta. Haastateltavista lainsäädännön asiantuntijoita ovat myös IP-asiantuntija ja tutkija, juristi Pekka Tarkela sekä Elinkeinoelämän keskusliiton yrityslainsäädäntö- ja tietosuoja-asiantuntija, juristi Sanna-Maria Bertell. Ihmiskeskeisen datatalouden näkökulmaa edustavat Hannu Hämäläinen ja Antti Poikola, jotka vastasivat kysymyksiin kuitenkin oman harkintansa mukaan yksityishenkilöinä. Hannu Hämäläinen työskentelee Sitrassa vanhempana neuvonantajana, erityisalanaan terveys- ja hyvinvointidatan hyödyntäminen ja on IHAN-hankkeen eli *reilun datatalouden periaatteiden* asiantuntija. Tutkija, ohjelmistokehittäjä ja datatalouden asiantuntija Antti Poikola on tunnettu MyData-aktiivina ja työskentelee yhtenä vetäjänä Teknologiateollisuuden Tekoälykiihdyttämö FAIA:ssa. Taloustieteellistä näkökulmaa edustamaan haastateltavaksi pyydettiin digitaalitalouden ja innovaatiopolitiikan asiantuntija ja Euroopan komission yhteisen tutkimuskeskuksen (JRC) Sevillan yksikön tutkija Néstor Duch-Brown.

Haastatteluaineistoa analysoitiin *teemoittelemalla* eli etsimällä aineistosta monen haastateltavan esille tuomia aiheita sekä niiden *tarkastelemalla näiden yhteyksiä* (Hirsjärvi & Hurme 2000, 173;174). Osaltaan tämä tapahtui luonnostaan, koska kyseessä oli teemahaastattelu ja haastateltavat tiesivät teemat ennalta. Esille nousi kuitenkin myös teemojen ja kysymysten ulkopuolisia näkökulmia, koska haastateltavia kannustettiin käsittelemään heidän näkemyksensä mukaisia

relevantteja asioita, joita ei ollut kysymyksissä käsitelty. Jo litteroinnin aikana aineistosta nousi esiin aiheita, joissa haastateltavien mielipiteet olivat erityisen kaukana toisistaan. Analyysiä jatkettiin lukemalla litteroidut haastattelu useaan kertaan läpi ja korostamalla aineistosta tutkimuksen ja tutkimuskysymysten kannalta oleellisia kohtia. Analyysi on ollut myös erottamaton osa itse kirjoitusprosessia. Tulokset on järjestetty haastattelun teemoja mukaillen.

6.1.3 Tutkimuksen luotettavuus

Haastattelussa pyrittiin saamaan mahdollisimman kattava ja monipuolinen kuva puettavilla älylaitteilla kerätyn terveysdatan oikeuksien hallinnan nykytilasta ja tulevaisuuden näkymistä. Tätä varten haastateltaviksi valittiin datan hallinnan asiantuntijoita eri organisaatioista ja erityisaloilta. Datatalous ja datan oikeudet koskettavat kuitenkin niin montaa eri alaa ja sidosryhmää, että näkökulmia löytyisi varmasti lisääkin. Myös aineiston riittävyys vaikuttaa tutkimuksen validiteettiin (Eskola & Suoranta 1999, 215). Haastateltavien suhteellisen pieni määrä lisäsi tältä osin riskiä yksittäisten haastateltavien voimakkaasta vaikutuksesta tuloksiin. Toisaalta haastatteluissa nousivat esiin spontaanisti ja toistuvasti tietyt seikat, mikä viittaa aineiston ainakin osittaiseen saturaatioon. Terveysdataan ja sen hyödyntämiseen liittyy myös vahva poliittinen aspekti. Tämän vuoksi tulosten tulkinnassa täytyy ottaa huomioon asiantuntijahaastateltavien mahdolliset poliittiset näkökannat (Gillham 2005, 59). Tämän vaikutusta pyrittiin minimoimaan aineistotriangulaatiolla.

Tutkimuksen luotettavuutta aineiston teknisessä käsittelyssä lisää se, että haastattelut litteroitiin mahdollisimman pian haastattelujen jälkeen ja tallenteista sai hyvin selvää. Epäselväksi jääneitä, aineiston sisältöön liittyviä asioita selvennettiin sähköpostilla jälkikäteen. (Hirsjärvi & Hurme 2000, 184-185) Haastattelurungon osalta luotettavuutta vähentää eri haastateltavien toisistaan jonkin verran poikkeavat kysymykset. Tämä oli kuitenkin monipuolisten kuvan saamiseksi ja haastateltavien erityisosaamisen hyödyntämiseksi perusteltua. Tulkinnallista riskiä lisää se, että haastateltavat puhuivat eri yhteyksissä terveysdatasta ja osin datasta yleensä. Osa käsitteistä selitettiin haastattelurungossa, jotta tutkimuksen lähtökohdat olisivat mahdollisimman selkeät (Hirsjärvi & Hurme 2000, 184). Tutkimuksen aikana kävi kuitenkin ilmi, että samat käsitteet voivat merkitä esimerkiksi juridisesta ja teknisestä näkökulmasta hieman eri asioita. Koska kaikki haastateltavat kuitenkin työskentelevät datan hallinnan tai oikeuksien parissa, erilaisia käsitteellisiä tulkintoja voi pitää pienenä tai kohtuullisena riskinä.

Hirsjärvi ja Hurme (2000, 186) ovat huomauttaneet, että reliaabelius ja validius ovat käsitteinä peräisin kvantitatiivisesta tutkimuksesta, eivätkä ne ole välttämättä täysin sovellettavissa kvalitatiiviseen tutkimukseen. Tämä johtuu heidän mukaansa ihmisen käyttäytymisen muutoksista eri tilanteissa ja eri aikoina. Tämän voi arvioida koskevan myös asiantuntijahaastatteluja, vaikka kaikki osapuolet pyrkisivät neutraaliuteen ja objektiivisuuteen. Koska datan ja terveysdatan hallinta on jatkuvassa muutoksessa aiheena ja tutkimuskohteena, myös henkilöiden näkemykset ja asenteet voivat muuttua suhteellisen piankin uusien tutkimustulosten myötä. Tutkimuksen tuloksia voi sen vuoksi ajatella tekijän tulkintana datan asiantuntijoiden *tämän hetkisestä* näkemyksestä datan oikeuksien hallintaan.

6.2 Datan hallinnan nykytilanne

6.2.1 GDPR:n vaikutukset

Koska GDPR on tällä hetkellä tärkeimpiä datan oikeuksia määritteleviä säädöksiä, on perusteltua tarkastella, miten GDPR on vaikuttanut käyttäjän oikeuksien toteutumiseen ja yritysten toimintaympäristöön käytännössä. Haastateltavien näkemykset GDPR:n vaikutuksista yksilöiden käytännön oikeuksiin eroavat jonkin verran toisistaan. Yhteistä useimmille näkemyksille on se, että GDPR:n nähdään lisänneen ihmisten tietoisuutta henkilötietojensa käytöstä, mutta asetus nähdään vasta yhtenä pienenä askeleena kohti yksilön henkilötietojen parempaa hallintaa. Bertell tiivistää asian näin:

> *[...] vois sanoo näin et GDPR on vielä kuitenkin tavallaan [...] semmosessa lastentautivaiheessa, että ylipäätään ennen kuin [...] tietosuoja-asetus on todella operationaalinen, niin meidän pitää varmaan mennä tietty määrä tämmösiä [...] muutossyklejä läpi ja ne muutossyklit tulee sit vaan sieltä oikeuskäytännön [...] ja viranomaisohjeistuksen kautta ja me ollaan [...] tavallaan vielä sillä matkalla [...]et [...] on ihan varmasti paljon semmosta, mitä ei olla vielä tavallaan ajateltu kysyäkään, et kaikkia niitä oikeuksia ei olla vielä testattu käytännössä.*

Bertell kuitenkin mainitsee GDPR:n tuomaksi eduksi käyttäjän kannalta käyttötarkoitussidonnaisuuden, joka on rajannut palveluntarjoajan mahdollisuutta laajentaa datan käyttötarkoitusta niistä, mitä suostumuksen yhteydessä on mahdollisiksi käyttökohteiksi mainittu.

Sekä Bertell, Hämäläinen että Aarnio mainitsevat käyttäjän asetuksen antamista oikeuksista siirrettävyyden ja sen toteutuksessa olevat ongelmat. He korostavat siirrettävyyden puutteellisuutta nykytilanteessa. Siirrettävyys antaa käyttäjälle oikeuden siirtää hänestä kerätyt tiedot *”jäsennellyssä, yleisesti käytetyssä, koneellisesti luettavassa ja yhteentoimivassa muodossa”* esimerkiksi palveluntarjoajalta toiselle (GDPR johdanto-osa 68). Aarnion mukaan yritykset eivät halua siirtää asiakasdataa toisille yrityksille asiakkaan tietosuojaan vedoten, mikä hänen mukaansa ei ole pätevä syy.

Bertell nostaa siirrettävyyden käytännön ongelmaksi datan laadun ja syvyyden rajaamisen, mitä käyttäjä saisi viedä mukanaan. Hänen mukaansa henkilötietoa sisältyy moniin yritykselle tärkeisiin järjestelmän osiin kuten IPR:ään. Hän pitää epäreiluna, jos kaikki henkilötietoon liittyvät osat kuten aineettomat oikeudet olisivat siirrettävissä.

[…] mun on myöskin vaikea nähdä, et miten se sitten käytännössä tapahtuis, koska nää pitäis varmaan olla jossain […] reaaliaikaisessa, koneluettavassa muodossa, et siitä olis mitään järkeä siirtää tämmöstä, niin sitten näiden palveluntarjoajien pitäis […] rakentaa tällaset rajapinnat sinne ja […] se tois tietenkin sit erityyppisiä liiketoimintamalleja, mut voin myöskin nähdä et tää mahdollisesti tuo lisäkustannuksia siihen.

Bertellin mukaan käyttäjän mahdollisuus esimerkiksi siirtää harjoittelutietonsa älykellosta toiseen tuo käyttäjälle melko pienen hyödyn verrattuna siirrettävyyden käytännön toteutuksen työläyteen. Siirrettävyyden mahdollistavien rajapintojen toteutuksen kustannukset voisivat myös nostaa puettavien älylaitteiden hintoja, mikä vaikuttaisi näiden yritysten kilpailukykyyn. Toisaalta Bertell näkee täydellisessä siirrettävyydessä riskin kilpailun häviämisestä, kun yrityksiltä häviäisi kannustimet innovoida. Bertell kuitenkin kannattaa rajapintojen kehittämistä julkisen sektorin dataan, jotta pystyttäisiin kehittämään niihin perustuvia palveluita.

GDPR:n 20 artiklan mukaan käyttäjällä on oikeus saada ja siirtää omat henkilötiedot, ”*jotka hän on toimittanut rekisterinpitäjälle*”. Tämä koskee esimerkiksi sykettä ja muuta laitteen mittaamaa dataa. Monimutkaisempaa on tulkita, koskeeko oikeus myös informaatiota, joka on *ennustettu* tai *arvioitu* kerätyn datan perusteella, kuten käyttäjän sairastumisriskiä tai eliniänodotetta. Malgieri & Comandé (2017, 232) ovat arvioineet, että käyttäjällä ei ole oikeutta siirtää tällaista dataa mukanaan. Aarnion mukaan asiasta on ristiriitaisia näkemyksiä. Hänen mukaansa Euroopan tietosuojaneuvosto on kallistunut siirrettävyyden puoltamiseen, kun taas teollisuus vastustaa sitä. Aarnio arvioi, että siirrettävyys on paremmin perusteltavissa, jos palvelun tarkoitus on nimenomaan tuottaa tietoa ennustamiseen. Puettavissa älylaitteissa tällaisten ominaisuuksien voi arvioida olevan juuri yksi syy ostaa ja käyttää laitteita. Aarnio kuitenkin viittaa, että asiasta ei ole vielä tuomioistuimen tulkintaa. (Aarnio 9.6.2020, asiaa tarkennettu sähköpostilla)

Aarnio näkee tietosuojavaltuutettuna tietosuoja-asetuksen vaikutukset yleisesti ottaen haastateltavista positiivisimmin. Hänen mielestään käyttäjän oikeudet on parantuneet, entistä laajemmat ja viranomaisten tuella toimeenpantavissa. Hän nostaa esille GDPR:n tuomana oikeutena siirrettävyyden ohella 3 artiklan, joka suojaa käyttäjää myös niitä yrityksiä kohtaan, jotka tarjoavat palveluita eurooppalaisille, vaikka eivät olisi etabloituneet Eurooppaan. Lisäksi hän nostaa asetuksen tuomana etuna viranomaisten paremmat toimivaltuudet ja tietosuojaviranomaisten keskinäisen päätöksentekomekanismin. Toisaalta hän näkee eurooppalaisessa yhteistyössä haittana sen, että päätöksenteko voi hidastua ja loitontua asioissa, joissa ei ole enää kansallista liikkumavaraa. Aarnion mukaan tietosuoja-asetus oli alun perin osa Euroopan unionin strategiaa edistää sisämarkkinoiden

kauppaa ja harmonisoida kuluttajakauppaan liittyvää tietosuojasääntelyä 2010 finanssikriisin jälkimainingeissa. Hänen mukaansa asetuksella oli kilpailuoikeudellinen aspekti, mutta samalla halutiin suojata yksilön oikeudet eurooppalaisiin arvoihin nojaten. Myös Aarnion mielestä asetuksen soveltaminen on osin vielä kesken.

Tietosuoja-asetus antoi kansalliselle *seuraamuskolleegiolle* valtuudet määrätä hallinnollisia sakkoja organisaatioille ja yrityksille vakavista tietosuojarikkomuksista (TSV 2019). Seuraamusmaksu voi olla enimmillään 4 % liikevaihdosta tai 20 miljoonaa. Tietosuojavaltuutetun toimiston seuraamuskolleegio määräsi toukokuussa 2020 ensimmäiset seuraamusmaksut tietosuojarikkomuksista Suomessa. Seuraamusmaksuja sai kolme määräyksiä rikkonutta yritystä, joille määrätyt summat vaihtelivat välillä 12500 - 100 000 euroa. Suurimman seuraamusmaksun sai Posti Oyj, joka oli informoinut puutteellisesti asiakkaitaan heidän oikeuksistaan kieltää tietojensa luovutus. (TSV 2020) Tämä on huomionarvoista siinä mielessä, että Posti on yksi MyData Global-organisaation jäsenistä, jotka ovat sitoutuneet edistämään yksilön oikeutta omiin henkilötietoihinsa (MyData.org 2020). Tämä voi kertoa siitä, että myös suurissa yrityksissä on haasteita noudattaa asetuksen määräyksiä käytännössä tai vaihtoehtoisesti MyDatan kannattamisesta pinnallisesti pr-mielessä.

Hämäläinen näkee GDPR:n ongelmana eri jäsenmaissa olevat erilaiset käytännöt ja tulkinnat, mutta näkee puutteiden paikkaamiselle myös nopeampia vaihtoehtoja yrityskentän sisällä:

> *[…] GDPR on ihan hyvä, mut siitä pitäis kehittää ja toinen kysymys on tietenkin, et kumpaas kautta tää nyt sit oikein sit etenee, et voiko tää edetä myöskin sillai, et syntyy sellaista code of conductia tai […] toimialojen välistä sopimista, joka on ketterämpi ja nopeampi tapa sitten kuin tämmöinen säännöstie, et tässä on tietyllä tapaa varmaan kaks tietä, jolla voidaan edetä.*

Tarkelan näkemys GDPR:n tuomista hyödyistä on kriittisempi. Hänen mielestään asetus on johtanut yksilön tiedostumiseen henkilötietojensa käytöstä ja yksilön emansipaation kasvamiseen, mutta käytännön hyödyt hän näkee vähäisempinä:

> *[…] ei ole oikeastaan yksilötasolla johtanut mihinkään sen kummempaan vielä, tietysti yksilö on paremmin suojattu […] se iso kysymys on kuitenkin se, että onko julkisoikeudellinen lainsäädäntöinstrumentti semmoinen vekotin, jolla voidaan ylipäätänsä yksilötasolla antaa riittäviä toimintamahdollisuuksia, mitä […] datasta disponoimiseen tulee. […] itse edustan vähän sitä kantaa, että ei voida. […] olen ollut*

sitä mieltä, että se ison kysymyksen pitäis olla GDPR:n ohella se, että miten datan sääntely kytketään osaksi yksityisoikeudellista sääntelymaastoa.

Poikolan näkemys GDPR:n käytännön vaikutuksista on vieläkin kriittisempi:

[…] tietosuoja-asetus on ollut ehkä […] suurimpia kansanvalitushankkeita lainsäädännön muotoon puettuna, et sehän ei sinänsä montaakaan perusprinsiippiä edes muuttanu siitä, mitä on ollu […] 95 lähtien voimassa direktiivin puitteissa, mutta […] et siitä on tullut asetus, jossa on sanktiot ja jota on puhuttu ja myllerretty tosi paljon, niin nyt yhtäkkiä sitten 20 vuoden jälkeen ihmiset tietää, et niillä on niitä oikeuksia, mitä niillä on ollut aikaisemminkin […] et se on ehkä se suurin muutos.

Poikola katsoo, että GDPR tai sen tuoma datan siirrettävyys ei anna vielä juurikaan työkaluja myöskään datan hyödyntämisen:

[…] niin kun nimikin sanoo, niin se on tietosuoja-asetus, et se lähtee siitä, että vältetään […] datan väärinkäyttöä ja pyritään […] minimoimaan siitä aiheutuneita harmeja […] tää data portability-pykälä 20, joka on nyt ehkä ensimmäinen viite siihen suuntaan, et […] dataa vois hyödyntää muuallakin kuin siellä, missä se alun perin on kerätty, mutta […] se ei […] sinänsä palvele vielä hirveen hyvin […] datan uudelleenkäyttöä, joka sit taas edellyttäis sitä, et ois […] rajapintoja ja tän tyyppistä ja […] on ehkä nyt […] havahduttu siihen, […], että tämmöstä […] nimenomaan datan hyödyntämistä tukevaa lainsäädäntöä syntyis[…]

Bertellin mukaan GDPR on lisännyt yritysten hallinnollista kuormaa, epävarmuutta ja tulkintahaasteita sekä aiheuttanut kustannuksia ja nostanut kynnystä innovoida ja hyödyntää innovaatioita. Hänen mukaansa kustannuksia on tuonut muun muassa asetuksen mukanaan tuoma uusi ammattiryhmä eli yritysten tietosuojavastaavat. Aarnio sen sijaan näkee GDPR:n Euroopan kilpailuetuna, ja kuluttajien luottamuksen vahvistaminen olevan globaali megatrendi, jonka perässä myös muut maat kuten Japani, Intia, Kiina sekä Yhdysvalloissa Kalifornia tekevät omia sovelluksiaan tietosuoja-asetuksesta.

Myös Duch-Brown näkee GDPR:lla olleen *odotetusti* negatiivinen vaikutus eurooppalaisiin markkinoihin, yrityksiin ja investointeihin lyhyellä aikavälillä. Hänen mukaansa järjestelmien muuttaminen ja muu määräysten noudattaminen on lisännyt kustannuksia, mikä on mahdollisesti vähentänyt Euroopan houkuttelevuutta sijoituskohteena. Hänen mielestään tärkeämpiä ovat kuitenkin pidemmän aikavälin *sekundääriset* vaikutukset, koska sopeutuminen uusiin sääntöihin ja uuteen järjestelmään tuo mukanaan innovaatioita organisaatioiden ja prosessien tasolla. Hänen mukaansa GDPR:n kokonaisvaltaisempia vaikutuksia voi tarkastella vasta 5-10 vuoden sisällä ja niiden nettovaikutus on hänen arvionsa mukaan positiivinen.

Duch-Brownin mukaan datataloudessa on vieläkin niin paljon epävarmuutta ja tuntematonta maaperää, että sääntely perustuu jossain määrin kokeiluille. Hän katsoo, että sääntely kuten GDPR on yrityksen ja erehdyksen politiikkaa: tehdään sääntöjä, tarkastellaan toimijoiden reagointia ja tehdään muutoksia vaikutusten perusteella.

6.2.2 Datan anonymisointi

Tutkimuksessa on aiemmin käsitelty näkemyksiä (e.g. Kauffman & Soares 2018, 531; Singh & Vipra 2019, 2), joiden mukaan anonymisointi kaventaa käyttäjän todellisia oikeuksia henkilötietoonsa, koska anonymisoinnin myötä käyttäjä ei voi enää käyttää GDPR:n tuomia oikeuksia terveysdataansa, vaikka käytännössä siitä monessa tapauksessa on vielä yksilö tunnistettavissa. Yhdysvalloissa tehdyssä tutkimuksessa (Emam et al. 2011, 8) pystyttiin tunnistamaan noin joka kolmas henkilö tunnistamattomaksi muokatusta – tai sellaiseksi luullusta – terveysdatasta. Haastateltavilta kysyttiin kuinka isona ongelmana he pitävät anonyymin ja henkilötiedon rajan häilyvyyttä käyttäjän ja yhteiskunnan kannalta. Tarkelan näkemys on haastateltavista kaikkein kriittisin:

> *[…] koko tää anonymisointi/de-anonymisointi-taistelu muistuttaa mun mielestä hieman panssarivaunun ja panssaritorjunnan suhdetta. Jos panssarivaunut on anonymisointi, niin kyllä ne on jollakin tasolla tuomittu häviämään sen jutun. Kaikki panssarointi voidaan murtaa. Ja ne taloudelliset insentiivit, joka tukevat anonymisoidun henkilötiedon de-anonymisoimista, niin taloudelliset intressit on niin valtavia, että mitä yksilön oikeuksien ja yksilön suojaamiseen tulee, niin tilannehan on ihan älyttömän kehno. Se on mun mielestä GDPR:n välttämätön, mut todella valitettava valuvika, koko tietosuojan itseasiassa, että se ei kykene estämään sitä […] Että GDPR on hoitanut tosi pienen siivun mielestäni tästä asiasta, jos ajattelee nimenomaa yksilönä, määräysvaltaa ja yksilön suojaamista.*

Bertellin mukaan anonymisoidun ja pseudonymisoidun datan raja ja sen tulkinta on nykytilanteessa niin häilyvä, että kaikkea dataa kannattaa käytännössä käsitellä siinä mielessä, että se on pseudonymisoitua ennemmin kuin anonyymiä. Hänen mukaansa nykytilanteeseen vaaditaan jonkinlaista apua viranomaisilta, kuten ennakkotapauksia, jotka selkeyttäisivät tulkintaa:

> *…mun mielestä tää on epätyydyttävä asiantila […] Et tällä hetkellä kukaan ei uskalla sanoa, et missä se raja kulkee.*

Hämäläinen katsoo, että anonymisointi ja datan hyödynnettävyys ovat asian kaksi eri puolta, joiden välillä käydään koko ajan tasapainoilua. Hänen mukaansa on keskeistä kuitenkin pystyä

hyödyntämään dataa, muuten sen keräämiseen tehdyt panostukset ja datan sisältämä potentiaali menevät hukkaan. Hämäläisen mukaan yksityisyydensuoja on hyvin tärkeä perusoikeutena, mutta se pitäisi suhteuttaa hyödyn ja muiden oikeuksien, kuten hyvinvoinnin, työn ja terveyden kanssa. Hänen mukaansa keskeistä anonymisoinnissa on datan hyödyntäjän velvollisuudet ja etiikka. Käyttäjän luottamus terveysdatan hyödyntämiseen tulisi säilyttää yhteisten sopimusten, kuten tilastoeettisten sääntöjen avulla, ja jos sääntöjä rikotaan, rikkomuksille täytyisi olla rangaistus. Hän viittaa yhtenä yksilön oikeuksia varmistavasta ratkaisusta sosiaali- ja terveysalan lupaviranomaista Findataa varten kootusta asiantuntijaryhmästä, joka vastaa kansalaisten terveystietojen hyödyntämisen tietosuojaan, tietoturvaan ja anonymisointiin liittyvistä kysymyksistä.

Yhtenä rangaistuksena henkilötietojen väärinkäytöstä voisi olla edellä mainittu seuraamuskolleegion antama seuraamusmaksu. Aarnio pitää hallinnollisten sakkojen määräämistä puutteellisesti anonymisoidulle tiedoille mahdollisena, jos rikkomus esimerkiksi on toistuva. Hän on kuitenkin lausumassaan pidättyväinen, kenties Bertellin kuvaaman anonymisoinnin epäselvyydestä johtuen. Aarnio painottaa anonymisoidun datan tarkoittavan kuitenkin lainsäädännön tasolla dataa, josta *ei voi* tunnistaa yksilöä, ja sellaisen datan olevan tietosuojasääntelyn ulkopuolella.

Duch-Brown mukaan riski henkilötietojen väärinkäytöstä on olemassa, mutta panostuksilla datan turvalliseen käsittelyyn riskiä voidaan minimoida. Yleisesti ottaen hän ei pidä tunnistettavuutta anonymisoidusta tiedosta ongelmana, koska dataa tarvitseva tahot, kuten yritykset eivät ole kiinnostuneita yksilöstä persoonana, vaan hänen ominaisuuksistaan kuluttajana.

Poikolan näkemys terveysdatan anonymisoinnin ongelmiin on liberaalein. Hän vertaa tietosuojaa datan ”vankilaan”, jossa on hyvä olla suojassa, mutta vaikea tehdä mitään. Hänen mielestään asiaa pitäisi katsoa ennemmin datan hyödynnettävyyden näkökulmasta: mitä vahvemmin data on anonymisoitu, sitä vähemmän sitä voidaan hyödyntää, erityisesti käyttäjän näkökulmasta:

> *[…] ennen kaikkea se ei auta sitä ihmistä itteään useinkaan kovin paljoa, että hänen dataansa käytetään anonyymissä muodossa jossain, vaan silloin se hyöty menee jollekin muulle, joka on kerännyt sen datasetin ja anonymisoinut sen ja tekee sillä jotain […] me (huom. MyData) […] pyritään siihen, et henkilötietoa voisi käyttää […] ihmisten omasta toivomuksesta ja heille hyödyllisiin asioihin, et mä nään […] sen koko anonymisointikeskustelun […] tietyl taval semmosena, vähän […] turhanakin vääntönä, koska niin paljon olis saavutettavissa sillä, että pystytään […] luotettava tiedonkäsittely tuomaan sille puolelle, missä ei tarvitse anonymisoida.*

6.2.3 Käyttäjän taloudelliset oikeudet

Suurin osa haastateltavista suhtautuu kriittisesti käyttäjän mahdollisuuteen hyötyä taloudellisesti omasta terveysdatastaan. Hämäläisen, Bertellin, Duch-Brownin ja Poikolan mielestä se ei toimisi, koska yksittäisen henkilön terveysdatankaan arvo on hyvin pieni ja suurin arvo syntyy jalostuksen myötä. Heidän mukaansa käyttäjän saama arvo datasta tulee parempien palveluiden ja paremmin räätälöityjen tuotteiden myötä.

Aarnio suhtautuu käyttäjän taloudellisiin oikeuksiin varovaisen myönteisesti ja viittaa aiemmin käsiteltyyn digitaalisen sisällön direktiiviin, jossa mainitaan, että digitaalisista palveluista voidaan maksaa rahalla tai henkilötiedoilla. Hänen mielestään GDPR:ää laajemmassa sääntelykehikossa tunnustetaan jo datan taloudellinen arvo. Aarnio ei kuitenkaan suoraan viittaa käyttäjän rahalliseen kompensaatioon.

Bertellin mielestä käyttäjän saama rahallinen kompensaatio ei toimisi käyttäjälle kannustimena jakaa dataa ja hänen mukaansa sellaiseen malliin on todennäköisesti myöhäistä pyrkiä enää tässä vaiheessa. Hän arvioi, että jos yhden ihmisen datalla olisi todellinen arvo, sille olisi jo syntynyt markkinat. Bertell kuitenkin arvioi internetin ansaintalogiikan muuttuvan tulevaisuudessa merkittävällä tavalla, viitaten esimerkkeinä Digital Services Actiin ja ePrivacy-asetukseen. Digital Services Act (DSA) on Euroopan komission suunnittelema viitekehys, jonka tarkoitus on edistää Euroopan yhteismarkkinoilla digitaalisten palveluiden kehitystä ja innovointia sekä edistää vapaata ja reilua kilpailua sähköisillä alustoilla (EU COM 2020a). Sähköisen viestinnän tietosuoja-asetus eli ePrivacy-asetuksen tarkoitus on taas *”lisätä luottamusta digitaalipalveluihin ja parantaa niiden turvallisuutta”* sekä *”tarjota korkeatasoinen yksityisyyden suoja sähköisten viestintäpalvelujen käyttäjille ja tasapuoliset toimintaedellytykset kaikille markkinatoimijoille”* (EU COM 2017c). Kummallakaan ei ole vielä varmaa aikataulua.

Myös Duch-Brownin mielestä yksittäisellä yksilön terveysdatalla ei ole sinänsä kaupallista arvoa yrityksille, vaan arvoa on vasta *aggregoidulla* datalla. Tämän vuoksi yritykset eivät hänen mukaansa ole halukkaita maksamaan yksittäisestä datasta. Hän huomauttaa, että yksilön data on helposti korvattavassa toisen – mahdollisesti myötämielisemmin jakamiseen suhtautuvan – yksilön datalla, joten neuvotteluvaraa ei juuri ole.

Tästä voi katsoa olevan poikkeus henkilöt, joiden terveys jostain syystä kiinnostaa suurta joukkoa hyödyntäjiä, esimerkiksi aiemmin mainitut amerikkalaisen jalkapalloliiton urheilijat, jotka voivat jo myydä harjoitteludataansa jo yhteistyössä urheiluliittonsa kanssa (Boyd 2018). Urheilijan terveysdatasta ovat kiinnostuneita niin fanit, liigat, tiimit, agentit kuin mediakin (Socolow & Jolly 2017, 15). Tutkijat kuitenkin varoittavat (Socolow & Jolly 2017, 17) asiaan liittyvän monia ongelmia, kuten pelaajien alisteiden suhde työnantajaseuraansa ja arkaluontoisen datan leviäminen, eli miten urheilijoiden ostettua biometristä dataa saisi jakaa tai myydä.

Poikola katsoo, että käyttäjän rahallisen kompensoinnin idea on noussut esiin erityisesti Yhdysvalloissa, jossa käyttäjien rahalliseen kompensaatioon suhtaudutaan enemmän itsestäänselvyytenä, mutta hän ei näe saman sopivan Eurooppaan. Hänen mielestään datan hyötyarvo käyttäjälle on moninkertainen verrattuna datan rahalliseen arvoon, koska se johtaa parempiin palveluihin ja niiden yhteentoimivuuteen. Rahallinen kompensaatio taas viittaisi siihen, että käyttäjä on kärsinyt tietojensa käytöstä jotenkin. Hän nostaa esille myös eettisen kysymyksen siitä, tekisikö taloudellinen palkkio yksityisyydestä luksustuotteen, johon vain rikkailla olisi varaa.

Poikola viittaa datayritysten suhteelliseen arvoon eli tuottoon jaettuna käyttäjien määrällä. Poikola vertaa tilannetta Facebookiin:

> *Voi aatella et vaikka, […] koko Facebookin tuotto jaettais sit niiden käyttäjien kesken niin sit se ei loppujen lopuks olekaan niin hirveen suuri summa rahaa ja kun se ei tietenkään koskaan oo sataprosenttinen niin silloin päädytään, […] siihen tulokseen, et […] voisin […] antaa datani käyttöön ja mä saisin joitain, yhden kauppakassillisen verran vuodessa, […] viiskymppiä jostain […] et se […] häviää sit kuitenkin se taloudellinen arvo aika nopeesti.[…] Mä en nää kyl sitä mitenkään erityisen positiivisena suuntana, mutta tiedän ja tiedostan kyllä, että ennen kaikkea […] jenkeissä se on hyvin vahva idea.*

Anagnostou & Lambrou (2017, 7;11) arvioivat Facebookin markkina-arvon jaettuna käyttäjien määrällä olevan noin 150 dollaria ja vuosittainen tuotto per käyttäjä noin 20 dollaria.

6.3 Omistusoikeus dataan

Kaikki haastateltavat suhtautuvat melko tai hyvin kriittisesti datan omistusoikeuden mahdollisuuteen ja useimpien mielestä pitäisi ennemmin puhua datan käyttöoikeuksista. Aarnion mielestä tietosuoja

antaa käyttäjälle merkittäviä oikeuksia, jotka ovat toimeenpantavissa viranomaisten avulla, mutta jotka eivät kuitenkaan vertaudu omistusoikeuteen. Hänen mielestään on voimakas yleistys sanoa, että tietosuoja-asetus olisi antanut *residuaalioikeudet* dataan sen kerääjälle, kuten Duch-Brown et al. (2017, 17) asian näkevät. Aarnio vertaa datan omistusoikeutta tekijänoikeuksiin:

> *[…] voiko oikeutta omistaa, […] joltain osin voi, tekijänoikeudet, joita voidaan siirtää ja käydä kauppaa […] omistusoikeus sellasenaan on tietysti joku, joka luo taloudellista arvoa, mut tietosuoja, niin se on […] enemmän jotain henkistä tahtotilaa kuvaavaa juttu, jota ei sellasenaan kukaan omista. […] datan voi kyllä omistaa, luettelot voi omistaa, […]ne […] ja tietokannat nauttii jonkinlaista omistusoikeuden suojaa, mut se on lähinnä silloin tekijänoikeudellisesta, mut se koskee sit kopiointia ja muuta tällast, mut se kysymys, et henkilöllä on oikeuksia ja esimerkiks kukaan ei voi torjua meidän oikeuksia kuluttajina tai rekisteröityinä sanomalla, et meillä on omistusoikeus tähän dataan, älä sä tuu sanoo mitään.*

Bertellin mielestä omistusoikeus olisi hankala ja kömpelö malli hallita datan oikeuksia ja GDPR:n kanssa ristiriitainen, koska oman henkilötiedon omistuksen siirtäminen toiselle olisi mahdotonta. Hän kuitenkin katsoo, että datan vaihdantaa ja markkinoiden kehittymistä pitäisi edistää ja hallita jonkinlaisilla määritellyillä datan käyttöoikeuksilla. Myös Hämäläisen mielestä datan omistajuus on väärä käsite ja sen sijaan pitäisi puhua datan hyödynnettävyydestä ja pääsystä dataan. Duch-Brownin mukaan datan omistusoikeutta ei ole *täysin* poissuljettu, mutta tällä hetkellä keskeisempää on datan jakaminen ja saatavuus.

Myös Tarkela on lähtökohtaisesti, mutta ei kuitenkaan kategorisesti datan omistusoikeutta vastaan:

> *Lyhyesti sanottuna mun mielestä missään tapauksessa ei omistusoikeutta voi ottaa sellaisenaan ja todeta vaan, että okei, nyt tehdään datalaki ja todeta, että data voi olla omistusoikeuden kohteena. Se ei onnistu, koska omistusoikeus on jo itsessään aika diffuusi olento. Omistusoikeus saa erilaisia ilmenemismuotoja, niin kuin vaikka perustuslain omaisuudensuojassa. Ja yksi erimerkkikysymys on se, että pitäisikö dataa voida käsitellä esimerkiksi Euroopan ihmisoikeustuomioistuimen omaisuudensuojakäytännössä, että se on niin kuin muutkin, että se rinnastuisi omaisuuteen. Se on mielestäni mielekäs kysymys, mutta sen sijaan mä en kykene vastaamaan oikein helpolla kysymykseen siitä, että pitäiskö datan olla omistusoikeuden kohde. Itseasiassa mä näen sen tosi vaikeaksi […]*

Tarkelan mukaan omistusoikeuden käsite on muuttunut ajan kuluessa sen mukaan, millaisia omistuksen kohteet ovat milläkin aikakaudella olleet. Hän katsoo, että data ei sovi objektina samanlaiseen kehikkoon ja relaatioanalyysiin, millaista esimerkiksi suomalaiseen

omistusoikeuskäsityksen kehitykseen merkittävästi vaikuttanut Simo Zitting oli aikoinaan väitöskirjallaan (Zitting 1951) luomassa. Tarkela torjuu myös mahdollisuuden siirtyä kohti angloamerikkalaista lähestymistapaa, jossa omistusoikeus nähdään *oikeuksien kimppuna.* Hän viittaa yhdysvaltalaiseen omistusoikeuskäsitteen uranuurtajaan Wesley Newcomb Hohfeldiin. Tarkelan mukaan Hohfeldin kehittämä *bundle of right*s -lähestymistapa kuvaa silloista 1900-luvun alun ajankuvaa, ja sopii siksi paremmin vakiintuneiden ja konkreettisten oikeusobjektien työkaluksi. Hohfeld muutti common law -oikeusjärjestelmän omistuksen käsitettä määrittelemällä omistusoikeuden ihmisten välisinä suhteina ja velvollisuuksina, pikemmin kuin omistussuhteena johonkin *esineeseen* (Johnson 2007, 251). Johnson (2007, 253) listaa common law -järjestelmän omistusoikeuden *kimppuun* kuuluvia oikeuksia, joista yksi on *oikeus tuloon,* joka omistuksen kohteesta on saatavissa sitä hyödyntämällä tai antamalla toisten hyödyntää. Tämä selittää miksi Yhdysvalloissa ajatus oman datan taloudellisten oikeuksien hyödyntämisestä on Poikolan mainitsemalla tavalla yleisempi kuin Euroopassa.

Tarkela näkee, että data ja immateriaalioikeudet ovat molemmat

> *[…] amorfisia olentoja ja käsitteitä, jotka eivät helpolla taivu relaatioanalyyseihin.*

Tarkela kuitenkin painottaa, että data liittyy niin kiinteällä tavalla jokaisen elämään ja arkeen, että se pitäisi jotenkin integroida oikeusjärjestelmään niin, että sen arvo voitaisiin kokonaisuudessaan hyödyntää ja siihen liittyviä oikeuksia käsitellä erilaisissa tilanteissa ja oikeuskäytännössä. Hänen mukaansa data pitäisi käsittää resurssi- ja prosessitasoiseksi samalla tavalla kuin esimerkiksi työvoima, ja jonka hyödyntämiseen pitäisi olla oma selkeä viitekehyksensä.

Vaikka Tarkelakaan ei kannata omistusoikeutta sinällään, on huomionarvoista, kuinka jyrkän kielteinen Poikolan mielipide on datan omistusoikeutta kohtaan. Hänen mielestään omistusoikeuden potentiaali terveysdatan hallintamallina on *”täysin nollassa tai negatiivinen”.* Hänen mukaansa omistusoikeus ei sovellu datan hallintaan:

> *[…] sanoisin, et valtavirtanäkemys on, et datan omistajuus, semmosta ei ole tällä hetkellä missään lainsäädännöissä ja siihen on […] syynsä, […] datan käyttöoikeuksista voi puhua, ja niistä pitääkin puhua, mut et omistajuus on lähtökohtaisesti […] eksklusiivinen oikeus ja sit eksklusiviteetin tuominen dataan […] ei aiheuta mitään muuta kuin vaikeuksia, että ehdottomasti erittäin negatiivisesti suhtaudun tähän ajatukseen.*

Poikolan mielipiteessä todennäköisesti painottuu datan erityislaatuisuus ja haasteet mahdollisen omistusoikeuden kohteena, joita on käsitelty kohdassa 3.2. Tarkelan mielipiteeseen vaikuttaa taas todennäköisesti hänen kokemuksensa immateriaalioikeusjuristina ja hänen hahmottamansa datan liityntäkohdat ja mahdolliset konfliktit muuhun oikeusjärjestelmään, joihin hänen mukaansa törmätään ennen pitkää. Toki haastateltavien mielipiteiden välinen ristiriita voi olla myös näennäinen ja johtua haastattelijan väärästä tulkinnasta.

Tarkela painottaa, ettei hän kannata myöskään dataspesifistä sääntelyä, kuten komission suunnittelemia *data-avaruuksia,* jotka sisältyvät komission helmikuussa 2020 julkaisemaan datastrategiaan vuosille 2019-2024 (EU COM 2020b). Sektorikohtaisten data-avaruuksien on tarkoitus edistää datan yhteisiä markkinoita ja datan jakamista (EU COM 2020c). Hankkeen tavoitteet ovat monipuolisen kunnianhimoiset (EU COM 2020d, 5):

> *Tavoitteena on luoda yhteinen eurooppalainen data-avaruus – todelliset datan sisämarkkinat, jotka ovat avoinna kaikkialta maailmasta tulevalle datalle ja joilla niin henkilötiedot kuin muut suojattavat tiedot, kuten liiketoiminnan kannalta arkaluonteiset tiedot, ovat turvattuja ja joilla yrityksillä on vaivaton pääsy lähes rajattomaan määrään laadukasta teollista dataa, mikä tukee kasvua ja luo arvoa minimoiden samalla ihmisen hiili- ja ympäristöjalanjäljen.*

Bertell sen sijaan suhtautuu varovaisen optimistisesti komission hankkeeseen. Hänen mukaansa on tarve markkinapaikalle, jossa datan käytölle olisi selkeät säännöt. Tarkela katsoo, että tällainen on reaktiivista sääntelyä, mikä on nykyisessä tilanteessa ymmärrettävä ratkaisu todettuihin ongelmiin, mutta ei ratkaise isoja ongelmia. Hänen mukaansa suuremmat muutokset datan oikeuksien määrittelyssä kilpistyvät jäsenmaiden erilaisiin kansallisiin varallisuusoikeudellisiin järjestelmiin. Kotimaan tasolla hänen mukaansa pitäisi integroida data osaksi olemassa olevia järjestelmiä käymällä läpi erilaiset säädökset, kuten yrityskauppojen ja kilpailuoikeuden normit ja tutkia ovatko ne datan kanssa yhteensopivia, ja miten ne voitaisiin muuttaa sellaisiksi. Tarkelan mukaan datatalous tuo väistämättä mukanaan konflikteja datan ja muiden normien kanssa. Yhtenä esimerkkinä hän mainitsee verottajan, joka tarvitsee tietoa datan varallisuusarvosta. Myös datan disponointiin liittyviin kysymyksiin, kuten voiko dataa luovuttaa tai periä, täytyy hänen mukaansa ennen pitkää ottaa kantaa. Hän näkee juridiikan tehtäväksi antaa työkaluja ja käsitteitä näiden kysymysten ratkomiseen ja muutoksen hallintaan.

6.4 Datan kerääminen ja jakaminen yritysten kesken

Useimpien haastateltavien mielestä omistusoikeutta oleellisempaa on pääsy dataan ja sen hyödyntämisen mahdollistaminen. Tämä vaatii sekä datan keräämistä että kerätyn datan jakamista yritysten kesken, koska kaikki yritykset eivät kerää tai tuota dataa.

Duch-Brownin johtaman tutkijaryhmän komissiolle tekemässä selvityksessä (Duch-Brown et al. 2017, 29-30) puhutaan datan arvoketjun horisontaalisista ja vertikaalisista esteistä. Horisontaalinen este liittyy *datan laajuusetuihin,* (economies of scope) joka tarkoittaa, että kahdella toimijalla on jollain tavalla päällekkäiset tai toisiaan täydentävät datasetit, joista saisi yhdistettynä enemmän tai arvokkaampaa informaatiota kuin molemmista erikseen. Datasettien hyödyntämisessä on vertikaalinen este, kun toimijat eivät pääse molempia tyydyttävään sopimukseen niiden yhdistämisestä. Vertikaalisessa esteessä on tällöin kyse siitä, että dataa hallitseva toimija, kuten sen kerääjä, ei suostu jakamaan tai myymään dataansa verkostossa alempana olevalle datan halukkaalle hyödyntäjälle, tai osapuolet eivät pysty sopimaan datan hinnasta. Näissä tilanteissa datan kerääjän de facto omistus johtaa datan alikäyttöön ja tehottomuuteen. (Duch-Brown et al. 2017, 29-30).

Duch-Brownin mukaan henkilötiedon kerääjän tosiasiallista omistajuutta tai hallintaa on vaikea korjata tai ehkäistä. Asian korjaaminen sääntelyllä on monimutkaista, koska data eroaa aineettomista oikeuksista siinä, että datalla laajuusedut ovat sääntö, eivät poikkeus, toisin kuin esimerkiksi patenteilla. Tämän vuoksi datan laaja jakaminen ja saatavuus on olennaista. Hänen mukaansa tärkeämpää olisi keskittyä varmistamaan, että dataa kerätään mahdollisimman paljon, ja yritysten lisäksi myös yhteiskunta pystyisi hyötymään datasta. Kokonaishyöty ja tehokkuusedut ovat hänen mukaansa sitä suurempia, mitä enemmän dataa on käytössä erilaisilla toimijoilla ja erilaisiin tarkoituksiin.

Datan kerääminen ei ole Duch-Brownin mukaan yleensä yrityksen ydinliiketoimintaa, vaan tapahtuu perusliiketoimintojen ohessa. Hän katsoo, että osaa yrityksistä pitäisi kuitenkin kannustaa datan keräämiseen ja huomaamaan sen potentiaali toiminnan tehostamisessa ja kehittämisessä, jotta dataa olisi saatavilla mahdollisimman paljon. Määrä on hänen mukaansa oleellista siksi, että datasta saadaan luotettavia tuloksia. Kerättävän datan pitää Duch-Brownin mukaan olla *edustava*, jotta sen perusteella tehdyt analyysit ja johtopäätökset ovat yleistettävissä: jos dataa käytetään algoritmien opettamiseen, vääristynyt datasetti voi johtaa siihen, että algoritmi oppii tuottamaan vääristyneitä tuloksia, mistä voi seurata haitallisia, vääristyneitä suosituksia.

Poikola kuitenkin huomauttaa, että keräämistäkin tärkeämpää on osata hyödyntää kerättyä dataa:

> *[…] jos joku vielä muistaa, et pari vuotta sitten puhuttiin big datasta, et se oli hypetermi, niin aika monet yritykset silloin […] alkoi kerryttää dataa ja sit vasta lopuks ne havahtu siihen, et eihän se kullaks muuttunutkaan […], et sille pitää tehäkkin jotain, et siitä pitää pystyä tuottamaan palveluita tai informaatiota, analyysejä, jotain muuta ja nyt sit ollaan siinä […], et tää data science on päivän sana, […]nyt sit haetaan hullun lailla […] osaamista ja […] palveluja sen päälle, […] tosiaan se arvo muodostuu vasta sitten, kun dataa käytetään, ja jos dataa käytetään […] laajasti, et sillä voi olla erilaisia käyttöpisteitä ympäri maailmaa, niin silloin se jakais sitä arvoakin tasaisemmin.*

Hämäläinen näkee, että datan jakaminen on yksi verkostotalouden muotoja ja hyödyt yritysten kesken eivät ole vain taloudellisia, vaan yritysten saama lisäarvo voi liittyä myös osaamisen ja palvelukyvyn kasvuun. Hänen mukaansa erityisesti kotimaiset pk-yritykset eivät tunnista vielä kumppanuuden ja vaihdannan mahdollisuuksia datataloudessa. Hän viittaa neljässä Euroopan maassa tehtyyn yrityskyselyyn, jossa todettiin, että suomalaisten yritysten omat arviot valmiudestaan hyödyntää dataa tai hyötyä sen vaihtamisesta muiden yritysten kanssa ovat huonommat kuin Ranskassa, Saksassa ja Hollannissa (Ulander et al. 2019, 26). Hämäläisen mukaan Sitra reagoi näihin tuloksiin ensi syksynä käynnistyvällä ohjelmalla, jossa valmennetaan pk-yrityksien kykyjä käyttää ja hyödyntää dataa sekä käydään läpi reilun datatalouden hyötyjä yritykselle.

Duch-Brownin mukaan ongelmia on niin datan jakamisessa kuin jakamattomuudessa. Yritysten ja yritysryhmien välisessä *horisontaalisessa* datan jakamisessa törmätään hänen mukaansa helposti kilpailuoikeudellisiin ongelmiin, koska yritykset pyrkivät jakamallaan datalla saavuttamaan kilpailuedun ryhmän ulkopuolisin yrityksiin verrattuna. Hänen mukaansa tärkeämpää on kuitenkin datan vertikaalinen jakaminen, eli datan jakaminen toimitusketjussa, esimerkiksi toimittajalta valmistajalle, joka voi käyttää dataa omien tuotteiden ja prosessien laadun parantamiseen. Datan jakamisen halukkuutta vähentää kuitenkin riski strategisten salaisuuksien paljastumisesta ja oman aseman suhteellisesta heikentymisestä. Hänen mukaansa yrityksille tulisi jotenkin osoittaa jakamisen hyödyt ja luoda jakamiseen selkeä viitekehys. Markkinoiden epäonnistumisia, kuten datan jakamisen esteitä ja ulkois- ja verkostovaikutuksia, voidaan hänen mukaansa korjata vain regulaatiolla.

Aarnion mukaan yrityksillä painottuu nykytilanteessa enemmän oman kilpailuedun säilyttäminen kuin mahdollisen jakamisen hyötyjen tavoittelu, eivätkä yritykset lähtökohtaisesti halua jakaa tietoa. Hänen mukaansa ongelmaan liittyy myös edellä käsitelty datan siirrettävyys:

[…] meillä […] tyypiteltiin kolme tilannetta. Ensimmäinen oli se, yritys ei halua jakaa kilpailijalle, toinen tilanne oli se, et ne ei halua myöskään et kuluttaja käyttää sitä oikeutta, et heidän pitäis jakaa se kilpailijalle ja kolmas on taas se, et ne rakentaa tällaisia ansaintalogiikkaan liittyvii, erilaisii allianssei sun muita, yhteenliittymiä, joiden sisällä sitä dataan jaetaan […]

Bertellin on sen sijaan sitä mieltä, että halu datan jakamiseen on olemassa, mutta vaatisi datan jakamiseen liittyvien oikeuksien ja velvollisuuksien selkeää määrittelyä ja jakamisen mahdollistavaa infrastruktuuria:

[…] yrityksethän haluaa jakaa tietoa, mut […] et missä ja miten sitä jakaa ja pelkästään,[…] vaikka API-rajapintojen tai infrastruktuurin puute tai sääntöjen puute tai […] yksinkertaisesti, että, […] se ei tuu samassa muodossa, et tiedonhallinnolliset puutteet, niin yksinkertaisesti […] saattaa ihan täysin estää sitä, et kyllähän nyt jo voi yritykset ihan helpostikin varmaan keskenään sopia et voidaan molemmat […] yhdessä luotua dataa […] käyttää omiin tarkotuksiin ja […] mut se on sit vaan kahden yrityksen tai, […] muutaman yrityksen välinen, et […] markkinapaikkojen sääntöjen selkeyttäminen olis tässä paikallaan […]

Myös Bertell viittaa yritysten välisen datan jakamisen kilpailuoikeudellisiin problematiikkaan. Hän sanoo kilpailuoikeudellisen sääntely kaipaavan tämän osalta selkeyttämistä. Bertellin mukaan dataan pitäisi päästä käsiksi myös esimerkiksi pk-yritykset, jotka eivät itse kerää tai tuota dataa.

Haastateltavien mielipiteet ovat pitkälti samassa linjassa Euroopan komission tekemän selvityksen kanssa (EU COM 2018, 78-79). Sen mukaan suurimpia esteitä yritysten väliselle datan jakamiselle ovat riskit arkaluonteisen datan jakamisesta ulkopuolisten kanssa: kilpailuedun menettäminen, sopimusoikeudellinen epävarmuus, epävarmuus datan oikeuksista, jakamisen tekniset ongelmat ja riski asiakkaiden luottamuksen menettämisestä. Selvityksen mukaan suuri osa yrityksistä näkee datan jakamisen riskit nykyisessä epävarmassa ja epäselvien sääntöjen tilanteessa vielä hyötyjä suurempina.

Duch-Brown kuitenkin pitää järjestelmien yhteentoimivuuden ongelmia vain oireena yritysten jakamisessa nähdyistä riskeistä. Hänen mukaansa teknisestä näkökulmasta järjestelmien yhteentoimivuus on helposti ratkaistavissa ja sen puute on enemmän strateginen valinta. Ongelma ratkeaa, jos ja kun yritykset näkevät datan jakamisessa tarpeeksi hyötyjä. Eri yritysten erilainen halukkuus ja motivaatio rakentaa yhteentoimivia järjestelmiä voidaan kuitenkin hänen mukaansa ratkaista vain sääntelyllä.

6.5 Ihmiskeskeiset datan hallintamallit

Haastattelun kysymyksissä nostettiin ihmiskeskeisistä datan hallintamalleista esimerkeiksi MyData ja Sitran *reilun datatalouden* IHAN-hanke. Poikolan mukaan MyData on IHAN-hankkeeseen verrattuna ennemmin yleisellä tasolla oleva idea tai filosofia ihmiskeskeisestä datan hallinnasta, jota edistetään ympäri maailmaan esimerkiksi erilaisissa projekteissa ja tutkimuksissa. Standardeilla on hänen mukaansa merkittävä rooli MyData-idean levittämisessä ja IHAN-hanke on MyDataan nähden astetta konkreettisemmalla tasolla oleva projekti. Poikolan mukaan molempien tavoitteet ovat samansuuntaiset ja MyDatan ja Sitra tekevän tiivistä yhteistyötä. MyData Global taas on alustaorganisaatio, joka pyrkii tuomaan eri puolilta maailmaa yhteen eri tasojen toimijoita, kuten yrityksiä, tutkijoita ja lainsäätäjiä. Poikolan mukaan MyData on merkittävä ilmiö Suomen lisäksi muun muassa Hollannissa, Ranskassa, Iso-Britanniassa, Japanissa ja Koreassa. Hänen mukaansa MyDatan idea keksittiin eri puolilla maailmaa samaan aikaan eikä MyData hänen mukaansa ole erityisesti suomalainen projekti, vaikka MyData Globalin päämaja onkin Suomessa.

MyData-liike pyrkii antamaan yksilölle työkalut omien henkilötietojensa hallintaan ja hyödyntämiseen, samalla kun pyritään edistämään datatalouden oikeudenmukaisuutta ja reilua kilpailua (MyData.org 2020). Yksilön henkilötieto on idean mukaan yksilön *MyDataa* silloin, kun hänellä on ”*oikeus ja käytännön mahdollisuus saada omat tietonsa itselleen, käyttää niitä vapaasti ja siirtää halutessaan kolmansille osapuolille”* (Poikola et al. 2018, 5). MyData mainitaan Euroopan komission helmikuussa 2020 julkaistussa Datastrategia-tiedonannossa (EU COM 2020d, 10). Komissio arvioi MyDatan ja muiden vastaavien liikkeiden olevan vasta alkuvaiheessa, mutta sisältävän ”*huomattavaa potentiaalia*” ja tarvitsevan sopivan ympäristön menestyäkseen. Suomella oli mahdollisuus edistää tietoisuutta ihmiskeskeisten datan hallintamalleista EU-puheenjohtajakaudellaan vuoden 2019 jälkipuoliskolla (Halenius 2020), jolloin julkaistiin myös EU-tasolla asiantuntijoiden ja sidosryhmien kanssa neuvotellut ihmiskeskeisen datatalouden periaatteet, *Principles for a human-centric, thriving and balanced data economy* -paperi (EU 2019).

Aarnio kertoo kannattavansa ihmiskeskeisiä malleja ”*99-prosenttisesti*”. Hän pitää ihmiskeskeisten datan hallintamallien mahdollisena riskinä väärinkäytöksiä, kuten käyttäjään kohdistuvaa painostusta jakaa omia asiaankuulumattomia henkilötietojaan esimerkiksi työhaastattelun yhteydessä. Muutoin ihmiskeskeiset mallit ovat Aarnion mukaan GDPR:n kanssa yhteneväisiä tukiessaan samoja tavoitteita, kuten yksilön itsemääräämisoikeutta, datan siirrettävyyttä, vastustamisoikeutta, kielto-oikeutta ja virheenoikaisuoikeutta.

Bertell viittaa samaan mahdolliseen riskiin kuin Aarniokin, eli yksilön itsemääräämisoikeuden mahdolliseen hyväksikäyttöön. Hänen mukaansa ihmiskeskeiset mallit siirtäisivät datan portinvartijan roolin datan kerääjältä käyttäjälle, eikä käyttäjä välttämättä ymmärtäisi oman datansa jakamisen seurauksia. Bertell arvioi, että ihmiskeskeiset mallit antaisivat käyttäjille enemmän oikeuksia, mutta pohtii pystyisivätkö he todellisuudessa kontrolloimaan oikeuksiaan, kun käyttäjän kynnys antaa suostumus on nykyisinkin hyvin matala. Hän viittaa käyttäjän potevan jo nykytilanteessa tietynlaista *suostumusväsymystä* ja pohtii, pahentaisivatko ihmiskeskeiset mallit sitä edelleen. Bertellin mukaan tätä voisi lieventää käyttäjän ja datan hyödyntäjän välinen, ihmiskeskeisiin malleihin jossain muodossa kuuluva, suostumusoperaattori, jolle käyttäjä voisi antaa mandaatin jakaa suostumus. Hänen mielestään dynamiikka voisi toimia tietyissä tilanteissa, kuten joidenkin luotettavien julkisten toimijoiden kautta. Bertell kuitenkin korostaa, ettei ole varsinaisesti kumpaakaan, ihmiskeskeisten mallien puolesta tai vastaan. Hänen mielestään mallit eivät ole vielä niin käytännönläheisiä, että niiden toimivuutta pystyisi arvioimaan.

Tarkela arvioi ihmiskeskeiset mallit sinällään hyviksi ideoiksi, mutta epäilee niiden käytännön toteuttamiskelpoisuutta. Hän on vakuuttunut, että mallit eivät menestyisi itsestään, vaan vaatisivat makrotasolla taakseen lainsäädännöllistä tukea ja jonkinlaisen dataspesifin infrastruktuurin. Tämä vaatisi monien tahojen ja maiden vakuuttamista mallien hyödyistä, mikä ei ole hänen näkemyksensä mukaan tällä hetkellä todennäköistä, koska organisaatiot, kuten OECD (Taloudellisen yhteistyön ja kehityksen järjestö), WIPO (Maailman henkisen omaisuuden järjestö) tai WTO (Maailman kauppajärjestö) eivät ole hänen mukaansa tehneet minkäänlaista aloitetta tällaisten mallien käsittelystä. Hän ei myöskään usko, että datan taloudellinen potentiaali pystyttäisiin tehokkaasti realisoimaan alueellisissa ihmiskeskeisissä malleissa. Juridisella tasolla hän viittaa mallien ongelmana sopimusoikeuden *inter partes* ja esineoikeuden *erga omnes* eroihin. Hänen mukaansa on juridisesti ylittämätön ongelma, että käyttäjän tiettyihin datan käyttötarkoituksiin antamalla suostumuksella ei pystytä sitomaan kolmansia osapuolia, jotka voivat saada datan haltuunsa jossain vaiheessa. Tarkela huomauttaa, että ei ole kuitenkaan perehtynyt malleihin erityisen syvällisesti ja olisi ”*mielellään väärässä*”.

Duch-Brown mukaan ihmiskeskeiset hallintamallit ovat yksi vaihtoehto, joka antaisi yksilölle enemmän hallintamahdollisuuksia henkilötietoihinsa, mutta samalla heikentäisi datan jakamisen hyötyjä yhteiskunnalle. Ihmiskeskeiset mallit antaisivat mahdollisuuden valikoida datan käyttömahdollisuuksia yksilöllisesti, joka hänen mukaansa vaikeuttaisi datan kokonaisarvon

realisoitumista. Hän katsoo, että kyse on lopulta siitä, suunnitellaanko datan jakamisen viitekehys yhteiskunnan vai yksilön etuja painottaen.

Hämäläisen ja Poikolan näkemykset ihmiskeskeisistä datan hallintamalleista ovat luonnollisesti positiivisia. Hämäläinen kuitenkin myöntää, että kehitys on vasta aluillaan ja itse idea on ”*vallankumouksellinen*”, mutta ”*niin on ollut aikanaan kiertotalouskin*”. Hänen mukaansa nykyinen tilanne, jossa muutama yhdysvaltalainen yritys dominoi kansainvälisiä markkinoita on kestämätön ja jonkin täytyy muuttua. Nykyinen markkina on Hämäläisen mukaan liian keskittynyt ja monopolisoitunut. Poikolan mielestä kehitys pyörii nykytilanteessa liikaa anonyymin datan ympärillä. Henkilödatan laajempi hyödynnettävyys avaisi hänen mukaansa paljon uusia mahdollisuuksia ja ihmiskeskeiset hallintamallit pystyivät antamaan tähän työkaluja. Hänen mielestään pitäisi siirtyä tiedollisen itsemääräämisoikeuden negatiivisesta – miten yksilö pystyy rajoittamaan datansa käyttöä – lähtökohdasta positiiviseen eli miten yksilö toivoo dataansa käytettävän.

Hämäläinen näkee, että ihmiskeskeisissä malleissa käyttäjän luottamus säilytettäisiin datan käytön läpinäkyvyydellä ja mahdollisuudella hallita suostumusta myös jälkikäteen. IHAN-mallissa datan hallinta olisi hänen mukaansa nykytilanteeseen nähden käänteinen niin, että data-avaruus on erillään palveluntarjoajasta, eikä syntyisi suuria datavarantoja, joihin käyttäjällä ei olisi hallinta- ja kielto-oikeuksia. Hämäläisen mukaan datan hyödyntämisen periaatteet ovat osa yritysvastuuta, joka vaatii yhteisiä sääntöjä ja läpinäkyvyyttä. Käyttäjän tietoisuuden lisääminen ja sitä kautta käyttäjän paine palveluntarjoajille on hänen mukaansa avain muutokseen. Hämäläinen katsoo, että ihmiskeskeiset mallit ja reilun datatalouden periaatteet ovat ainoat mahdolliset tavat päästä turvallisesti ja luotettavasti hyödyntämään ihmisiä koskevaa dataa, jota kerätään ja kertyy koko ajan valtavia määriä.

Poikolan mukaan ihmiskeskeisten mallien etuna on datan hyödyntäjien ja innovaattoreiden mahdollisuus pyytää datan oikeuksia suoraan yksilöltä, eivätkä ne näin olisi enää riippuvaisia dataa hallitsevista kerääjistä tai alustoista. Hänen mukaansa käyttäjä ja data on nykytilanteessa liikaa sidottu laitteeseen ja sen alkuperäiseen valmistajaan, joka pystyy hallitsemaan kerättyä dataa. Tämä estää arvoketjun pilkkoutumisen ja uusien toimijoiden alalle tulon.

Poikola näkee, että ihmiskeskeisistä malleista olisi hyötyä niin yksilöille kuin yrityksillekin:

[…] ihmisten tiedollinen itsemääräämisoikeus on […] yks ajuri, joka […] poliittisella tasolla on vahva ja […] tavallaan se on […] seuraava askel siitä tietosuojasta siihen, että ihmisillä on myös mahdollisuus hyötyä omasta datastaan, […] et päästäs […] tiedollisen itsemääräämisoikeuden myös […] positiiviseen puoleen, eikä vaan negatiiviseen, niin et minä rajoitan sitä, ettei minulle tapahdu mitään pahaa, ettei kukaan tee pahaa datallani, et […] saatais myös […] proaktiivinen puoli, joka sanois, et minä haluan, että minun dataani käytetään tähän asiaan […] sitten toinen on ihan sit tuolta yritystoiminnan näkökulmasta, että päästäs […] siihen, että sellasillakin toimijoilla, joilla ei ole valtaisaa datankeräysinfraa maailmassa niin, että he pystyisivät […] tuomaan markkinoille henkilödataan pohjautuvia palveluita, jos ihmiset […] itse näkisivät ne palvelut hyödyllisinä, et ikään kuin sen sijaan, että uuden startupin pitää mennä kolkuttelemaan jonkun Googlen tai […] ovelle, niin se startup vois tulla kolkuttelemaan mun ovelle, […] et nykyisin, kun se data on […] sidoksissa sinne lähtöpalveluntuottajaan, niin silloin se hidastaa aika paljon sitä, tai jopa estää […], et ei oo […] mahdollista tuoda markkinoille dataan pohjautuvia palveluita, ellei ole […] kyvykkyyksiä saada, […]kerättyä sitä dataa, niin tässä se ois mahdollista […]

Sekä Poikolan että Hämäläisen mukaan hallintamallin muutos ei voisi koskea vain Suomea, vaan vaatisi tapahtuakseen laajempaa mittakaavaa, vähintään Euroopan tasoista. Ihmiskeskeisillä malleilla on Poikolan mukaan tällä hetkellä Euroopassa ja EU:ssa vahva poliittinen tuki, mikä antaa hyvän kasvualustan, mutta ei kuitenkaan yksinään riitä. Hänen mukaansa tarvitaan myös liiketoimintamallien kehittymistä niin, että ne tarjoaisivat liiketaloudellisesti houkuttelevan vaihtoehdon nykyisille mainosrahoitteisille malleille. Poikola näkee mahdollisina muutoksen ajureina esimerkiksi valveutuneisuuden kasvun, yksityisyyteen liittyvät skandaalit ja tiukemman tietosuojalainsäädännön. Poikola kuitenkin korostaa, että muutokset tuskin tapahtuvat kovin nopeasti, vaan voivat vaatia jopa kymmeniä vuosia.

Myös Hämäläinen sanoo Euroopassa olevan tilausta ihmiskeskeisille datan hallintamalleille ja kertoo komission pyytäneen Sitraa vetämään hanketta, jossa kehitetään ihmiskeskeisiä malleja hyvinvointi- ja terveyssektorille. Euroopan laajuisena ihmiskeskeinen hallintamalli toisi hänen mukaansa myös globaalia painetta muutokseen. Hämäläisen näkemys yksityishenkilönä on, että paine paradigman muutokseen voi tulla monesta suunnasta: säännösten, juridiikan, markkinan oman sääntelyn, kuluttajaliikkeen tai yhteiskunnasta tulevan poliittisen paineen kautta. Myöskään hän ei kuitenkaan usko nopeaan tai yhtäkkiseen muutokseen.

6.6 Datan hallinnan tulevaisuus

Poikolan näkemys suomalaisten dataintensiivisten yritysten mahdollisuuksista on optimistinen eikä hän näe erityisiä esteitä yritysten kasvulle tai kilpailulle. Hänen mukaansa Suomella on paljon vahvuuksia kuten korkeaa osaamista ja suuriin maihin verrattuna helpommat yhteistyö- ja keskustelumahdollisuudet organisaatioiden välillä. Tämä mahdollistaisi Poikolan mukaan esimerkiksi suomalaisen terveysteknologian paremman yhteentoimivuuden ja sitä kautta saatavan kilpailuedun. Saatavilla olevan rahoituksen määrät saman tason ideoille ovat hänen mukaansa Suomessa kuitenkin selvästi pienemmät kuin esimerkiksi Piilaaksossa. Poikolan mukaan helpommin saatavan rahoituksen piirissä ja maissa pystytään dominoimaan markkinoita huonommallakin tuotteella. Poikola uskoo, että markkinoiden luonnollinen kehitys vie siihen suuntaan, että eri osat arvoketjusta päätyvät sen parhaiten hallitsevalle, erikoistuneelle toimijalle. Tämä toisi hänen mukaansa lisää kilpailua ja ihmisille parempia palveluita. Tällöin yritykset pystyisivät tulemaan markkinoille myös nopeammin esimerkiksi ilman olemassa olevaa käyttäjäkuntaa.

Poikola ei näe GAFA -yrityksissäkään (Google, Amazon, Facebook, Apple) erityistä uhkaa pienemmille yrityksille. Hän kuitenkin viittaa *Kronos-efektiin* eli suurien yritysten mahdollisuuteen ostaa heidän toimintaansa uhkaavat pienemmät toimijat markkinoilta suurten kassavarantojensa mahdollistamana. Hän ei kuitenkaan näe ilmiötä kovin negatiivisena. Poikola näkee, että GAFA-yritykset ovat vahvoja toimijoita ja jonkinlaisessa portinvartijan asemassa, mutta epäilee osan niistäkään pysyvän markkinoilla kovin pitkään:

> *[…] en usko esimerkiksi Facebookin tulevaisuuden pituuteen ollenkaan kovin paljon, mut Google on paljon vahvempi […] ne ei oo […] mitenkään […] samasta puusta veistettyjä toimijoita […]*

Yksityisyysparadoksista puhuttaessa Poikola ei näe syytä, että käyttäjiä pitäisi erityisesti kannustaa kiinnostumaan henkilötietojensa käytöstä. Hänen mukaansa olisi yhteiskunnan tehtävä rakentaa instituutioita ja turvallinen ympäristö, jotka varmistavat, että käyttäjän ei tarvitse huolehtia datansa käytöstä. Poikola ei näe, että ylhäältä annetulla tiedolla ja valistuksella voitaisiin muuttaa ihmisten käyttäytymistä, mutta hän uskoo, että ihmisten *datalukutaito* kehittyy ajan ja palveluiden käytön myötä. Hänen mielestään käyttöehtojen pitäisi muuttua helpommin hahmotettavaan ja räätälöitävämpään suuntaan, jolloin käyttäjä voisi valita minkä datan käyttöön suostuu, samalla tavoin kuin mobiilisovelluksissa voi nykyään valita mihin tietoihin sovellus pääsee käsiksi. Poikola

odottaa myös tulevan sääntelyä, joka pakottaisi tarjoamaan palveluita tietyllä perustasolla ja vähemmälläkin tietojen luovuttamisella.

Duch-Brown on Poikolan kanssa osittain samoilla linjoilla. Hänen mukaansa nykytilanteessa ongelmana on joidenkin toimijoiden dominoiva asema ja valta tehdä käyttäjälle *ota-tai-jätä*-tarjouksia perustuen pitkiin ja vaikeasti ymmärrettäviin sopimuksiin, joita ei jakseta lukea. Tämä johtaa siihen, että vaikka yksilölle olisi olemassa vaihtoehtoja, niistä ei jakseta ottaa selvää. Duch-Brownin mukaan ongelmaan tulisi puuttua pakottamalla yrityksiä selkeyttämään sopimusehtoja sekä kertomaan selkeämmin datan hyödyntämistavoista. Hänen mukaansa nykyinen kerääjän de facto omistajuus henkilötietoihin voi kuitenkin olla lopullinenkin asiantila.

Duch-Brownin mukaan ongelma GAFA-yrityksissä on se, että ne ovat olleet markkinoilla niin pitkään ja saavuttaneet niin vahvan aseman, että sitä on henkilödatan suhteen enää vaikea horjuttaa tai muuttaa, ellei markkinoille tule jotain uutta markkinat mullistavaa toimijaa. Ei-henkilödatan eli esimerkiksi teollisen datan suhteen tilanne on hänen mukaansa toinen. Hänen mukaansa Euroopalla on mahdollisuus vielä hallita omia ei-henkilödatan markkinoitaan ja kasvattaa omia *datajättejä*, jos perinteisten vahvojen toimialojen, kuten autoteollisuuden, pankkitoiminnan ja energia-alan, data saadaan hyötykäyttöön ja toiminnan tehostamiseen. Duch-Brownin mukaan Euroopan komissiokin keskittyy jo enemmän ei-henkilödatan markkinaan:

> *[…] I think that's the whole idea behind the European data strategy, to create these data spaces, basically to first avoid that Europe also loses control of non-personal data and perhaps creating, say, the European champions as the GAFAs, […] but for non-personal data that can perhaps also be worldwide operators and perhaps expand to other markets as well, and […] I see, a lot of potential […] in Latin America and Asia etc. […] I think that's a, say, […] hidden strategy of the commission, seems the personal data battle is already lost, we need to concentrate on the other type of the market and let's try to be the champions there […] to have this first mover's advantage, in data spaces, in industrial spaces and then export [that] to other potential partners or countries*.

Hämäläisen mukaan Suomessa ollaan verkostotaloudessa ja palveluliiketoiminnassa muita maita jäljessä. Kotimassa keskitytään hänen mukaansa liikaa yksittäisen tuotteen arvoketjuun, vaikka datan hyödyntämiseen tarvittaisiin verkostomainen yhteistyörakenne. Kuitenkin myös Hämäläinen näkee Suomella vahvuuksia kuten hyvät rekisteridata-aineistot, sähköiset järjestelmät ja edelläkävijyyden rekisteridatan toisiokäytössä. Hämäläinen antaa yhtenä esimerkkinä saavutettavissa olevista eduista

säästöt, joita voidaan saada hyödyntämällä hyvinvointi- ja terveysdatasta ennustettua työkyvyttömyysriskiä.

Bertellin mukaan suuret yritykset pystyvät sopeutumaan datamarkkinan muutokseen ja arvioimaan riskit, mutta pk-yrityksillä tilannetta vaikeuttavat resurssien kuten oman juristin puute. Hänen mukaansa datataloudessa vahvoilla ovat ne yritykset, jotka pystyvät strategisesti hahmottamaan koko datan hyödyntämisen koko elinkaaren ja hyödyntämisen liittyvät riskit, alkaen esimerkiksi käyttötarkoitusmäärittelyistä. Bertellin mielestä markkina vaatisi kuitenkin alustatoimijoiden aseman ja kilpailuoikeussääntöjen selventämistä regulaatiolla ja myös niiden toimijoiden pääsyä datamarkkinalle, jotka eivät itse kerää dataa. Esimerkiksi Drexl (2018, 4) on arvioinut Euroopan unionin tuomioistuimen mahdollisuudet puuttua kilpailuoikeudellisesti datatalouden markkina-aseman väärinkäyttöön hyvin rajoitetuksi, perustuen tuomioistuimen oikeuskäytäntöön.

Bertell odottaa datan saatavuuteen osaltaan auttavan komission suunnittelemien, edellä mainittujen *data-avaruuksien* (EU COM 2020b). Datan jakamista yritysten kesken hän näkee hidastavan infrastruktuurin, API-rajapintojen sekä selkeiden sääntöjen puute. Hän kuitenkin huomauttaa eri yritysten kesken olevan myös ristiriitaisia intressejä datan jakamisen suhteen.

Poikolan tapaan myös Bertell korostaa, että kehityksen pitäisi tapahtua markkinaehtoisesti. Lainsäätäjän pitäisi hänen mukaansa kuitenkin luoda markkinoille perussäännöt ja yhteiset standardit. Hän näkee yhtenä mahdollisuutena sen, että ei kehity julkista markkinapaikkaa vaan yritykset alkavat jakaa dataa kahdenvälisesti tai tiettyjen ryhmien sisällä sopimuksiin perustuen. Bertell näkee, että ainoa mahdollisuus muutokseen datan markkinoilla tulee komissiolta, koska kukaan nykyisistä toimijoista tai ryhmistä ei halua muuttaa toimintaansa eikä markkinoille mahdu uusia ideoita.

Tarkelan mukaan nykytilanteen heikkous on datamarkkinan läpinäkymättömyys. Hänen mukaansa käyttäjällä tai yhteiskunnalla yleensä on hyvin vähän tietoa siitä, mitä datalle ja datalla tehdään sen jälkeen, kun se kerätty ja päätynyt ekosysteemiin. Hänen mielestään datan markkinaan liittyvät riskit ovat ennen kaikkea poliittisia ja juontuvat juuri läpinäkymättömyydestä, joka taas johtaa hänen mukaansa toiminnan kontrolloimattomaan keskittymiseen. Tarkela uskoo, että datan oikeuksia hallitaan tulevaisuudessakin sopimuspohjaisesti, datan hallintaan liittyvät normit pysyvät hajanaisina ja EU:n komissio reagoi ongelmiin pistemäisellä sääntelyllä. Tarkelan mukaan väistämättömät konfliktit olemassa olevien normien kanssa kuitenkin pakottavat julkisen vallan ennen pitkää ottamaan kantaa dataan varallisuuseränä. Nykykeinoilla hänen mukaansa kuitenkin jatketaan, kunnes

tapahtuu jonkinlainen läpimurto tai löytyy motivaatio järjestää datan oikeuksien hallintaan kansainväliset säännöt.

7 Yhteenveto ja johtopäätökset

Tutkimuksen ensimmäisessä osassa selvitettiin puettavilla älylaitteilla kerätyn terveysdatan oikeuksien nykytilannetta ja jakautumista lainopillisessa kirjallisuustutkimuksessa. Datan oikeuksia tarkasteltiin sopimusoikeuden, varallisuusoikeuden ja immateriaalioikeuden sekä henkilötietolainsäädännön näkökulmasta.

Puettavien älylaitteiden käyttö yleistyy koko ajan ja monilla niistä kerätään arkaluonteista, käyttäjän terveyteen liittyvää dataa. Tämä on herättänyt kysymyksiä niin yksityisyydestä ja tietosuojasta kuin kerättyyn dataan liittyvistä oikeuksista ja niiden hallinnasta. Kehittyvät analyysityökalut ja teknologia mahdollistavat yhä tarkemman datan analyysin ja samalla käyttäjän profiloinnin. Laitteet ovat usein kokoaikaisesti kiinni käyttäjässä ja keräävät monenlaista käyttäjän terveyteen ja fysiologiaan liittyvää tietoa, joka on tietosuoja-asetuksessa (GDPR) määriteltyä *arkaluonteista henkilötietoa,* ja jonka kerääminen vaatii laitteen käyttäjän antaman suostumuksen. Laitteiden käyttöön liittyvät sopimukset ovat laitteiden valmistajien tai palveluntarjoajien itsenäisesti laatimia vakioehtosopimuksia, joiden ehtoihin käyttäjä ei voi vaikuttaa, ja joita käyttäjät harvoin edes lukevat. On kyseenalaistaa antaako käyttäjä GDPR:n vaatiman *tietoisen tahdonilmaisun* hyväksyessään käyttöehdot, ja ymmärtääkö hän sopimuksen ja suostumuksen seuraukset henkilötietojensa käytölle.

Kerättyyn dataan ja sen hyödyntämiseen liittyy monien tahojen intressejä. Esimerkiksi yritykset, tutkijat ja valtio haluaisivat käyttäjän terveysdatan hyödynnettäväksi eri tarkoituksiin. Globaalisti hyvinvointi- ja terveysdatan hyödyntämisestä on arvioitu olevan saatavissa jopa 600 miljardin säästöt pelkästään terveydenhuollossa (Manyika et al. 2015, 43). Laitteiden käyttö kuitenkin vaatii käyttäjien luottamusta kerätyn datan tietosuojaan ja rajattuihin käyttötarkoituksiin. Vuonna 2018 voimaan tullut EU:n tietosuoja-asetus (GDPR) on tuonut laitteiden käyttäjille monia oikeuksia kerätyn datan hallintaan ja rajoituksia datan hyödyntämiseen sen kerääjille. Asetuksen käyttäjälle antamia oikeuksia kuitenkin rajaa se, että datan kerääjä eli palveluntarjoaja pitää dataa tosiasiallisesti hallussaan ja voi näin käyttää siihen omistusoikeuden kaltaisia oikeuksia, kuten rajoittaa dataan pääsyä ja hyödyntää dataa taloudellisesti. GDPR antaa myös mahdollisuuden anonymisoida kerätyn datan, minkä jälkeen se rajautuu GDPR:n soveltamisalan ulkopuolelle. Tämä on ongelma käyttäjän oikeuksien kannalta, koska näennäisesti anonymisoidusta tai anonyymistä datasta on monessa tapauksessa pystytty tunnistamaan yksilöitä.

Datan tehokas hyödyntäminen vaatii kuitenkin tarkat määrittelyt datan oikeuksien hallintaan ja tietosuoja-asetuksessa dataa käsitellään lähinnä vain datan tietosuojan, ei sen hyödyntämisen näkökulmasta. Omistusoikeutta on toistuvasti esitetty ratkaisuksi vahvistamaan käyttäjän tietosuojaa, antamaan datan hyödyntämiselle selkeän viitekehyksen ja jakamaan datan arvoa tasaisemmin yhteiskunnassa. Käytännössä datan vaikea määriteltävyys omistuksen kohteena tekee kuitenkin tehtävästä vaikean, jos ei mahdottoman. Jonkinlaiselle datan oikeuksien selventämiselle on kuitenkin tarve, koska epäselvyyden on todettu nostavan kynnystä jakaa ja hyödyntää dataa, ja hidastavan eurooppalaisen datatalouden kehitystä (EU COM 2018, 78).

Tutkimuksen toisessa osiossa tehtiin haastattelututkimus, jossa pyrittiin selvittämään ensimmäisen osassa esille tulleita terveysdatan oikeuksien hallinnan haasteita, vertailtiin kahta mahdollista terveysdatan hallintamallia oikeuksien hallinnan nykytilanteeseen ja kartoitettiin asiantuntijoiden näkemyksiä datan hallinnan kehityksestä. Malleiksi valittiin *omistusoikeus* ja *ihmiskeskeiset datan hallintamallit*. Ihmiskeskeisistä malleista käytettiin esimerkkeinä MyDataa ja Sitran IHAN-hanketta. Tutkimuksessa haastateltiin kuutta datan hallinnan asiantuntijaa eri aloilta ja organisaatioista puolistrukturoiduissa teemahaastatteluissa. Haastateltavien valinnassa pyrittiin monipuoliseen näkemykseen datan hallinnan eri näkökulmista: tietosuojan, yritysten toimintaympäristön, teknologian ja juridiikan asiantuntijoita.

Koska GDPR on tällä hetkellä keskeisimpiä datan oikeuksia määrittelevää sääntelyä, haastattelussa kartoitettiin GDPR:n vaikutuksia yksilön oikeuksiin ja yritysten toimintaympäristöön. Näkemykset erosivat jonkin verran toisistaan. Osan mielestä GDPR on parantanut käyttäjän oikeuksia ja toisten mielestä se on vain lisännyt yksilöiden tietoisuutta olemassa olevista oikeuksista. Yhteistä kaikille näkemyksille oli se, että asetuksen soveltamisen katsottiin olevan vasta alussa ja monia käytännön asioita vielä ratkaisematta. Siirrettävyyden (GDPR 20 artikla) toteutuksessa nähtiin yleisesti olevan ongelmia. Erityisesti se, onko käyttäjällä oikeus siirtää ja viedä mukanaan kerätystä terveysdatasta tehtyjä *ennusteita* ja *arvioita* on epäselvää. Siirrettävän datan rajaaminen on yritysten näkökulmasta haasteellista ja tarvittavien rajapintojen rakentaminen aiheuttaa lisäkustannuksia. Toisaalta älylaitteilla kerätyn datan siirrettävyyden hyötyjä verrattiin toteutuksen ja käytännön toteutus työläyteen ja kustannuksiin. Asetuksen lopullisten vaikutusten ja oikeuksien sisällön odotetaan selkeytyvän oikeuskäytännön ja viranomaisohjeistuksen kautta. Asetuksen puutteiden korvaajaksi esitettiin myös markkinan sisäistä säätelyä. Haastatteluissa nousi esiin asetuksen rajallisuus datan oikeuksien hallinnan välineenä ja datan hyödyntämisen edistäjänä.

Haastateltavien mukaan GDPR:n soveltamisessa yritysten toimintaan on vielä paljon epäselvyyttä ja tuntemattomia tekijöitä, joihin odotetaan tulkintaa niin viranomaisilta kuin oikeuskäytännöstäkin. Asetuksessa nähtiin niin positiivisia kuin negatiivisiakin vaikutuksia yritysten toimintaympäristössä. Sen nähtiin lyhyellä välillä lisänneen yritysten hallinnollista taakkaa, epävarmuutta ja kustannuksia sekä vähentäneen Euroopan houkuttelevuutta investointikohteena. Toisaalta pitkän ajan *sekundääristen* vaikutusten eli sopeutumisen uusiin sääntöihin odotetaan tuovan innovaatioita organisaatioiden ja prosessien tasolla. Asetuksen nähtiin myös olevan Euroopalle mahdollinen kilpailuetu ja lisänneen kiinnostusta GDPR:n kaltaiseen tietosuojasääntelyyn myös globaalilla tasolla.

Datan anonymisoinnin vaikutus käyttäjän oikeuksien rajaajana nousi esiin tutkimuksen ensimmäisessä osassa. Esimerkiksi Kauffman & Soares (2018, 531) ja Purtova (2017, 73;75-76) ovat nähneet anonymisoinnin heikentävän yksilön oikeutta omiin henkilötietoihinsa. Haastatelluilta kysyttiin kuinka isona ongelmana he pitävät yksilöiden tunnistamista anonymisoituna pidetystä datasta. Vastauksissa tunnustettiin anonymisoinnin ongelmat, mutta näkemyksissä painottui enemmän datan hyödyntämismahdollisuuksien tärkeys. Anonymisointi nähtiin murrettavissa olevana suojauksena ja anonyymin ja henkilötiedon rajaa pidettiin epäselvänä, mihin odotettiin ennakkotapauksia tulkinnan tueksi. Toisaalta anonymisointi ja datan hyödynnettävyys nähtiin vastakkaisina ja toisiaan heikentävinä ilmiöinä. Suurin osa näki datan hyödynnettävyyden ja arvon realisoinnin mahdollisia riskejä olennaisempana. Ilmiön aiheuttamien ongelmien ehkäisyyn esitettiin datan hyödyntäjän vastuuta ja rangaistuksia sääntöjen rikkomisesta. GDPR on tuonut tähän yhden työkalun eli *seuraamusmaksun* vakavista tietosuojarikkomuksista.

Tieteellisessä keskustelussa on nostettu esiin datan arvon epätasainen ja käyttäjälle läpinäkymätön jakautuminen. Esimerkiksi Malgieri & Custers (2018, 290; 302) ovat vaatineet palveluntarjoajille velvollisuutta ilmoittaa käyttäjälle hänen henkilötietojensa arvo. Haastateltavat suhtautuivat käyttäjän mahdollisuuteen hyötyä taloudellisesti terveysdatastaan enimmäkseen kriittisesti. Yksittäisen raakadatan arvoa pidettiin hyvin pienenä ja arvon nähtiin syntyvän jalostuksen myötä. Käyttäjälle tuleva hyötyarvo esimerkiksi parempina palveluina nähtiin moninkertaisena mahdolliseen taloudelliseen arvoon nähden. Taloudellisen arvon ei uskottu myöskään toimivan kannustimena jakaa dataa ja esille nousi eettinen kysymys siitä, tekisikö taloudellinen palkkio yksityisyydestä vain varakkaiden luksustuotteen. Lisäksi huomautettiin, että suurienkaan datayritysten arvo käyttäjien määrällä jaettuna ei ole kovin suuri.

Omistusoikeutta on nostettu aika ajoin nostettu esiin ratkaisuna monenlaisiin datatalouden tuomiin ongelmiin, markkinoiden epäonnistumiseen ja ulkoisvaikutuksiin. Mielipiteitä on ollut tieteellisessä keskustelussa niin puolesta (e.g. Tai 2017, 11; Janeček 2018, 1044; Purtova 2017, 77) kuin vastaankin (e.g. Thouvenin et al. 2017, 136-137; Drexl 2018, 2). Ongelmina on nähty esimerkiksi datan arvon epätasainen jakautuminen yhteiskunnallisesti ja yksilön heikentyvä hallinta henkilötietoonsa (Purtova 2017, 77) sekä epäselvien oikeuksien haitta Euroopan datatalouden kasvulle ja datan saatavuudelle (Stepanov 2019, 3). Myös kansainvälisten datajättien dominointi Euroopan markkinalla on nähty ongelmallisena niin yksilön kuin yritysten kannalta (Purtova 2017, 71).

Haastateltavien näkemykset datan mahdollisesta omistusoikeudesta olivat melko tai erittäin kriittisiä. Useimpien mielestä pitäisi puhua ennemmin datan käyttöoikeuksista ja pääsystä dataan. Omistusoikeuden nähtiin olevan hankala ja kömpelö malli datan hallintaan ja eksklusiviteetin tuovan vain lisää ongelmia. Juridisesta näkökulmasta nähtiin kuitenkin, että data pitäisi jotenkin integroida oikeusjärjestelmään, jotta siihen liittyviä oikeuksia voitaisiin käsitellä eri tilanteissa ja oikeuskäytännössä. Datan arvioitiin olevan niin jokapäiväinen ilmiö ja yleinen resurssi, että siihen liittyvien oikeuksien disponointiin ja arvonmääritykseen joudutaan ottamaan ennen pitkää kantaa.

Useimpien haastateltavien mielestä datan omistusoikeutta olennaisempaa on puhua datan käyttöoikeuksista ja hyödynnettävyydestä. Hyödynnettävyyden kannalta olennaista on se, että dataa on hyvin saatavilla kaikille sitä tarvitseville. Nykytilanteessa datan kerääjä on myös sen de facto omistaja, ja useimmat kerääjät näkevät nykyisessä epäselvien sääntöjen tilanteessa datan jakamisen riskit suurempina kuin mahdolliset hyödyt. Toisaalta yritysten välinen datan jakaminen kilpailijoiden kesken on myös kilpailuoikeudellinen riski. Tämän vuoksi haastateltavat peräänkuuluttavat sääntelyä, joka loisi toimivat datan markkinat ja selkeät säännöt datan jakamiselle. Datan kokonaishyötyjen realisoimiseksi yhteiskunnassa tarvitaan heidän mukaansa paitsi laajaa datan keräämistä kaikilla aloilla, myös sen mahdollisimman tehokasta ja asiantuntevaa hyödyntämistä esimerkiksi prosessien ja palveluiden tehostamisessa.

Edellä mainitut datamarkkinoiden epäonnistumiset ja ulkoisvaikutukset kuitenkin vaativat jonkinlaista ratkaisua. Myös ihmiskeskeisiä datan hallintamalleja on esitetty vaihtoehdoksi ratkomaan näitä datatalouden ongelmia.

Haastatteluissa kartoitettiin asiantuntijoiden näkemyksiä ihmiskeskeisistä datan hallintamalleista esimerkkinä MyData ja Sitran IHAN-hanke. MyData on enemmän idean tasolla oleva

yksilökeskeinen datan hallinnan muoto, kun IHAN-hanke taas on konkreettisempi hanke pyrkiä kehittämään viralliset standardoidut määrittelyt *reilulle datataloudelle*. Molempien tavoitteet ovat samankaltaiset eli vahvistaa yksilön käytännön oikeuksia omiin henkilötietoihinsa ja saada data oikeudenmukaisella ja turvallisella tavalla hyödynnettäväksi, niin yksilön, yritysten kuin yhteiskunnankin hyödyksi. Ihmiskeskeiset mallit ovat olleet esillä niin kotimaisessa politiikassa kuin EU:n tuoreessa datastrategiassakin.

Ihmiskeskeisiä malleja pidettiin käyttäjän oikeuksien kannalta yleisesti hyvänä hallintamallina, mutta riskiksi nähtiin yksilön vastuu oman datansa suojaamisessa. Ongelmana pidettiin yksilölle lankeavaa vastuuta suojella omia tietojaan portinvartijana ja mahdollisuus painostaa yksilöä luovuttamaan asiaankuulumattomia henkilötietoja esimerkiksi työhaastattelussa. Yksilön esitettiin potevan *suostumusväsymystä*, jota tällainen portinvartijanrooli voisi mahdollisesti pahentaa ja sitä kautta tuoda riskejä tietosuojaan. Malleihin kuuluva suostumusoperaattori arvioitiin voivan vähentää tätä riskiä. Myös mallin yleistä toteuttamiskelpoisuutta ja soveltuvuutta datan arvon realisoimiseen epäiltiin. Mallin arvioitiin vaativan onnistuakseen lainsäädännöllistä tukea ja vähintään Euroopan laajuista soveltamista. Ongelmana nähtiin myös se, että yksilön suostumus datan käyttöön ja tiettyyn käyttötarkoitukseen ei sido kolmansia osapuolia.

Ihmiskeskeisten mallien edustajat itse suhtautuvat niihin luonnollisesti positiivisesti. He kuitenkin myöntävät, että kehitys on vasta aluillaan ja idea on *vallankumouksellinen.* Malleille uskotaan olevan kysyntää, koska nykyinen markkina on liian keskittynyt, monopolisoitunut ja pyörii liikaa anonyymin datan ympärillä. Heidän mukaansa henkilötieto pitäisi saada tehokkaasti hyödynnettäväksi ja ihmiskeskeiset mallit antaisivat tähän turvallisen ja luotettavat työkalut. Käyttäjien luottamus nähdään säilytettävän datan hyödyntämisen läpinäkyvyydellä ja mahdollisuudella hallita suostumusta myös jälkikäteen. Datan oikeudenmukainen hyödyntäminen nähdään myös osana yritysvastuuta. Ihmiskeskeisissä malleissa ei heidän mukaansa syntyisi myöskään datavarantoja, joihin yksilöllä ei olisi hallinta- ja kielto-oikeuksia. Mallien eduksi esitetään myös se, että datan hyödyntäjät eivät olisi enää riippuvaisia datan kerääjistä tai alustoista, vaan voisivat pyytää datan käyttöoikeuksia suoraan yksilöltä. Tämä mahdollistaisi uusien toimijoiden alalle tulon ja edistäisi kilpailua. He kuitenkin myöntävät, että malli ei voisi koskea vain Suomea, vaan vaatisi laajempaa – vähintään Euroopan – mittakaavaa, joka toisi myös globaalia painetta. Lisäksi tarvittaisiin taloudellisesti houkutteleva liiketoimintamalli vaihtoehdoksi nykyisille mainosrahoitteisille malleille. He uskovat, että mahdollinen muutos tulisi vaatimaan pidemmän aikaa, jopa kymmeniä vuosia.

Terveysdatan hallinta ja oikeuksien kehitys näyttää riippuvan lopulta siitä, painotetaanko enemmän datan hyödyntämistä vai yksilön oikeuksia. Nykymallissa datan kerääjän tosiasiallista omistusta dataan rajaa ensisijaisesti vain tietosuojalainsäädäntö ja käyttäjien tietoisuus oikeuksistaan sekä halu käyttää näitä oikeuksia. Ihmiskeskeiset hallintamallit vakuuttavat turvaavan niin datan tehokkaan hyödyntämisen kuin yksilön tosiasiallisen hallinnan dataansa, mutta mallit ovat niin alkuvaiheessa, että niiden käytännön toimivuutta on vielä vaikea arvioida.

Datan markkina muuttuu koko ajan ja asiantuntijoiden näkemyksiin perustuen muutos tulee olemaan uusi normaali seuraavat vuodet, ellei vuosikymmenet. Ihmiskeskeiset mallit ovat niin alkuvaiheessa, että niiden käytännön potentiaalista löytyy seurattavaa vielä pitkään. Aiheesta löytyy myös muita jatkotutkimusmahdollisuuksia, kuten datan kerääjien markkina-aseman vaikutus terveysdatan jakamiseen ja terveysdatan oikeuksien määrittely oikeustapausten perusteella. Tulevaisuus tuo mitä todennäköisimmin tullessaan eri viranomaisten ja tuomioistuimien kannanottoja terveysdatan asemaan oikeuksien kohteena niin kotimaisella kuin EU:n tasollakin. Jos henkilödatan oikeuksista ei päästä kansainvälisesti selkeään sopimukseen, näiden ennakkotapaukset tulevat lopulta tarkemmin määrittelemään oikeudet terveysdataan.

Lähteet

(Aarnio 2020)
Aarnio, R. 2020. Tietosuojavaltuutetun toimisto. 7.4.2020. *MyData ja tietosuoja lähtökohtana terveyssovellusten suunnittelussa.* https://tietosuoja.fi/artikkeli/-/asset_publisher/mydata-ja-tietosuoja-lahtokohtana-terveyssovellusten-suunnittelussa Viitattu 13.5.2020.

(Alanko & Salo 2013)
Alanko, M. Salo, I. 2014. *Big Data Suomessa.* Liikenne- ja viestintäministeriön julkaisuja 25/2013. http://julkaisut.valtioneuvosto.fi/handle/10024/77955 Viitattu 27.4.2020.

(Anagnoustou & Lambrou 2017)
Anagnostou, M. E., & Lambrou, M. A. 2017. *A review of approaches to the value of privacy*. Ithaca: Cornell University Library, arXiv.org.

(Banerjee et al. 2018)
Banerjee, S. Hemphill, T. Longstreet, P. 2018. *Wearable devices and healthcare: Data sharing and privacy.* The Information Society, 34(1), pp. 49-57. doi:10.1080/01972243.2017.1391912

(Banterle 2018)
Banterle, F. 2018. *Data Ownership in the Data Economy: A European Dilemma.* SSRN Electronic Journal. 10.2139/ssrn.3277330.

(Benvie 2013)
Benvie, D. 2013. *Quantified Self.* Kirjasta: *Share This Too: More Social Media Solutions for PR Professionals.* edited by Rob Brown, and Stephen Waddington, John Wiley & Sons, Incorporated, 2013. ProQuest Ebook Central.

(Drexl et al. 2016)
Drexl, J. Hilty, R. Desaunettes, L. Greiner, F. Kim, D. Richter, H. Surblyte, G. Wiedemann, K. 2016. *Data Ownership and Access to Data - Position Statement of the Max Planck Institute for Innovation and Competition of 16 August 2016 on the Current European Debate*. Max Planck Institute for Innovation & Competition Research Paper No. 16-10. http://dx.doi.org/10.2139/ssrn.2833165

(Drexl 2017)
Drexl, J. *Designing Competitive Markets for Industrial Data – Between Propertisation and Access.* 8 (2017) JIPITEC 257 para 1. https://www.jipitec.eu/issues/jipitec-8-4-2017/4636/JIPITEC_8_4_2017_257_Drexl Viitattu 30.4.2020.

(Drexl 2018)
Drexl, J. 2018. *Data Access and Control in the Era of Connected Devices.* Study on behalf of BEUC.
https://www.beuc.eu/publications/beuc-x-2018-121_data_access_and_control_in_the_area_of_connected_devices.pdf Viitattu 1.5.2020.

(Duch-Brown et al. 2017)
Duch-Brown, N. Martens, B. Mueller-Langer, F. 2017. *The Economics of Ownership, Access and Trade in Digital Data.* Digital Economy Working Paper 2017-01; JRC Technical Reports. SSRN Electronic Journal. 10.2139/ssrn.2914144.

(Dynes 2018)
Dynes, C. 2018. ITProPortal 15.10.2018. *Data ownership: Time to start reading those T&Cs.* https://www.itproportal.com/features/data-ownership-time-to-start-reading-those-tcs/ Viitattu 2.4.2020.

(EDPS 2016)
European Data Protection Supervisor. *Opinion on Personal Information Management Systems Towards more user empowerment in managing and processing personal data.* Opinion 9/2016. https://edps.europa.eu/sites/edp/files/publication/16-10-20_pims_opinion_en.pdf Viitattu 27.4.2020.

(Emam et al. 2011)
Emam, K. E. Jonker, E. Arbuckle, L. & Bradley, M. 2015. *Correction: A systematic review of re-identification attacks on health data.* PLoS One, 10(4) doi:http://dx.doi.org/10.1371/journal.pone.0126772

(EU 2019)
EU2019.fi. 2019. *Principles for a human-centric, thriving and balanced data economy.* https://dataprinciples2019.fi Viitattu 4.6.2020.

(EU 2020)
Euroopan Unioni; Sinun Eurooppasi. 2020. *Tietokantasuoja.* https://europa.eu/youreurope/business/running-business/intellectual-property/database-protection/index_fi.htm Viitattu 2.5.2020.

(EU COM 2015)
European Commission. 6.5.2015. *Digitaalisten sisämarkkinoiden strategia Euroopalle.* Komission tiedonanto euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden Komitealle. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52015DC0192 Viitattu 23.4.2020.

(EU COM 2016)
European Commission. 19.4.2016. *Advancing the Internet of Things in Europe*. Accompanying the document COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS Digitising European Industry Reaping the full benefits of a Digital Single Market. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52016SC0110 Viitattu 27.4.2020.

(EU COM 2017a)
European Commission. 10.1.2017. *Staff Working Document on the free flow of data and emerging issues of the European data economy*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017SC0002 Viitattu 1.5.2020.

(EU COM 2017b)
Euroopan komissio. 10.1.2017. *Komission tiedonanto Euroopan parlamentille, neuvostolle, euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Euroopan datavetoisen talouden rakentaminen.* https://eur-lex.europa.eu/legal-content/FI/TXT/PDF/?uri=CELEX:52017DC0009&from=EN Viitattu 29.4.2020.

(EU COM 2017c)
Euroopan komissio. 10.1.2017. *Ehdotus EUROOPAN PARLAMENTIN JA NEUVOSTON ASETUS yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus)*. https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A52017PC0010 Viitattu 2.6.2020.

(EU COM 2018)
European Commission. 25.4.2018. *Study on emerging issues of data ownership, interoperability, (re-)usability and access to data, and liability* 29.4.2020. https://ec.europa.eu/digital-single-market/en/news/study-emerging-issues-data-ownership-interoperability-re-usability-and-access-data-and Viitattu 17.6.2020.

(EU COM 2020a)
European Commission. 2.6.2020. *The Digital Services Act package.* https://ec.europa.eu/digital-single-market/en/digital-services-act-package Viitattu 2.6.2020.

(EU COM 2020b)
Euroopan komissio. 19.2.2020. *Euroopan datastrategia.* https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_fi Viitattu 3.6.2020.

(EU COM 2020c)
European Commission. 6.5.2020. *Common European data spaces for Smart Manufacturing.* https://ec.europa.eu/digital-single-market/en/news/common-european-data-spaces-smart-manufacturing-0 Viitattu 3.6.2020.

(EU COM 2020d)
Euroopan komissio. 19.2.2020. *Komission tiedonanto Euroopan parlamentille, neuvostolle, euroopan talous- ja sosiaalikomitealle ja alueiden komitealle. Euroopan datastategia.* https://ec.europa.eu/transparency/regdoc/rep/1/2020/FI/COM-2020-66-F1-FI-MAIN-PART-1.PDF Viitattu 3.6.2020.

(Erkinheimo 2019)
Erkinheimo, P. 2019. *Suomesta on tehtävä Omadatan suurvalta – Olemme antaneet arvokkaan datamme amerikkalaisille ja kiinalaisille verkkojäteille.* Tekniikka ja Talous 5.1.2019. https://www.tekniikkatalous.fi/uutiset/suomesta-on-tehtava-omadatan-suurvalta-olemme-antaneet-arvokkaan-datamme-amerikkalaisille-ja-kiinalaisille-verkkojateille/7e18d7ad-87c8-4c4b-891b-b3bd15696585 Viitattu 12.4.2020.

(Eskola & Suoranta 1999)
Eskola, J, Suoranta, J. 1999. *Johdatus laadulliseen tutkimukseen.* Vastapaino. ISBN 951-768-035-X

(Floridi & Taddeo 2016)
Floridi, L. & Taddeo, M. 2016. *What is data ethics?* Philosophical transactions. Series A, Mathematical, physical, and engineering sciences, 374(2083). doi:10.1098/rsta.2016.0360

(Garcia Martinez 2019)
Garcia Martinez, A. 2019. Wired 26.2.2019. *No, Data Is Not The New Oil*. https://www.wired.com/story/no-data-is-not-the-new-oil/ Viitattu 2.4.2020

(Gillham 2005)
Gillham, B. 2005. *Research Interviewing : The Range of Techniques.* McGraw-Hill Education. ProQuest Ebook Central, https://ebookcentral.proquest.com/lib/aalto-ebooks/detail.action?docID=287863.

(Halenius 2020)
Halenius, L. 2020. *The European Commission's new data strategy paves the way for a fair data economy.* https://www.sitra.fi/en/blogs/the-european-commissions-new-data-strategy-paves-the-way-for-a-fair-data-economy/ Viitattu 4.6.2020.

(Harenko et al. 2016b)
Harenko, K. Niiranen, V. Tarkela, P. 2016. *Tekijänoikeus.* AlmaTalent. ISBN 978-952-14-2513-4

(Herschel & Miori 2017)
Herschel, R. & Miori, V. M. 2017. *Ethics & Big Data.* Technology in Society, 49, pp. 31-36. doi:10.1016/j.techsoc.2017.03.003

(Hirsjärvi & Hurme 2000)
Hirsjärvi, S. & Hurme, H. 2000. *Tutkimushaastattelu - Teemahaastattelun teoria ja käytäntö.* Helsinki University Press. ISBN 951-570-458-8

(Honkinen et al. 2016)
Honkinen, T. Innanen, A. Lindgren, J.Pello, J. Rantanen, J. Siltala, K. Tuomala, S. 2016. *Startup-juridiikan käsikirja.* Alma-Talent. ISBN 978-952-14-2921-7

(Holst 2020)
Holst, A. 2020. *Wearable Technology – Statistics & Facts.* Statista. 9.3.2020. https://www.statista.com/topics/1556/wearable-technology/#dossierSummary__chapter5 Viitattu 7.4.2020.

(Hukkanen 2018)
Hukkanen, V. 2018. Yle Uutiset 29.8.2018. *Suomalainen start-up rakentaa Facebookin kilpailijaa – Suomesta halutaan henkilötiedon "muumilaakso" vastaiskuna Piilaakson jäteille.* https://yle.fi/uutiset/3-10374480 Viitattu 12.4.2020.

(HUS 2016)
HUS 27.4.2016. *Helsingin Biopankista kehitetään suurta lääketieteen innovaatioiden veturia.* https://www.hus.fi/hus-tietoa/uutishuone/uutisarkisto/Sivut/Helsingin-Biopankista-kehitetään-suurta-lääketieteen-innovaatioiden-veturia.aspx Viitattu 2.4.2020.

(Isaak & Hanna 2018)
Isaak, J. & Hanna, M. J. 2018. *User Data Privacy: Facebook, Cambridge Analytica, and Privacy Protection.* Computer, 51(8), pp. 56-59. doi:10.1109/MC.2018.3191268

(Janeček 2018)
Janeček, V. 2018. *Ownership of personal data in the Internet of Things.* Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(5), pp. 1039-1052. doi:10.1016/j.clsr.2018.04.007

(Johnson 2007)
Johnson, D.R. 2007. *Reflections On The Bundle Of Rights.* Vermont Law Review. pp. 32. 247-272.

(Jülicher & Delisle 2018)
Jülicher, T. & Delisle, M. 2018. *Step into "The Circle"—A Close Look at Wearables and Quantified Self.* 10.1007/978-3-319-62461-7_10. Kirjasta Hoeren, T. & Kolany - Raiser, B. 2017. *Big Data in Context: Legal, Social and Technological Insights.*

(Kailio 2018)
Kailio, A. 2018. *Sinun datasi, sinä päätät.* https://www.tivi.fi/uutiset/sinun-datasi-sina-paatat/0653e1a9-4885-3da0-a6bb-30d617acf6fb%20 Viitattu 17.6 2020.

(Kaisto & Lohi 2013)
Kaisto, J. Lohi, T. 2013. *Johdatus varallisuusoikeuteen.* AlmaTalent. ISBN 978-952-14-2244-7

(Kaisto & Tepora 2012)
Kaisto, J. Tepora, J. 2012. *Esineoikeus eurooppalaistuvassa Suomessa.* Lakimiesliiton kustannus. ISBN 978-952-246-176-6

(Kanta-palvelut 2019)
Kanta-palvelut.Kansaneläkelaitos. 2019. 31.12.2019. *Hyvinvointitiedot Omatietovarannossa.* https://www.kanta.fi/web/guest/hyvinvointitiedot Viitattu 3.4.2020.

(Kauffman & Soares 2018)
Kauffman, M. E. & Soares, M. N. 2018. *New Technologies and Data Ownership: Wearables and The Erosion of Personality Rights.* Revista Direitos Sociais e Políticas Públicas *(UNIFAFIBE), 6*(1), s.21. doi:10.25245/rdspp.v6i1.444

(Komulainen 2020)
Komulainen, J. 2020. *Asiakastietolaki uudistuu.* 8.3.2020. STM. https://stm.fi/documents/1271139/20600699/Komulainen+Joni_Asiakastietolain+tilannekatsaus.pdf/154a4d20-52f6-198e-eec2-112024606a06/Komulainen+Joni_Asiakastietolain+tilannekatsaus.pdf Viitattu 3.4.2020.

(Koronacki et al. 2010)
Koronacki, J. et al. 2010. *Advances in Machine Learning II, Dedicated to the Memory of Professor Ryszard S. Michalski.* 10.1007/978-3-642-05179-1.

(Kuoppamäki 2018)
Kuoppamäki, P. 2018. *Uusi kilpailuoikeus.* AlmaTalent. ISBN 978-952-14-3117-3

(Kurppa 2017)
Kurppa, T.2017. *Itsensä mittaaminen ja biohakkerointi.* 2.11.2017. Turun sanomat. https://www.ts.fi/puheenvuorot/3712637/Itsensa+mittaaminen+ja+biohakkerointi Viitattu 13.4.2020.

(Kääriä 2018)
Kääriä, S. 2018. *Data-analytiikka mahdollistaa terveydenhuollon uudistamisen*. https://aureolis.com/analytiikka/data-analytiikka/ Viitattu 3.4.2020.

(LVM 2020)
Liikenne- ja viestintäministeriö. 2020. *LVM2020-00037. Perusmuistio.* https://www.eduskunta.fi/FI/vaski/Liiteasiakirja/Documents/EDK-2020-AK-295429.pdf Viitattu 6.6.2020.

(Malgieri 2016)
Malgieri, G. 2016, *"Ownership" Of Customer (Big) Data In The European Union: Quasi-Property As Comparative Solution?*", Journal of Internet Law*,* vol. 20, no. 5, s. 3-17.

(Malgieri & Comandé 2017)
Malgieri, G. Comandé, G. 2017. *Sensitive-by-distance: quasi-health data in the algorithmic era.* Information & Communications Technology Law, 26:3, 229-249. doi:10.1080/13600834.2017.1335468

(Malgieri & Custers 2018)
Malgieri, G. & Custers, B. 2018. *Pricing privacy – the right to know the value of your personal data.* Computer Law & Security Review: The International Journal of Technology Law and Practice, 34(2), pp. 289-303. doi:10.1016/j.clsr.2017.08.006

(Manyika et al. 2015)
Manyika et al. 2015. *The Internet Of Things: Mapping The Value Beyond The Hype.* McKinsey&Company. https://www.mckinsey.com/~/media/McKinsey/Industries/Technology%20Media%20and%20Telecommunications/High%20Tech/Our%20Insights/The%20Internet%20of%20Things%20The%20value%20of%20digitizing%20the%20physical%20world/The-Internet-of-things-Mapping-the-value-beyond-the-hype.ashx
Viitattu 3.4.2020.

(Mattern & Floerkemeier 2010)
Mattern, F. & Floerkemeier, C. 2010. *From the Internet of Computers to the Internet of Things.* Informatik-Spektrum. 33. 242-259. 10.1007/978-3-642-17226-7_15. Kirjasta Sachs, Kai & Petrov, Ilia & Guerrero, Pablo. (2010). From Active Data Management to Event-Based Systems and More. 10.1007/978-3-642-17226-7. Viitattu 17.6.2020.

(McKean 2014)
McKean, J. 2014. *Customer's New Voice: Extreme Relevancy and Experience Through Volunteered Customer Information.* John Wiley & Sons, Incorporated. ISBN 9781119004363

(Mikkola 2017)
Mikkola, T. 2017. *Yhteisomistus.* AlmaTalent. ISBN 978-952-14-2848-7

(MyData 2018)
MyData.org. 2018. https://mydata.org/about/ Viitattu 13.4.2020.

(MyData.org 2020)
MyData.org. 2020. https://mydata.org/declaration/ Viitattu 31.5.2020.

(Niilola 2019)
Niilola, M. 2019. Yle Uutiset 14.6.2019. *Selvitys antaa karun kuvan tietosuojauudistuksesta – Annatko sinäkin riskillä ja summassa suostumuksen tietojesi käyttöön?* https://yle.fi/uutiset/3-10828341 Viitattu 17.4.2020.

(Norrgård, 2008)
Norrgård, M. 2008. *Patentin loukkaus.* AlmaTalent. ISBN 978-952-63-2812-6

(Oesch 2008)
Oesch, R. 2008. *Tekijänoikeus, kuluttaja ja Lex Karpela.* s.4-27. Kirjassa: toim. Oesch, R. Heiskanen, H. Hyyrynen, O. 2008. *Tekijänoikeus ja digitaalitalous.* AlmaTalent. ISBN 978-952-63-2840-9

(Oesch 2017)
Oesch, R. 2017. *Johdatus aiheeseen: yleinen etu ja immateriaalioikeuden suoja – mitä uutta?* s. 1-19. Kirjassa: toim. Oesch, R. Eloranta, M. Heino, M. Kokko, N. 2017. *Immateriaalioikeudet ja yleinen etu.* AlmaTalent Oy. ISBN 978-952-14-3071-8

(Osborne Clarke LLP 2016)
Osborne Clarke LLP. European Commission. 28.11.2016. *Legal study on ownership and access to data*. https://op.europa.eu/en/publication-detail/-/publication/d0bec895-b603-11e6-9e3c-01aa75ed71a1 Viitattu 30.4.2020.

(Ovaskainen 2018)
Ovaskainen, T. 2018. Uusi Suomi 27.1.2018. https://www.uusisuomi.fi/uutiset/asiantuntija-varoittaa-suomea-google-petti-raikeasti-lupauksensa-terveystiedot-lipuvat-helposti-vaaraan-kayttoon/2722e03a-2e8c-3e5f-b3ad-3e7c54fd5700 Viitattu 2.4.2020.

(Paul & Irvine 2014)
Paul, G. & Irvine, J. 2014. *Privacy Implications of Wearable Health Devices.* AMC Digital Library. https://doi.org/10.1145/2757302.2757306 Viitattu 7.6.2020.

(Poikola 2020)
Poikola, A. 2020. Teknologiateollisuus 28.1.2020. *Omadata toisi valtavasti hyötyjä ihmisten arjen asiointiin - lainsäädännön esteet purettava.* https://www.uusisuomi.fi/uutiset/asiantuntija-varoittaa-suomea-google-petti-raikeasti-lupauksensa-terveystiedot-lipuvat-helposti-vaaraan-kayttoon/2722e03a-2e8c-3e5f-b3ad-3e7c54fd5700 Viitattu 13.4.2020.

(Poikola et al. 2018)
Poikola, A. Kuikkaniemi, K. Kuittinen, O. Honko, H. Nuutila, A. 2018. *My Data – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen.* Liikenne- ja viestintäministeriön julkaisu 3/2018. ISBN 978-952-243-418-0 http://julkaisut.valtioneuvosto.fi/handle/10024/160954

(Purtova 2017)
Purtova, N. 2017. *Do Property Rights in Personal Data Make Sense After the Big Data Turn?* 경제규제와 법, 10(2), pp. 208-222.

(Purtova 2018)
Purtova, N. 2018. *The law of everything: Broad concept of personal data and future of EU data protection law.* Law, Innovation and Technology, 10(1), pp. 40-81. doi:10.1080/17579961.2018.1452176

(Sankari & Wiberg 2019)
Sankari, V. & Wiberg, M. *GDPR ei toimi: Tietosuojakäytännöt eivät noudata asetusta.* Turun yliopisto. Yhteiskuntapolitiikka. Julkaisu 84:3.
http://www.julkari.fi/handle/10024/138277 Viitattu 17.6.2020.

(Savonen 2020)
Savonen, S. 2020. *Suomalaisesta älyratkaisusta toivottaisiin löytyvän ratkaisu koronan havaitsemiseen – ”me ei olla mikään koronadiagnostinen firma”.* Tekniikka ja talous 25.3.2020.
https://www.tekniikkatalous.fi/uutiset/suomalaisesta-alyratkaisusta-toivottaisiin-loytyvan-ratkaisu-koronan-havaitsemiseen-me-ei-olla-mikaan-koronadiagnostinen-firma/00b50c2c-a64a-4d04-b14c-a45c1ee106b9/ Viitattu 2.4.2020

(Statista 2020)
Statista 2020. *Number of connected wearable devices worldwide from 2016 to 2022*
https://www.statista.com/statistics/487291/global-connected-wearable-devices/ Viitattu 2.4.2020

(Stepanov 2019)
Stepanov, I. 2019. *Introducing a property right over data in the EU: The data producer's right - an evaluation.* International Review of Law, Computers & Technology, 34(1), pp. 65-86. doi:10.1080/13600869.2019.1631621

(Silbert 2019)
Silbert, S. 2019. *All the Things You Can Track With Wearables.* https://www.lifewire.com/what-wearables-can-track-4121040 Viitattu 12.4.2020.

(Singh & Vipra 2019)
Singh, P. & Vipra, J. 2019. *Economic Rights Over Data: A Framework for Community Data Ownership. Development (Basingstoke), 62*(1-4), s.1. doi:10.1057/s41301-019-00212-5

(Sitra 2020)
Sitra. 22.1.2020. *IHAN-blueprint.* https://www.sitra.fi/artikkelit/ihan-blueprint/ Viitattu 5.6.2020.

(Socolow & Jolly 2017)
Socolow, B. R. & Jolly, I. 2017. *Game-changing wearable devices that collect athlete data raise data ownership issues.* World Sports Advocate*, 15*(7), s. 15-17.

(Sorvari 2007)
Sorvari, K. 2007. *Tekijänoikeuden loukkaus.* AlmaTalent. ISBN 978-952-63-2839-3

(STM 2016)
STM. 2016. 14.6.2016. *Hallitus luo edellytyksiä terveystoimialojen osaamispohjaiselle kasvulle.*
https://valtioneuvosto.fi/artikkeli/-/asset_publisher/1271139/hallitus-luo-edellytyksia-terveystoimialojen-osaamispohjaiselle-kasvulle
Viitattu 2.4.2020

(Suomalainen 2019)
Suomalainen, K. 25.6.2020. *Hyvinvointidata avuksi varusmiesten kuntotalkoisiin.* https://www.sitra.fi/artikkelit/hyvinvointidata-avuksi-varusmiesten-kuntotalkoisiin/ Viitattu 8.6.2020.

(Suomalainen 2020)
Suomalainen, K. 2.4.2020. *Reilun datatalouden standardisointityö etenee.* https://www.sitra.fi/uutiset/reilun-datatalouden-standardisointityo-etenee/ Viitattu 7.6.2020.

(Boyd 2018)
Boyd, D. 2018. Sports Tech Group 15.10.218. *The Great Debate: Athlete Data - Who Owns It?* https://www.sportstechgroup.co/sports-tech-education/athlete-data Viitattu 2.4.2020.

(Tai 2018)
Tai, E. T. T. 2018. *Data ownership and consumer protection.* Journal of European Consumer and Market Law, 7(4), pp. 136-140.

(Takki & Halonen 2017)
Takki, P & Halonen, S. 2017. *IT-sopimukset – Käytännön käsikirja.* AlmaTalent Helsinki. ISBN 978-952-14-3206-4

(Terveystalo 2018)
Terveystalo. 6.4.2018. *Yli kolmannes suomalaisista mittaa terveystietojaan – digitaalisilla palveluilla suuri potentiaali asiantuntijoiden ja potilaiden vuorovaikutuksen kehittämisessä.* https://www.terveystalo.com/fi/Ajankohtaista/Uutiset/Yli-kolmannes-suomalaisista-mittaa-terveystietojaan--digitaalisilla-palveluilla-suuri-potentiaali-asiantuntijoiden-ja-potilaiden-vuorovaikutuksen-kehittamisessa/ Viitattu 7.6.2020.

(Thouvenin et al. 2017)
Thouvenin, F., Weber, R. H. & Fr¨Uh, A 2017. *Data ownership: Taking stock and mapping the issues.* 10.1201/9781315156408-4. Kirjasta Frontiers in Data Science.

(Trakman et al. 2019)
Trakman, L., Walters, R. & Zeller, B. 2019. *Is Privacy and Personal Data Set to Become the New Intellectual Property?* IIC - International Review of Intellectual Property and Competition Law, 50(8), pp. 937-970. doi:10.1007/s40319-019-00859-0

(TSV 2019)
Tietosuojavaltuutetun toimisto. 15.10.2019. *Tietosuojavaltuutetun seuraamuskollegio aloitti työnsä – vireille tulevien asioiden määrä tasaantuu.* Tiedote. https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetun-seuraamuskollegio-aloitti-tyonsa-vireille-tulevien-asioiden-maara-tasaantuu Viitattu 17.6.2020.

(TSV 2020)
Tietosuojavaltuutetun toimisto. 22.5.2020. *Tietosuojavaltuutetun toimiston seuraamuskollegio määräsi kolme seuraamusmaksua tietosuojarikkomuksista.* Tiedote. https://tietosuoja.fi/artikkeli/-/asset_publisher/tietosuojavaltuutetun-toimiston-seuraamuskollegio-maarasi-kolme-seuraamusmaksua-tietosuojarikkomuksista Viitattu 31.5.2020.

(Tuomi & Sarajärvi, 2002)
Tuomi, J. & Sarajärvi, A. 2002. *Laadullinen tutkimus ja sisällönanalyysi.* Kustannusosayhtiö Tammi. ISBN 951-26-4856-3

(UIC)
UIC. Big Data and Wearable Health Monitors: Harnessing the Benefits and Overcoming Challenges https://healthinformatics.uic.edu/blog/big-data-and-wearable-health-monitors-harnessing-the-benefits-and-overcoming-challenges/ Viitattu 7.4.2020.

(Ulander et al. 2019)
Ulander, M. Ahomäki, M. Laukkanen, J. 2019. *Eurooppalaisten yritysten tulevaisuus datataloudessa.* Sitra. https://media.sitra.fi/2019/09/18132601/eurooppalaisten-yritysten-tulevaisuus-datataloudessa.pdf Viitattu 6.6.2020

(Valkama 2019)
Valkama, H. 2019. *Uusi viranomainen alkaa välittää suomalaisten potilastietoja eteenpäin, mutta lupaa yksityisyyden suojan olevan turvattu.*
https://yle.fi/uutiset/3-11133001 Viitattu 2.4.2020.

(Valkjärvi 2017)
Valkjärvi, A. 2017. *Henkilötietoja sisältävä tietokanta – konflikti immateriaalioikeuden hyödyntämisen ja henkilötietojen suojan välillä.* s.127-167 Kirjassa: Oesch, R. Eloranta, M. Heino, M. Kokko, N. 2017. *Immateriaalioikeudet ja yleinen etu.* AlmaTalent Oy. ISBN 978-952-14-3071-8

(Valtioneuvosto 2017)
Valtioneuvosto 14.8.2017. Valtioneuvoston viestintäosasto. *Terveystiedosto uutta tutkimusta ja liiketoimintaa* https://valtioneuvosto.fi/artikkeli/-/asset_publisher/10616/terveystiedosta-uutta-tutkimusta-ja-liiketoimintaa/ Viitattu 2.4.2020

(van Erp 2017)
van Erp, S. 2017. Ownership of data: The numerus clausus of legal objects. Brigham-Kanner Property Rights Conference Journal, 6, pp. 235-257.

(Venhe 2020)
Venhe, N. 2020. *Itsensä mittaaminen antaa illusion elämänhallinnasta.* Itä-Suomen Yliopisto. https://www.uef.fi/fi/artikkeli/itsensa-mittaaminen-antaa-illuusion-elamanhallinnasta Viitattu 27.4.2020.

(Western Digital 2020)
Western Digital 2020. *Dawn Of The Data Marketplace – Data Makes Possible.*
https://datamakespossible.westerndigital.com/value-of-data/dawn-of-data-marketplace/ Viitattu 3.4.2020.

(Zech 2015)
Zech, H. 2015. *Information as Property*. JIPITEC 6 (3) 2015, 192 SSRN:
https://ssrn.com/abstract=2731076 Viitattu 26.4.2020.

(Zhang 2018)
Zhang, S. 2018. *Who Owns The Data Generated By Your Smart Car?* Harvard Journal of Law & Technology. Volume 32, Number 1 Fall 2018

(Zitting 1951)
Zitting, Simo. 1951. *Omistajanvaihdoksesta silmällä pitäen erityisesti lainhuudatuksen vaikutuksia.* Suomalaisen lakimiesyhdistyksen julkaisuja. A-sarja N:o 43.

Liitteet

Liite 1. Teemahaastattelurunko

Näkökulmani aiheeseen on kuluttajille suunnatulla, puettavalla älylaitteella kerätyn datan oikeuksien nykytilanne ja erilaisten hallintamuotojen vaikutus yksilön oikeuksiin, yritysten toimintamahdollisuuksiin ja yhteiskunnalliseen etuun.

Määritelmät

Käyttäjällä tarkoitetaan puettavan älylaitteen kuten älykellon käyttäjää kuluttajana.

Terveysdatalla tarkoitetaan käyttäjän terveyteen liittyvää henkilötietoa tietosuoja-asetuksen määritelmää mukaillen.

Palveluntarjoajalla tarkoitetaan puettavan laitteen valmistajaa tai laitteeseen liittyvän digitaalisen palvelun tarjoajaa, jos tämä on eri kuin laitteen valmistaja. Käyttäjän dataa keräävä taho, jonka kautta data päätyy ekosysteemiin.

Yksilön oikeudet

Miten tietosuoja-asetus on vaikuttanut käyttäjän toteutuneisiin oikeuksiin?

Onko tietosuoja-asetuksen antamat oikeudet riittävät käyttäjän kannalta nyt tai tulevaisuudessa (haastateltavan arvio)?

Kuinka suuri ongelma käyttäjän ja yhteiskunnan kannalta on mahdollinen tunnistettavuus anonymisoidusta terveysdatasta?

Pitäisikö käyttäjien pystyä estämään omista henkilötiedoista anonymisoidun tiedon/datan käyttäminen mahdollisen tunnistamisen vuoksi? Miten estäminen olisi mahdollista?

Onko käyttäjällä oikeuksia (GDPR) myös raakadatasta (kuten käyttäjän syke, hengitystiheys, lämpötila) pääteltyyn ja ennakoituun terveyteen liittyvään informaatioon (kuten sairastumisriski, hedelmällisyys, eliniänodote)? Pitäisikö olla?

Miten käyttäjän omistusoikeus omaan dataansa vaikuttaisi käyttäjän tietosuojaan ja muihin oikeuksiin?

Voisiko ja pitäisikö käyttäjän hyötyä omasta terveysdatasta taloudellisesti?

Miten käyttäjiä voidaan kannustaa kiinnostumaan henkilötietojensa käytöstä, kun käytännössä he vain haluavat palvelun/informaation ja luovuttavat tietonsa sen saamiseksi?

Yritysten kilpailukyky ja vapaa kilpailu

Millaisia vaikutuksia tietosuoja-asetuksella on ollut suomalaisten ja eurooppalaisten yritysten kilpailukykyyn verrattuna muuhun maailmaan?

Onko nykytilanne datan oikeuksien/omistuksen suhteen riittävä käyttäjän/palveluntarjoajan/muun ekosysteemin kannalta/yhteiskunnan etujen kannalta?

Millainen käyttäjän datan oikeuksien järjestäminen lisäisi suurien datayritysten kannustimia jakaa dataa pienten toimijoiden kanssa?

Mitkä asiat ovat esteenä tai hidasteena eurooppalaisten dataintensiivisten yritysten kasvulle ja kilpailulle kansainvälisten suurien datayritysten kanssa?

Miten estetään EU:n ja sen kansalaisten sekä yritysten jääminen kansainvälisten datajättien, kuten Apple ja Huawei, hyödynnettäväksi resurssiksi?

Miten paikalliset ilmiöt, kuten suomalainen/eurooppalainen MyData ja Sitran IHAN-standardi reilusta datataloudesta, vaikuttavat yritysten kilpailukykyyn, jos ne noudattavat sellaisia tai jos ne tulisivat pakollisiksi? Miten tällaiset standardit pakollisina vaikuttaisivat eurooppalaisten yritysten kilpailukykyyn suuria datayrityksiä vastaan?

Yhteiskunnan etu ja oikeudenmukaisuus

Pitäisikö datan arvoketjun olla läpinäkyvämpi? Miten sen voisi toteuttaa?

Miten datan arvoa voisi jakaa käyttäjän ja yhteiskunnan kannalta sekä globaalisti tasa-arvoisemmin?

Millaisia hyötyjä ja riskejä mahdollinen kodifioitu omistusoikeus toisi yksilön/yritysten/yhteiskunnan näkökulmasta?

Millaisia tulevaisuuden riskejä on datan omistusoikeuden säätämisellä/sillä ettei sitä säädetä?

Ovatko yksilön ja yhteiskunnan edut datan hyödyntämisen suhteen ristiriidassa ja jos ovat, millainen datan hyödyntämisen malli olisi hyvä kompromissi molempien etujen suojelemiseksi?

Mitkä ovat mahdolliset kehityspolut nykyisestä datan hallinnan tilanteesta ja mikä olisi yhteiskunnallisesti tutkimuksen, vaihdannan ja investointien kannalta ideaali kehityspolku?