LIIKENNE- JA VIESTINTÄMINISTERIÖ

Antti Poikola
Kai Kuikkaniemi
Ossi Kuittinen
Harri Honko
Aleksi Knuutila

MyData

– johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen

MyData

– johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen

Antti Poikola | Kai Kuikkaniemi | Ossi Kuittinen
Harri Honko | Aleksi Knuutila

MyDatalla (myös omadata) tarkoitetaan yhtäältä ihmiskeskeisiä henkilötiedon hallinta- ja hyödyntämismalleja, joissa ihmisille annetaan oikeus omaan dataansa ja toisaalta tällaisten mallien mukaisesti hallinnoitua henkilötietoa. Lähtökohtana on, että ihmiset itse voivat hyödyntää, hallita ja luvittaa eteenpäin heistä kerättyä dataa kuten ostos-, liikkumis-, talous- tai terveystietoja. Ihmiskeskeisellä datan hallinnalla luodaan yhteentoimivuutta ja minimoidaan palvelulukkojen syntymistä dataa hyödyntävien alustojen kehittyessä. Malli sovittaa yksilön oikeudet ja korkeat tietosuojavaatimukset yhteen datan saatavuuden edistämisen ja liiketoiminnan kanssa.

MyData on kansainvälinen kehitysvaiheessa oleva ilmiö, malli ja tulevaisuusskenaario, jonka ympärille on kertymässä kasvavaa vauhtia teknologiaa ja liiketoimintaa. Mallin yleistyminen voi merkittävästi nopeuttaa datatalouden kehitystä ja avointen ekosysteemien syntymistä erityisesti vahvan tietosuojan ympäristöissä.

Kansainvälinen MyData-toimijoiden yhteisö julkaisi vuonna 2017 tavoitteet ja periaatteet[1], joiden pääkohdat on suomennettu alla.

MyData tavoitteet: Minkä tulee muuttua?

Muodollisista käytännöllisiin oikeuksiin

Tavoitteena on, että pääsy omiin tietoihin, tietojen oikaiseminen ja siirrettävyys, sekä oikeus tulla unohdetuksi kehittyvät “yhden klikkauksen oikeuksiksi”, jotka ovat yhtä yksinkertaisia ja tehokkaita käyttää kuin tämän päivän ja huomisen parhaat verkkopalvelut.

Tietosuojasta tiedolla voimaantumiseen

Tietosuoja-sääntely ja yritysten yksityisyyskäytännöt on suunniteltu suojaamaan ihmisiä, etteivät organisaatiot väärinkäyttäisi heidän henkilötietojaan. Tämä on tärkeää tulevaisuudessakin ja lisäksi yleisiä toimintatapoja tulee muuttaa suuntaan, jossa yksilöitä sekä suojellaan, mutta myös voimaannutetaan käyttämään dataa, jota organisaatioilla on heistä.

Suljetuista avoimiin ekosysteemeihin

Tämän päivän datatalous tuottaa verkostoefektejä, jotka hyödyntävät alustatoimijoita, joilla on mahdollisuus kerätä ja käsitellä suuria määriä henkilötietoja. Antamalla yksilöiden määrätä mitä heidän datalleen tapahtuu, pyrimme luomaan todellista datan vapaata liikkuvuutta, tasapainoa, oikeudenmukaisuutta, monipuolisuutta ja kilpailua digitaaliseen talouteen.

MyData-periaatteet

Ihmiskeskeinen henkilötiedon hallinta	**Datan siirrettävyys ja uudelleenkäyttö**
Ihminen oman datansa yhdistäjänä	**Läpinäkyvyys ja luotettavuus**
Ihmisten voimaantuminen	**Yhteentoimivuus**

https://mydata.org/declaration

1 https://mydata.org/declaration Tämän selvityksen ensimmäisessä painoksessa (2014) MyData-periaatteet esitettiin hieman eri muodossa, mutta samat ajatukset sisältyvät myös kansainväliseen julkilausumaan.

Tiivistelmä

Tiivistelmään on koottu selvityksen kaikki kuvat pienoiskoossa ja kerrottu lyhyesti kunkin kuvan ydinviesti. Kuvamateriaali on julkaistu myös uudelleenkäytön sallivalla Creative Commons -lisenssillä osoitteessa **okf.fi/mydata-selvitys-2018**

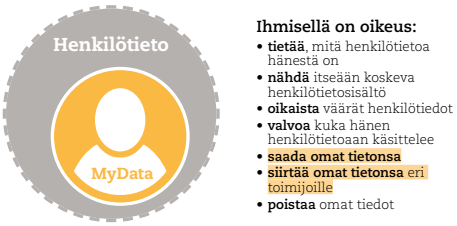
Johdanto / Kuva 0.1 / s. 18

Termillä MyData viitataan ensinnäkin ilmiöön ja ajattelutavan muutokseen, jossa henkilötiedon hallintaa ja käsittelyä pyritään viemään nykyisestä organisaaatiokeskeisestä mallista **ihmiskeskeiseksi**. Toisaalta MyDatalla viitataan henkilötietoon resurssina, jota ihmiset voivat itse hyödyntää. Mikäli ihmisellä ei ole mahdollisuutta hyödyntää itse jonkun muun hänestä keräämää henkilötietoa, niin sitä ei voida kutsua MyDataksi.

Johdanto / Kuva 0.2 / s. 19

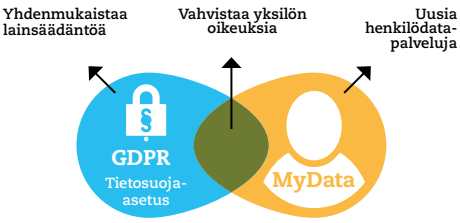
MyData-ajattelu tuo datan hyödyntämisnäkökulman tasavertaisena yksityisyydensuojan rinnalle niin, että hyödyt maksimoidaan ja yksityisyydensuojan heikkeneminen minimoidaan. Tähän pyritään tarjoamalla ihmisille mahdollisuuksia hyödyntää itse omaa dataansa sekä keinoja hallita, kuinka dataa kerätään, jalostetaan, hyödynnetään ja jaetaan edelleen.

Luku 1. / Kuva 1.1 / s. 23



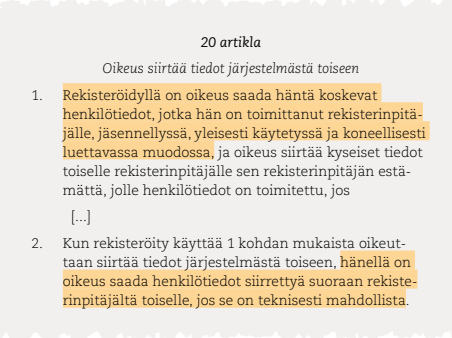
MyData on **henkilötiedon osajoukko.** Kaikki MyData on henkilötietoa, mutta kaikki henkilötieto ei ole MyDataa. Oikeudet ja hallinnan taso, jotka ihmisillä on omiin tietoihinsa, voivat vaihdella eri tilanteissa. MyDatasta voidaan puhua silloin, kun ihmisillä on oikeus ja käytännön mahdollisuus saada omat tietonsa itselleen, käyttää niitä vapaasti ja siirtää halutessaan kolmansille osapuolille.

Luku 1. / Kuva 1.2 / s. 26



EU:n tietosuoja-asetuksen (EU General Data Protection Regulation, GDPR) ja MyDatan tavoitteet ovat osin yhteneviä. MyData-käytännöillä pyritään siihen, että ihmisten oikeuksista tulee käytännössä helppoja ja hyödyllisiä ja että määräysten toteuttaminen on joustavaa ja helppoa organisaatioille.

Luku 1. / Kuva 1.3 / s. 27



20 artikla

Oikeus siirtää tiedot järjestelmästä toiseen

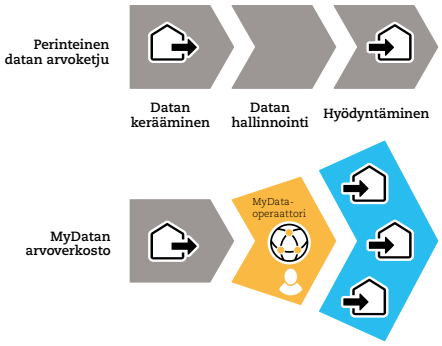
1. Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu, jos

   [...]

2. Kun rekisteröity käyttää 1 kohdan mukaista oikeuttaan siirtää tiedot järjestelmästä toiseen, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista.

Tietosuoja-asetuksen 20. artikla tuo ihmisille uuden oikeuden ladata omia tietojaan joko itselleen tai siirtää suoraan palvelujen välillä. Tällä oikeudella pyritään varmistamaan, ettei datan keruusta tule palvelujen välistä kilpailua rajoittava tekijä, vaan että ihmisillä on mahdollisuus vapaasti valita kilpailevien palveluntarjoajien välillä ja siirtää myös tietonsa mukanaan, mikäli päättävät vaihtaa palvelua.

Luku 1. / Kuva 1.4 / s. 28



Merkittävä seuraus MyData-periaatteiden toteuttamisesta on henkilötiedon arvoketjujen pilkkoutuminen ja tiedon hallinnan keskittyminen sen ihmisen ympärille, jonka tiedoista on kysymys. Tämä avaa mahdollisuuksia uusille toimijoille ja rikkoo perinteisiä sektoreiden ja toimialojen rajoja. Avoimissa arvoverkostoissa eri vaiheisiin voi syntyä erikoistuneita toimijoita.

Luku 2. / Kuva 2.1 / s. 35

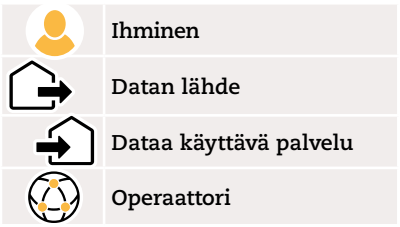
MyDatassa ei ole kyse yksittäisestä teknologiasta vaan kokonaisvaltaisesta viitekehyksestä, joka koostuu toisiaan täydentävistä ja tukevista kerroksista. Eri kerroksilla on kullakin itsenäinen arvo ja niitä kehitetään joka tapauksessa MyData -infrastruktuurista riippumatta.

Luku 2. / Kuva 2.2 / s. 36

Nykykehitys on vienyt niin sanotun API-ekosysteemin suuntaan. Toisaalla taas on syntynyt alustoja, joissa yksittäinen toimija kerää ja harmonisoi dataa useasta lähteestä ja jakelee sitä eteenpäin. MyData-mallissa henkilötiedon hallinnan palveluja tarjoavat toimijat ovat keskenään kilpailevia, mutta muodostavat yhteentoimivan verkoston ja yhdessä tarjoavat infrastruktuurin henkilötiedon välittämiseen.

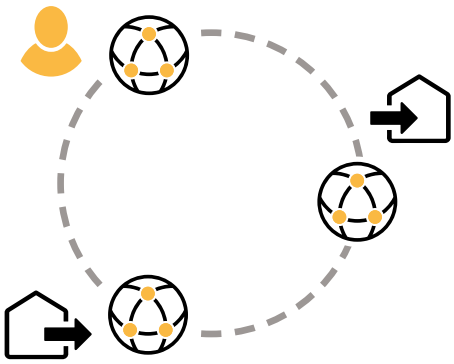
Luku 2. / Kuva 2.3 / s. 40

Roolit MyData-ekosysteemissä



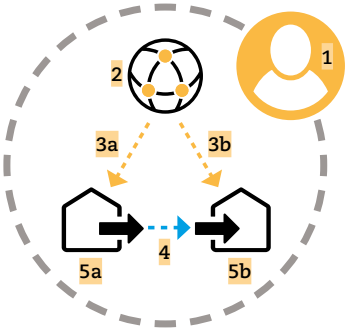
Henkilötiedon jakamisen ekosysteemissä on neljä roolia: ihminen, datan lähde, dataa käyttävä palvelu sekä operaattori. Toimijat voivat samanaikaisesti olla monessa roolissa. Esimerkiksi yritykset ovat tyypillisesti sekä datan lähteitä että dataa hyödyntävien palvelujen tarjoajia. Muissa rooleissa olevat toimijat voivat lisäksi ottaa operaattorin roolin.

Luku 2. / Kuva 2.4 / s. 43



Sekä ihmisillä, datan lähteillä että dataa hyödyntävillä palveluilla tulee olla tiedonvaihdannan verkostoon kytketty digitaalinen identiteetti, jotta tiedon välittäminen eri toimijoiden välillä on mahdollista. Digitaalisia identiteettejä hallinnoidaan MyData-tilien kautta. Tili on metaforana tuttu pankkitileistä, sähköpostitileistä ja asiakastileistä. MyData-tilit tarjoavat keskitetyn näkymän omiin tietoihin sekä siihen, kuka näitä tietoja tällä hetkellä käyttää.

Luku 2. / Kuva 2.5 / s. 45

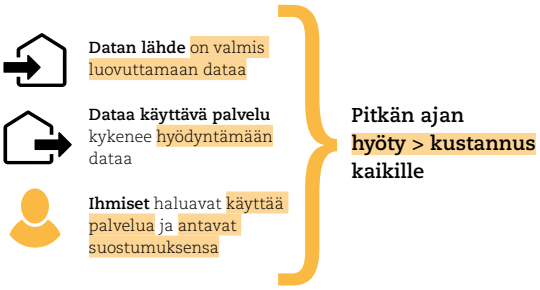


Operaattorimallissa ihmiset [1] voivat hallinnoida yksityisyysasetuksiaan, sopimussuhteitaan ja tiedon käyttölupia etänä MyData-operaattorikäytöölittymän [2] kautta. Tapa, jolla tieto käyttöluvista liikkuu verkostossa, on erillään itse datan siirrosta: kun lupa datan luovuttamiseen [3a] ja hyödyntämiseen [3b] on varmennettu, niin data voi virrata [4] datan lähteiden [5a] ja dataa käyttävien palvelujen [5b] välillä suoraan (ei operaattorin kautta).

Luku 2. / Kuva 2.6 / s. 49

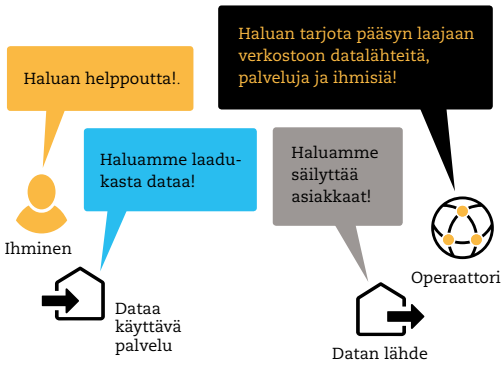
Jotta palvelujen käyttäjien olisi helppo ymmärtää henkilötiedon jakamiseen liittyviä ehtoja, niiden pitäisi olla mahdollisimman selkeät ja rakenteeltaan yhtenäiset eri palveluissa. Jatkossa voisimme kehittää yhtenäisiä standardeja rakenteisessa muodossa julkaistaville käyttöehdoille. Vakiomuotoiset käyttöehdot voitaisiin visualisoida vaihtoehtoja kuvaavilla ikoneilla.

Luku 3. / Kuva 3.1 / s. 53



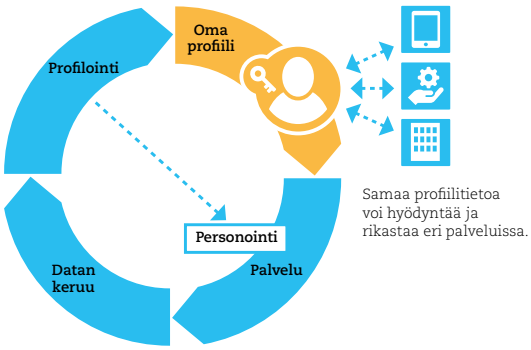
Markkinat toimivat, jos datan lähteillä, dataa hyödyntävillä palveluilla, ihmisillä itsellään ja infrastruktuurin tarjoajilla (operaattorit) on kullakin pitkässä juoksussa omia kustannuksiaan suuremmat hyödyt. Mikäli jokin osapuoli ei ole mukana, ei data liiku eikä kukaan hyödy. Jos kannustimet saadaan kohdalleen ja ekosysteemi syntyy, niin verkostovaikutukset voivat kiihdyttää sen kasvua nopeastikin.

Luku 3. / Kuva 3.2 / s. 54



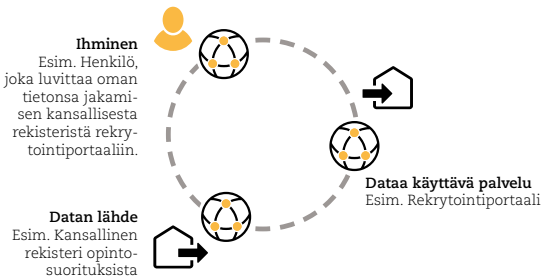
Ihmisille MyData lupaa muun muassa parempaa käyttökokemusta digitaalisissa palveluissa. Samoja tietoja ei tarvitse syöttää ja päivittää moneen paikkaan, palvelut ovat automaattisempia ja yksilöidympiä jne. Tämä riippuu toteutuksien käytettävyydestä. Ei ole vaikea kuvitella päinvastaista skenaariota, missä MyData ei toisi helppoutta, vaan vaatisi ihmisiltä nykyistä enemmän ajankäyttöä ja viitseliäisyyttä oman datansa hallinnoinnissa.

Luku 3. / Kuva 3.3 / s. 55



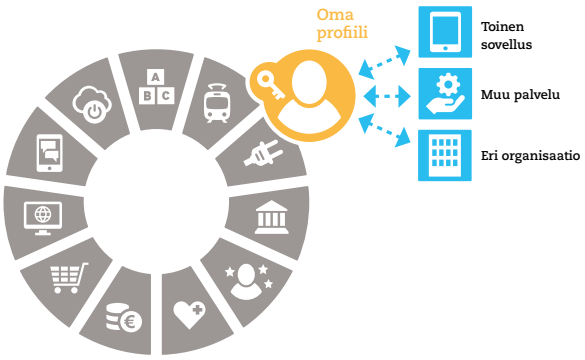
Ihmisen itse hallitsema profiilitieto mahdollistaisi tiedon koostamisen useista lähteistä ja saman profiilin hyödyntämisen eri palveluissa. Esimerkiksi liikkumisprofiili voisi olla jaettu niin sanottujen liikkuminen palveluna (Mobility as a Service, MaaS) tarjoajien kanssa ja terveysprofiili helpottaisi vuorovaikutusta erilaisten terveyden ja hyvinvoinnin palveluntarjoajien kanssa. Muita mahdollisia omia profiileja olisivat esimerkiksi kontaktiprofiili ja yksityisyysasetusten profiili.

Luku 3. / Kuva 3.4 / s. 56



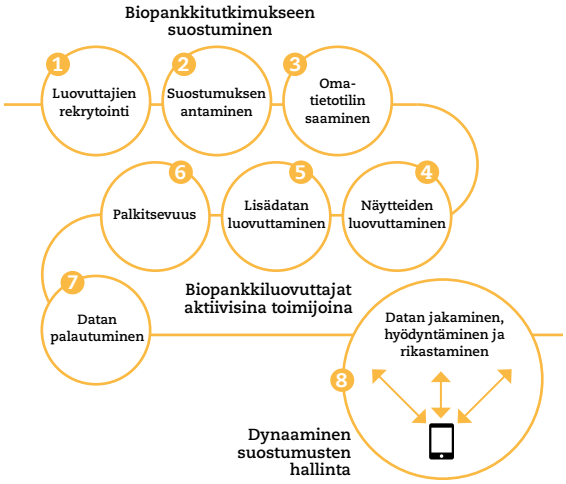
Esimerkiksi tulevaisuuden rekrytointipalvelut ja työnantajien henkilöstöhallinnon palvelut voisivat toimia ihmisten MyDatana välittämien osaamisprofiilien avulla. Osaamisprofiilia on luontevaa ajatella uudenlaisena digitaalisena CV:nä, jossa oma osaaminen on paitsi kuvattu koneluettavassa muodossa niin myös opinto- ja tutkintotiedot sekä muut pätevyydet olisi mahdollista tarvittaessa varmistaa sähköisesti.

Luku 3. / Kuva 3.5 / s. 57



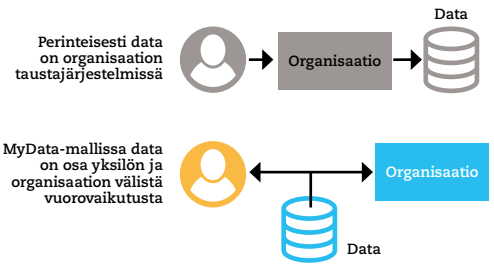
Käyttäjän suostumuksella yritykset voivat saada käyttäjästä rikasta profiilitietoa, jonka pohjalta ja vastineeksi yritys pystyy tuottamaan käyttäjälle parempaa palvelua ja palveluun liittyvää viestintää.

Luku 3. / Kuva 3.6 / s. 59



Yhteiskunnallisesti merkittävä tutkimus edellyttää usein tietojen keräämistä suuresta joukosta ihmisiä ja usein myös monesta tietolähteestä. Suomen lainsäädäntö on verrattain salliva sen suhteen, että julkisia rekistereitä on saatavilla tutkimuskäyttöön. Keinot tiedon hankkimiseen ovat kuitenkin tarkkaan säädeltyjä. Tulevaisuudessa tutkimus ja muu yhteisten ongelmien ratkaiseminen vaatii uudenlaisia keinoja tiedonkeruuseen. Esimerkissä ihmiset ovat aktiivisia biopankkinäytteen luovuttajia ja henkilökohtainen terveystili toimii tiedon hallinnan alustana ja mahdollistaa analysoidun tiedon palauttamisen luovuttajalle.

Luku 3. / Kuva 3.7 / s. 60

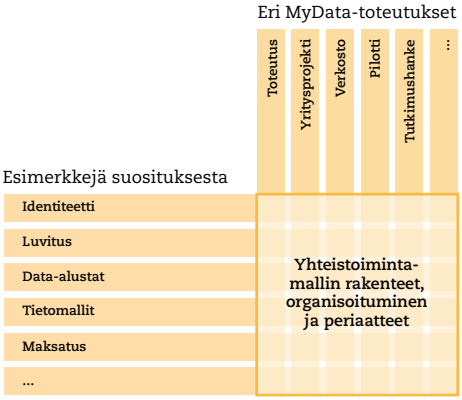


Perinteisesti data on organisaatioiden taustajärjestelmissä, jonka vuoksi asiakkaan ja asiakaspalvelijan näkymät tietoihin poikkeavat toisistaan. Tiedon määrän ja näkyvyyden epäsymmetrisyyden takia asiakkaan voi olla hankala ymmärtää häntä koskevia päätöksiä ja niiden perusteita (esim. pankin lainapäätös). MyData-lähestymisessä data on osa henkilön ja organisaation välistä vuorovaikutusta. Ihmisellä on yhtäläinen pääsy häntä koskeviin tietoihin kuin organisaatiollakin.

Luku 4. / Kuva 4.1 / s. 63

Helsingissä järjestetyn MyData-konferenssin ja sittemmin kansainvälisen MyData-verkoston slogan *"make it happen make it right"* (toteutetaan se ja tehdään se oikein) kuvaa kehityksen kahta puolta. Yhtäältä pitää huolehtia, että kehityssykli kohti todellista ja toimivaa MyDataa pysyy vauhdissa eikä kuihdu kasaan. Toisaalta pitää ymmärtää, että kehitys voi eri toimijoiden ja toiminnan tuloksena muuttaa suuntaa ja pahimmillaan lukittua joltain osin ei toivottuun tilaan.

Luku 5. / Kuva 5.1 / s. 78



Vaikka erilaiset MyData-toteutukset pyrkisivätkin noudattamaan samoja korkean tason periaatteita ihmiskeskeisestä henkilötiedon hallinnasta, niin toteutusten välistä yhteentoimivuutta ei synny ilman erityistä panostusta. Kevyt ja mahdollisimman paljon käytännön toteutuksia tukeva malli yhteentoimivuuden kehittämiseen on eri MyData-toteutusten yhteinen suosituksia antava toimielin. Toimielin antaisi teknisiä suosituksia, joita MyData-toteutuksia tekevät tahot asteittain sitoutuvat noudattamaan, ja suosituksia tarkennettaisiin saatujen käytännön kokemusten myötä.

Luku 5. / Kuva 5.2 / s. 82

Tekesin strateginen avaus Digital Health Revolution (2014–2018) oli edelläkävijä ihmiskeskeisen tiedonhallinnan tutkimuksessa. Hanke edesauttoi MyDatan integroitumista valtakunnantason toimenpiteisiin ja oli osaltaan tukemassa kehitystä, jonka ansiosta Suomi tunnistetaan kansainvälisissä verkostoissa MyDatan ja yksilökeskeisen datan hallinnan edelläkävijänä. Hanke on tukenut myös tämän suomenkielisen MyData-selvityksen päivitystyötä.

Esipuhe

Liikenne- ja viestintäministeriön vuonna 2014 julkaisema MyData-selvitys oli keskustelunavaus, jolla kannustettiin yrityksiä, hallintoa ja kansalaisia pohtimaan uudenlaisen henkilötietomallin mahdollisuuksia ja vaikutuksia. Neljässä vuodessa on tapahtunut paljon ja MyData on kehittynyt eteenpäin. Henkilötiedon hallintamallit ovat murroksessa muun muassa toukokuussa 2018 täysimääräisenä voimaan tulleen EU:n tietosuoja-asetuksen myötä. Suomessa MyData-periaatteisiin on tartuttu yhteistyössä yritysten, tutkijoiden ja julkishallinnon kesken.

Nykyisessä hallitusohjelmassa linjataan, että kansalaisten oikeutta valvoa ja päättää itseään koskevien tietojen käytöstä vahvistetaan. MyData-lähestymistapa on huomioitu hallituksen kärkihankkeissa *"Digitaalisen liiketoiminnan kasvuympäristön rakentaminen"* ja *"Yhteisen tiedon hallinta"*. Väestörekisterikeskus on käynnistänyt MyData-pilotin osana kansallista palveluväylää, jossa Suomi.fi-palvelut muodostavat jatkossa alustan digitaalisen yhteiskunnan palveluille.

Yritysten yhteistyöfoorumina toimii MyData-Allianssi (mydata.fi), jossa on mukana suomalaisia suuryrityksiä, startup-yrityksiä, tutkimuslaitoksia ja julkishallintoa. Kansainvälisesti vertailtuna Allianssi on yhteistyöfoorumina edistyksellinen erityisesti siinä, miten se hakee toimijoiden välistä pilotointia organisaatiorajat ylittäviin MyData-ratkaisuihin. Suomalainen MyData-kehitys on saanut paljon positiivista huomiota kansainvälisesti ja vastaavia vuoropuhelua edistäviä verkostoja perustetaan muuallakin. Myös EU on nostanut MyDatan esille hyvänä esimerkkinä osana datatalous-tiedonannon valmistelutyötä.

Tämän päivän päätöksillä on suuri vaikutus siihen, syntyykö oman datan jakamiseen ja hallintaan yhteisiä standardeja kuten aiemmin matkapuheluihin ja sähköpostiin vai hallitsevatko markkinoita jatkossakin yksittäisten yritysten tarjoamat keskenään kilpailevat alustaratkaisut. Isot kansainväliset data-alustat toteuttanevat tiukentuvan tietosuojasääntelyn vaatimukset, mutta ainakaan vielä ne eivät aktiivisesti pyri alustojen väliseen yhteentoimivuuteen.

Henkilötiedon välittämisen helppous sekä alustojen ihmiskeskeisyys, avoimuus ja yhteentoimivuus ovat Suomelle ja Euroopalle mahdollisuus erottua kilpailussa ja vaikuttaa merkittävästi kansainvälisten toimintamallien muotoutumiseen. Suomen vahvuutena voidaan nähdä myös käyttäjien luottamus palveluntarjoajiin datan käsittelyssä ja valmiudet digitaalisten palvelujen käyttöön, joiden hyvästä tasosta on huolehdittava myös tulevaisuudessa.

Tämä päivitetty versio aiemmasta MyData-selvityksestä vastaa tarpeeseen ajantasaisesta suomenkielisestä johdatuksesta MyData-malliin. Selvitys valottaa, mitä hyötyä MyDatasta on, ketkä sen parissa toimivat ja millainen on näkyvissä oleva polku käytännön toteutuksiin ja kohti yhteentoimivaa ja ihmiskeskeistä henkilötiedon jakamisen ekosysteemiä. Päivitystyö on tehty osana Digital Health Revolution -tutkimushanketta ja selvityksen julkaisijana toimii liikenne- ja viestintäministeriö. Selvityksessä esitetyt näkemykset ovat selvityksen toteuttajien, eivätkä välttämättä heijasta liikenne- ja viestintäministeriön näkemyksiä.

Taru Rastas ja **Maritta Perälä-Heape**
Liikenne- ja viestintäministeriö

Kiitokset

Selvittääksemme henkilötiedon käsittelyn tulevaisuutta ja MyDatan teknisiä, juridisia ja liiketoiminnallisia piirteitä haastattelimme tämän selvityksen ensimmäistä julkaisua varten vuonna 2014 seuraavia asiantuntijoita:

Jari Manninen, **Anssi Mikola**, **Jussi Muurikainen**, **Juha Kenraali**, **Ville Peltola**, **Jouni Sintonen**, **Anu Talus**, **Tuomas Teuri**, **Eero Toivanen** ja **Sakari Vaelma**.

Sen jälkeen ja lisäksi suuri joukko muita aiheesta kiinnostuneita on yhteisönä kasvattanut ymmärrystä henkilötiedon ihmiskeskeisen käsittelyn mahdollisuuksista. Erityisesti haluamme mainita seuraavat henkilöt, jotka ovat eri vaiheissa kommenteillaan auttaneet tämän selvityksen ja sitä edeltäneen vuoden 2014 version syntymistä:

Jouni Alanen, **Emil Asp**, **Reuben Binns**, **Leif Beilinson**, **Myles Byrne**, **Antti Eskola**, **Konsta Hansson**, **Bo Harald**, **William Heath**, **Kari A. Hintikka**, **Emilia Hjelm**, **Mika Honkanen**, **Nina Honkela**, **Markus Kalliola**, **Antti Kettunen**, **Eija Kalliala**, **Matti Kinnunen**, **Otso Kivekäs**, **Miska Knapek**, **Jaakko Korhonen**, **Ismo Kosonen**, **Johanna Kotipelto**, **Krista Lagus**, **Alpo Lahtinen**, **Tuukka Lehtiniemi**, **Risto Linturi**, **Mark Lizar**, **Markus Petteri Laine**, **Aimo Maanavilja**, **Sami Majaniemi**, **Kiti Müller**, **Ville Oksanen** (Ville Oksasen muistoa lämpimästi kunnioittaen), **Mika Pantzar**, **Juuso Parkkinen**, **Maritta Perälä-Heape**, **Olli Pitkänen**, **Olli-Pekka Pohjola**, **Elias Pöyry**, **Taru Rastas**, **Mikael Rinnetmäki,** **Samuel Rinnetmäki**, **Aleksi Rossi**, **Minna Ruckenstein**, **Daniel Schildt**, **Molly Schwartz**, **Jaakko Talvitie**, **Laura Tarhonen**, **Marko Turpeinen** ja **Veera Virta**.

Foorumeina MyData-ajattelun ja toiminnan kehittämisessä Suomessa toimivat kaikille kiinnostuneille avoin Open Knowledge Finlandin MyData-työryhmä sekä yritysten, julkishallinnon ja tutkimuslaitosten edustajille suunnattu MyData-allianssi, jota fasilitoivat liikenne- ja viestintäministeriö ja Aalto-yliopisto. Avoimen työryhmän ja Allianssin tiedot löytyvät osoitteesta **mydata.fi**. Samassa osoitteessa on myös tämän julkaisun verkkoversio.

Sisältö

Infoboksit

Johdanto

Digitaalinen jalanjälkemme kasvaa vauhdilla. Meidän on vaikea hahmottaa, mitä meistä kerättyä tietoa eri organisaatioilla on, emmekä useinkaan ymmärrä tapoja, joilla näitä tietoja hyödynnetään esimerkiksi sosiaalisen median palveluissa tai verkkomainonnassa. Tämä herättää huolestuneisuutta, jota vahvistavat paljastukset valtioiden massiivisista tiedonkeräysjärjestelmistä sekä uutisoinnit yksityisyydensuojaa heikentävistä lainsäädäntöuudistuksista ja tietomurroista. Kyselytutkimuksissa näkyy selvästi suuntaus, että ihmiset luottavat entistä vähemmän siihen, että organisaatiot käyttävät heidän henkilötietojaan asianmukaisesti (Sirkkunen & Haara, 2017). Mitä meidän tiedoillemme ja yksityisyydellemme on tapahtumassa ja miten tämä vaikuttaa elämäämme?

Tallennetun tiedon määrä lisääntyy digitalisaation seurauksena jatkuvasti ja samalla lisääntyy sen liiketaloudellinen ja muu hyödyntäminen. Suuri osa tästä tiedosta on henkilötietoa. World Economic Forum on arvioinut henkilötiedon yhdeksi merkittävimmistä tulevaisuuden liiketoimintakenttää muokkaavista voimista (World Economic Forum, 2013). Henkilötiedon avulla voidaan kehittää muun muassa ennakoivaa terveydenhoitoa sekä sovelluksia oman elämän hallintaan ja itsestä oppimiseen. Henkilötiedon avulla yritykset ja muut organisaatiot voivat räätälöidä palvelujaan vastaamaan paremmin ihmisten tarpeisiin. Yhteiskunnan tasolla henkilötietoa voidaan käyttää päätöksenteon pohjana tai esimerkiksi julkisten palvelujen tarkemmassa kohdentamisessa.

Saumattomat organisaatiorajat ylittävät digitaaliset palvelut tulevat mahdollisiksi, jos henkilötietoa voidaan liikutella sujuvasti ja turvallisesti. Sama datan siirrettävyys tukee myös avointa kilpailua markkinoilla, koska ihmisten on helpompi halutessaan vaihtaa palvelusta toiseen.

Henkilötiedon laajempaan hyödyntämiseen liittyy siis paljon mahdollisuuksia, mutta samalla sitä varjostavat yksityisyyden katoamiseen liittyvät uhkakuvat. MyData-ajattelussa henkilötiedon hyödynnettävyyttä lähestytään asettamalla ihminen itseään koskevan tiedon käytön keskiöön. Näin tietosuoja ja tiedon hyödynnettävyys eivät ole ristiriidassa keskenään, vaan ne päinvastoin tukevat toisiaan. Vahva tietosuoja ja läpinäkyvyys henkilötietojen käytössä lisää ihmisten ja organisaatioiden välistä luottamusta ja avaa sitä kautta mahdollisuuksia innovatiivisten henkilötietoon pohjautuvien palvelujen kehittämiseen. Tavoitteena on, että eettisesti kestävä ihmiskeskeinen tapa hallita henkilötietoa olisi tulevaisuudessa kaikkien kannalta aina käytännöllisin ja myös taloudellisesti kannattavin tapa toimia.

MyDataan liittyvän ajattelun lähtökohta on ihmiskeskeisyys, jossa yhteiskunnan toimintaa rakennetaan ihmisten ympärille. Se on vastapaino suuntaukselle, jossa keskitytään pelkästään organisaatioiden toimintaedellytyksiin. Yhteiskunnan toiminta perustuu kasvavassa määrin tiedon keräämiseen ja hyödyntämiseen. Kansalaiset eivät ole muutoksen kohde vaan muutoksen tekijöitä. Ratkaiseva ero on siinä, suunnitellaanko tiedon keräämisen ja hyödyntämisen mekanismit ensisijaisesti ihmisten vai organisaatioiden näkökulmasta.

Onko tämä MyDataa?

Alun perin Britanniasta lähtenyt MyData ei ole käsitteenä vielä kansainvälisesti täysin vakiintunut. MyData-termin käyttö on kuitenkin yleistynyt huomattavasti tämän selvityksen ensimmäisen version (Poikola, Kuikkaniemi, & Kuittinen, 2014) julkaisemisen jälkeen. Kotimaisten kielten keskus on ehdottanut suomennokseksi termiä omadata. Tässä selvityksessä käytetään englanninkielistä termiä, koska ilmiö on kansainvälinen ja pyrkimyksenä on, että kehitys Suomessa ja maailmalla yhdistyvät toisiinsa.

Termillä MyData viitataan ensinnäkin ilmiöön ja ajattelutavan muutokseen, jossa henkilötiedon hallintaa ja käsittelyä pyritään viemään nykyisestä organisaatiokeskeisestä mallista ihmiskeskeiseksi. Toisaalta MyDatalla viitataan henkilötietoon resurssina, jota ihmiset voivat itse hyödyntää. Mikäli ihmisellä ei ole mahdollisuutta hyödyntää itse jonkun muun hänestä keräämää henkilötietoa, niin sitä ei voida kutsua MyDataksi.

Kuva 0.1: Ihmisen elämän eri alueilla syntyy paljon henkilötietoa. MyData-periaatteet edesauttavat erityisesti toimialarajat ylittävää tiedonsiirtoa. MyDatan kannalta keskeisiä ja paljon henkilötietoa tuottavia aloja ovat muiden muassa liikkuminen, terveys- ja hyvinvointiala sekä pankki- ja vakuutustoiminta.

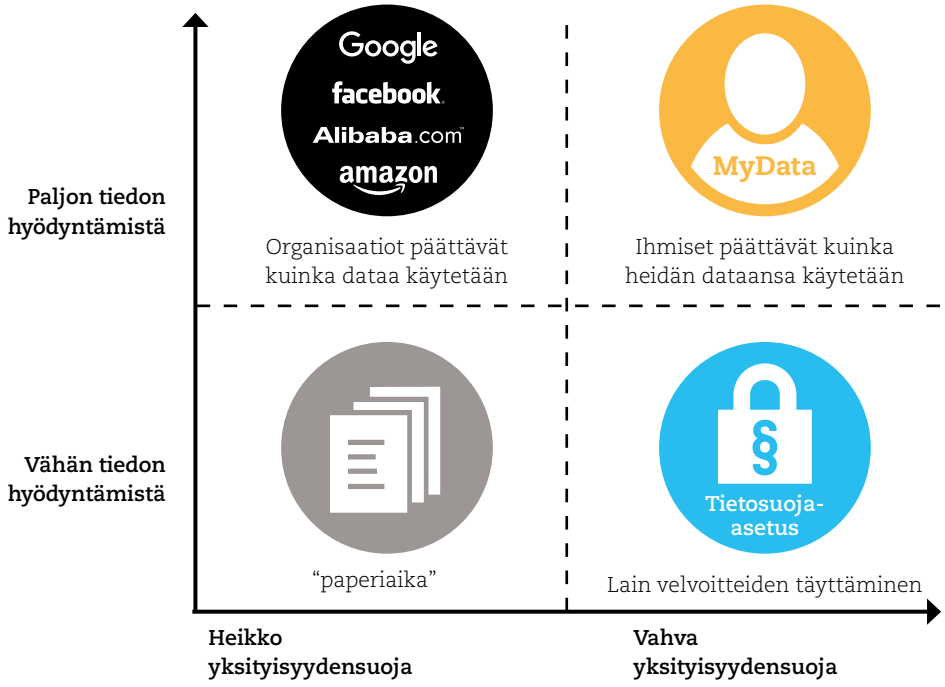
Henkilötieto ei tarkoita vain kaikkein yksilöivimpiä tietoja, kuten nimeä ja osoitetta, vaan laajasti kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja (EU:n tietosuoja-asetus, Artikla 4, 2016). Esimerkiksi kauppaketjuilla on ostostietoa, verkkopalvelut keräävät käyttäjädataa, teleoperaattorille jää tietoa puheluista ja puhelimen liikkeistä. Myös julkishallinnolla on paljon henkilötietoa aina kirjastojen lainaustiedoista ja terveystiedoista rikosrekistereihin. MyData on henkilötiedon osajoukko. Kaikki MyData on henkilötietoa, mutta kaikki henkilötieto ei ole MyDataa.

Tietosuoja ja tiedon hyödyntäminen

Sääntelyn haasteena on tasapainottaa tietosuojaan ja henkilötiedon hyödyntämiseen liittyvät toimet. Kaikki henkilötiedon kerääminen ja käyttö saattaa heikentää yksityisyydensuojaa. Eurooppalaisen vahvan tietosuojalainsäädännön yksi lähtökohta on tietojen keräämisen minimoinnin (data minimization) periaate, jonka mukaan tallennetaan vain sellaisia henkilötietoja, jotka ovat organisaation ennalta määrittämän käyttötarkoituksen mukaan tarpeellisia – *"mitä vähemmän henkilötietoa kerätään ja jaetaan, sen pienempi riski"*. Tämä jättää kuitenkin huomiotta datasta ihmisille itselleen kertyvän arvon ja on vastakkainen henkilötiedon määrän ja käytön lisääntymisen megatrendille.

Yhdysvalloissa vallitseva lainsäädäntö ja käytännöt sallivat organisaatioille varsin vapaan henkilötiedon hyödyntämisen, jos käyttäjä on vain rastittanut lukeneensa ja hyväksyvänsä käyttöehdot. Tämä korostaa henkilötiedon laajaa uudelleenkäyttöä, mutta se tapahtuu yksityisyydensuojan kustannuksella ja yksinomaan yritysten asettamista lähtökohdista. Myös hyödyt tulevat ensisijaisesti yrityksille. Yhdysvaltain kuluttajasuojaviranomaisen mukaan kuluttajatietoa keräävillä ja myyvillä yrityksillä on hallussaan lähes jokaisen yhdysvaltalaisen kattavat tarkat tietovarannot, jotka on kerätty kuluttajien tietämättä (FTC 2014).

MyData-ajattelu tuo datan hyödyntämisnäkökulman tasavertaisena yksityisyydensuojan rinnalle. Tähän pyritään tarjoamalla ihmisille mahdollisuuksia hyödyntää itse omaa dataansa sekä keinoja hallita, kuinka dataa kerätään, jalostetaan, hyödynnetään ja jaetaan edelleen. Olisi toivottavaa, että yrityksiä ja organisaatioita kannustetaan ja ohjataan avaamaan henkilötietorajapintoja.



Kuva 0.2: MyData mahdollistaisi henkilötiedon jouhevan käytön niin, että hyödyt maksimoidaan ja yksityisyydensuojan heikkeneminen minimoidaan.

Voiko dataa omistaa?

MyDataan liitetään usein mielikuva tiedon omistajuudesta. Arkikielisesti on luontevaa sanoa, että *"ihmisillä pitäisi olla oikeus omistaa omat tietonsa"*. Datan omistajuuden käsite on kuitenkin hankala ja sen sijaan puhumme oikeuksista henkilötietoon. MyDatalla tavoitellaan sitä, että ihmisillä on oikeus ja käytännöllinen mahdollisuus hyödyntää omia tietojaan ja hallita sitä, kuka niitä käyttää. Tämä ei kuitenkaan tarkoita, etteikö myös tietoa tuottavilla organisaatioilla voisi olla oikeuksia samaan tietoon.

Omistaminen on helppo ymmärtää irtaimiston tai kiinteän omaisuuden kohdalla. Omistaja voi määrätä omistuksesta muut poissulkevasti. Tuolin omistaja voi yleensä päättää, kuka tuolilla saa istua tai minkä väriseksi tuoli maalataan. Toisen maalle ei saa rakentaa eikä toisen metsästä kaataa puita ilman lupaa.

Tiedon omistaminen ei ole näin suoraviivaista. Monet ihmiset voivat tietää samoja asioita. Taloustieteellisin termein: tieto on kilpailematon hyödyke. Se, että yksi ihminen tietää jotain ja käyttää sitä hyödykseen, ei sinällään estä muita samanaikaisesti tietämästä ja hyödyntämästä samaa tietoa. Vastaavasti, kun dataa kopioidaan, ei yhden kopion käyttö estä muiden kopioiden käyttöä. Datan saatavuutta ja hallintaa voidaan toki rajoittaa niin, että käytännöllisesti vain harvoilla on mahdollisuus sitä hyödyntää.

Pääsääntöisesti tietoon tai dataan ei kohdistu yksinoikeuksia, kukaan ei omista tietoa. Sen sijaan joihinkin tietoihin voi kohdistua esimerkiksi tekijänoikeuksien, liikesalaisuuden tai yksityisyydensuojan takia rajoitetumpia oikeuksia. Tietoon kohdistuvat oikeudet ovat yleensä kielto-oikeuksia: ne antavat oikeudenhaltijalle mahdollisuuden kieltää muita hyödyntämästä tietoa.

Moniin tietoihin voi useilla osapuolilla olla perusteltu intressi. Esimerkiksi kaupalla on asiakassuhteessa hyvä syy saada käyttää keräämiään asiakastietoja, vaikka asiakkailla olisikin samoihin tietoihin oikeuksia, kuten mahdollisuus saada data itselleen tai poistaa data asiakassuhteen päättyessä. (Pitkänen 2014)

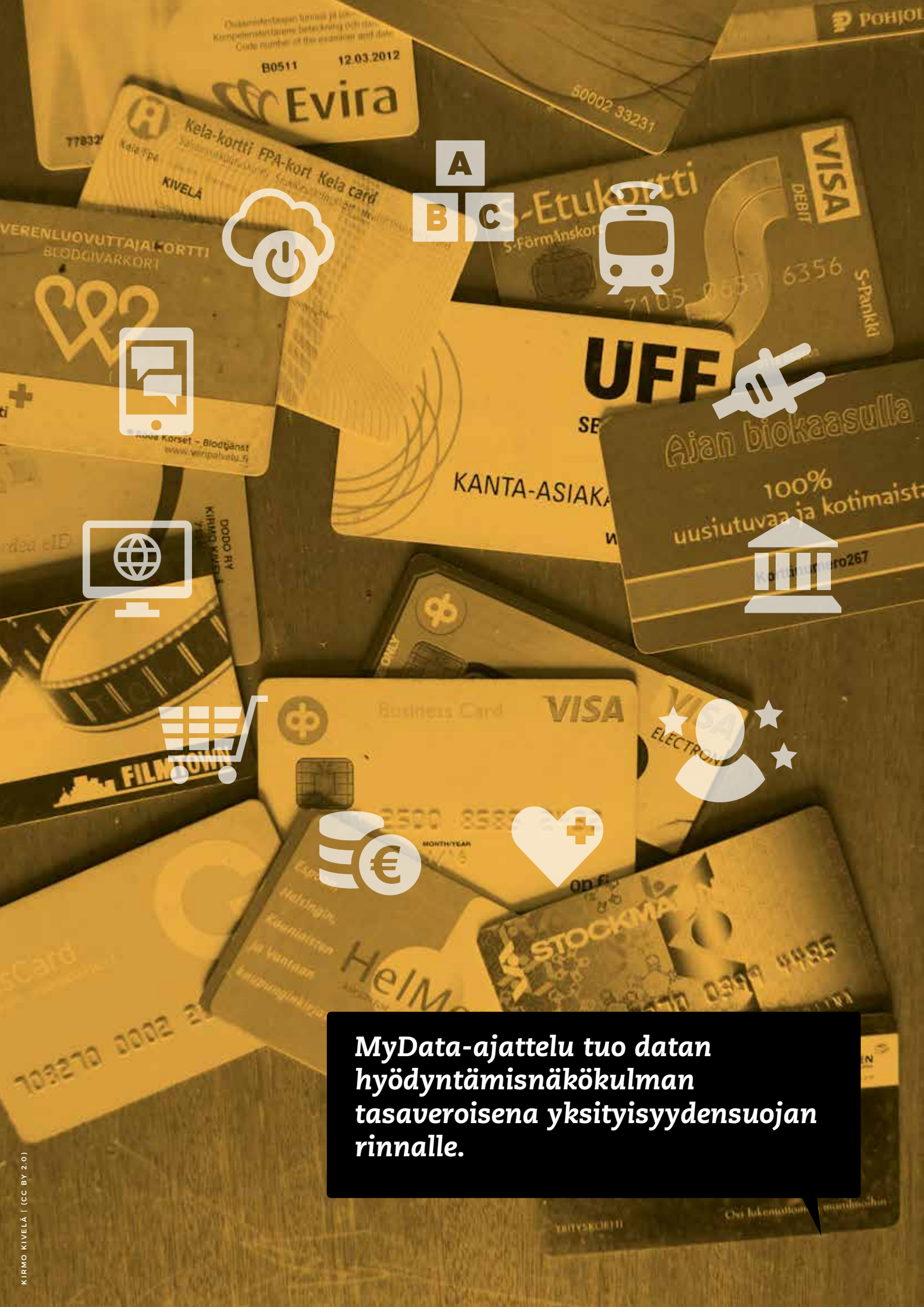
Julkishallinto ja MyData

Julkisella sektorilla on runsaasti lakisääteistä henkilötiedon käsittelyä, joka ei pohjaudu ihmisten itsensä antamaan suostumukseen. Lakisääteinen käsittelyperuste ei kuitenkaan estä MyData-periaatteiden vähimmäisvaatimusten toteuttamista.

Oikeudet ja hallinnan mahdollisuudet omaan dataan vaihtelevat eri tapauksissa. Minimivaatimus MyData-periaatteiden toteuttamiselle on, että ihmiset saavat pääsyn omaan dataansa ja voivat käyttää sitä myös muualla ja muihin tarkoituksiin. Täysi kontrolli, joka mahdollistaisi mm. oman datan muuttamisen tai poistamisen alkuperäislähteestä ei ole edellytys MyDatalle. Keskeistä on, että henkilötieto on teknisesti helposti käytettävissä ihmisille ja niille palveluille ja toimijoille, joille ihminen haluaa sallia oman datansa käytön.

Henkilötietojen käsittely on välttämätöntä viranomaistehtävissä, esim. verottaja tarvitsee henkilötietoja verotusta varten, eivätkä ihmiset voi poistaa itseään verottajan rekistereistä. Julkishallinnon toimijat voivat noudattaa MyData-periaatteita tekemällä henkilötiedon käsittelystä läpinäkyvää ja tarjoamalla ihmisille koneluettavassa ja uudelleenkäytön mahdollistavassa muodossa pääsyn tasapuolisesti kaikkiin tietoihin, joihin heillä on pääsy perinteisessä verkkopalvelussa.

Henkilötietorajapintojen kehittämisessä julkisen sektorin toimijat voivat jopa näyttää esimerkkiä. MyData-periaatteiden mukainen henkilötiedon hallinta voisi helpottaa julkisten ja yksityisten palvelujen yhteentoimivuutta, kun ihminen saisi itse siirtää datan palvelusta toiseen. Julkisella sektorilla on useita ainutlaatuisia tietovarantoja, joita ei ole saatavilla muualla. Esimerkiksi perusrekisterien sisältämä tieto on keskeistä perustietoa, luonteeltaan virallista ja luotettavaa ja siksi erityisen arvokasta.



1. Mitä MyData muuttaisi?

MyData pyrkii tarjoamaan ihmisille mahdollisuuden käyttää henkilötietojaan omiin tarkoituksiinsa ja jakaa niitä turvallisesti omilla ehdoillaan. Uudistuva eurooppalainen lainsäädäntö antaa tähän periaatteessa hyvän pohjan, mutta toisaalta aiempikin tietosuojalainsäädäntö on tarjonnut ihmisille oikeuksia, jotka ovat usein jääneet lähinnä nimellisiksi, koska niitä ei tunneta ja niitä on vaikea valvoa. Kansainvälisessä MyData-periaatteiden julistuksessa (**mydata.org/declaration**) tavoitteeksi on kirjattu: *"pääsy omiin tietoihin, tietojen oikaiseminen ja siirrettävyys, sekä oikeus tulla unohdetuksi kehittyvät yhden klikkauksen oikeuksiksi, jotka ovat yhtä yksinkertaisia ja tehokkaita käyttää kuin tämän päivän ja huomisen parhaat verkkopalvelut"*.

Datatalouden nopea kasvu perustuu verkostovaikutuksiin. Niiden tehokkaimpia hyödyntäjiä ovat alustatoimijat, joilla on mahdollisuus kerätä ja käsitellä suurimmat määrät henkilötietoja. Nämä alustat sulkevat markkinoita paitsi kilpailijoiltaan myös monilta muilta yrityksiltä, jotka ovat nyt vaarassa menettää suoran yhteyden omiin asiakkaisiinsa. Yksilön oikeuksien vahvistaminen ja käytännöllistäminen nähdään merkittävänä yritysten kilpailua edistävänä muutosvoimana.

1.1 Käytännölliset oikeudet ja käytettävä data

Oikeus omaan dataan ja sen hallintaan nähdään digitaalisen ajan ihmisoikeutena. MyData-periaatteiden mukaan ihmisillä on paitsi oikeuksia myös käytännön työkaluja, joiden avulla he hallitsevat omia tietojaan, yksityisyyttään ja omaa elämäänsä verkossa. Lähtökohtana on, että ihminen saa tietää, mitä tietoja hänestä on kerätty ja millä tavalla niitä hyödynnetään. Lisäksi omat tiedot voi helposti siirtää itselleen uudelleenkäytettävässä muodossa ja niitä voi jakaa edelleen muiden käyttöön, ja tiedon jakamisen voi myös lopettaa yhtä helposti.

Ihmisellä on oikeus:

- **tietää** tietää, mitä henkilötietoa hänestä on olemassa
- **nähdä** itseään koskeva henkilötietosisältö
- **oikaista** väärät henkilötiedot
- **valvoa** ja tarkistaa, kuka hänen henkilötietoaan käsittelee ja miksi
- **saada omat tietonsa** ja käyttää niitä vapaasti
- **siirtää omat tietonsa** eri toimijoille ja antaa lupa niiden käyttämiseen
- **poistaa** omat tiedot ja tulla unohdetuksi

Kuva 1.1: Oikeudet ja hallinnan taso, jotka ihmisillä on omiin tietoihinsa, voivat vaihdella eri tilanteissa. MyDatasta voidaan puhua silloin, kun ihmisillä on oikeus ja käytännön mahdollisuus saada omat tietonsa itselleen, käyttää niitä vapaasti ja siirtää halutessaan kolmansille osapuolille.

Laista tulevat oikeudet tukevat MyDatan periaatteiden toteutumista. Silti pelkkä lain vaatimusten seuraaminen ei yksin riittää ihmiskeskeisen henkilötiedon ekosysteemin synnyttämiseksi. Esimerkiksi henkilörekistereihin liitetyn tarkastusoikeuden nojalla ihmisillä on nykyisinkin muodollinen mahdollisuus saada itseään koskevat tiedot. Nykyisin yritykset toteuttavat tarkastusoikeuden velvoitteen usein niin, että tarkastusoikeuden nojalla pyydetty tieto lähetetään sitä pyytävälle henkilölle postitse. Esimerkiksi teleoperaattorilta saa oman puhelinliittymän puhelu- ja paikkatiedot paperitulosteena maksamalla noin 10 euron toimitusmaksun. Tietojen joustavan jatkohyödyntämisen kannalta tällainen paperinen ja kallis datatuloste on hyödytön.

MyData pyrkii antamaan ihmisille lainsäädännön minimivaatimuksia laajemmat mahdollisuudet hallita omia tietojaan ja sen myötä tekemään henkilötiedosta uudelleenkäytettävän resurssin niin, että yksityisyydensuoja otetaan huomioon. Lain mukaisesti rekisterinpitäjät saavat kerätä, tallentaa, käsitellä ja hyödyntää henkilötietoja vain ennalta määriteltyihin käyttötarkoituksiin. Henkilöitä, joiden datasta on kyse, nämä rajoitukset eivät koske. Ihminen itse voi hyötyä datastaan käyttämällä sitä joustavasti itse määrittämiinsä tarkoituksiin. Käytännössä tämä tarkoittaisi myös, että yksilöt voivat antaa suostumuksen oman tietonsa uudelleenkäyttöön ja jakaa dataansa palveluiden välillä omien tarpeidensa mukaan.

MyDatan minimitoteutus on, että ihmiset voivat ladata omat tiedot koneluettavassa muodossa itselleen. Innovatiivisten sovellusten kannalta olisi kuitenkin parempi, että ajantasaiseen dataan olisi jatkuva pääsy standaroitujen ohjelmointirajapintojen (API) kautta. Näin tiedon päivittäminen ei vaatisi vierailuja tiedon tarjoajan sivustolla, vaan palveluja voitaisiin automatisoida. Esimerkiksi ostosdata on hyödyllisintä, jos sähköisen eKuitin saa automaattisesti heti ostoksen maksettuaan kuten paperikuitin nykyään.

eKuitti yrityksille ja kuluttaja-asiakkaille

Monille niin sanottu “kuittirumba” on tuttua. Paperikuitteja pyörii taskuissa ja lompakossa, osa on henkilökohtaisista pikkuostoksista, mutta joukossa on myös tärkeitä tositteita, jotka tulisi säilyttää takuuta varten tai liittää esimerkiksi työnantajalle tehtävään kululaskuun.

Suomessa tehdään vuosittain 1,3 miljardia korttimaksua, joista kymmenen prosenttia yrityskorteilla. Kuluttajien korttimaksujen osalta jotkut pankit lähettävät jo lähes reaaliaikaisesti sähköisen kuitin pankin tarjoamaan mobiilisovellukseen. Laajemmin ajatus digitaalisista niin sanotuista eKuiteista tarkoittaisi, että ostaja saisi maksutavasta riippumatta kattavan myös ostosten rivitiedot sisältävän datakuitin haluamaansa paikkaan ilman, että ostotilanteessa tarvitsisi sitä erikseen ilmoittaa. Yritykset tarvitsevat kuittitietoa kirjanpitojärjestelmissä ja kuluttaja-asiakkailla voisi olla oma datalompakko, mihin eKuitit tallentuvat automaattisesti.

Ero paperikuitteja pursuavan nahkalompakon ja datalompakon välillä on se, että jälkimmäiseen voidaan asentaa hyödyllisiä ohjelmia, jotka käsittelevät ja havainnollistavat tietoa. Datalompakossa voi toimia vaikkapa reaaliaikainen talousseuranta-ohjelma, takuukuittiarkisto ja muita ostokäyttäytymiseen liittyviä henkilökohtaisia palveluja. Käyttäjä voi itse valita, mitä ohjelmia datalompakkoonsa asentaa, mutta kauppias voi myös suositella ohjelmia, jotka erityisesti ottavat huomioon heidän lähettämänsä kuittidatan.

Taloushallinnon automatisointi on yritysten tuottavuuskehityksen kannalta keskeisimpiä alueita. Sen onnistuminen vaatii sekä standardoitua rakenteista dataa että avoimia rajapintoja. Sähköisenä saatavan kirjanpitokelpoisen eKuitin säästöpotentiaalin on arvioitu olevan lähes 800 miljoonaa euroa vuodessa. Suomalaisessa Taltio-hankkeessa[2] on määritelty verkkolaskustandardia käyttävä ekosysteemi eKuittien välitykseen. Jatkohankkeissa pyritään käynnistämään kuitinvälitys laajasti ja yhteistyössä mm. Viron kanssa sekä lisäämään yritysten verkkolaskuihin koneluettavaa tietoa, jolla voidaan mm. syventää tilitoimistojen analyysipalveluita.

Vaikka yritysten taloushallinnon automatisointi on nyt veturina eKuittien kehityksessä, niin samoja mekanismeja kannattaa hyödyntää myös kuluttajapuolella, jolloin ei tarvitse rakentaa erillistä toimintatapaa kuluttajien kuitinvälitykseen myöhemmin. Kuluttajille eKuitti toimisi rivikohtaisena takuutodistuksena sekä takaisinkutsu-, huoltomuistutus- jne. välineenä.

2 Taltio ja RTECO hankkeet https://www.lvm.fi/-/talousdatasta-yhteen-toimivia-ja-parempia-digitaalisia-palveluja-956152

1.2 MyData ja lainsäädäntö

Lainsäädäntö, säätely sekä teknologiset muutokset voivat osaltaan tukea MyDatan toteutumista. Sääntelyllä voi olla kiihdyttävä tai hidastava vaikutus, mutta lainsäädäntö yksin ei saa aikaan muutosta. Haasteena on datatalouden kansainvälistyminen ja sääntelyn soveltaminen maailmanlaajuisesti toimiviin palveluihin.

Eurooppalaisen tietosuojalainsäädännön lähtökohtana on yksityisyyden suojaaminen ja henkilörekisterin tietosisällön oikeellisuus, ei niinkään henkilötiedon mahdollisten hyötyjen toteutuminen. Laki antaa muun muassa ihmisille oikeuden tarkistaa omat tietonsa henkilörekisterin pitäjältä ja pyytää korjaamaan tai tietyissä tilanteissa myös poistamaan tiedot. EU:n perusoikeuskirjaan on kirjattu, että *"jokaisella on oikeus tutustua niihin tietoihin, joita hänestä on kerätty, ja saada ne oikaistuksi"*.

Henkilötietoa saa lain mukaan käyttää lähtökohtaisesti vain siihen tarkoitukseen, mihin se on alun perin kerätty. Esimerkkejä laissa erikseen määritellyistä sallituista jatkokäyttötarkoituksista ovat tieteellinen tutkimus ja tilastointi. Yksityisyyden suojan kannalta on perusteltua, etteivät organisaatiot voi noin vain, varsinkaan ihmisten tietämättä, käyttää henkilötietoa uusiin tarkoituksiin. Toisaalta taas datan järkevät käyttötarkoitukset saattavat nousta esiin vasta jälkikäteen. Suostumuksen pyytäminen jälkikäteen on usein käytännössä vaikeaa, vaikka uusi käyttötarkoitus olisikin rekisteröityjen mielestä hyväksyttävä. Lain hengen ja tarkoituksen mukaisesti henkilötietojen käyttötarkoituksen tulisi aina olla mahdollisimman tarkasti määritelty.

MyData-lähestymistavassa tasapainoa haetaan sitä kautta, että ihminen toimii kontrollipisteenä oman datansa käytön suhteen. Silloin kaikkia tulevaisuuden hyödyntämismahdollisuuksia ei tarvitse etukäteen luetella, sillä ihminen itse saa käsitellä omaa dataansa vapaasti. Ihminen saa oman datansa itselleen, jolloin hän voi antaa sen eteenpäin niihin tarkoituksiin, joihin itse haluaa. On kuitenkin huomioitava, että suostumus ei syrjäytä tarpeellisuutta, eli vaikka ihminen antaisi oman suostumuksensa datan keräämiseen ja käyttöön, niin sen lisäksi rekisterinpitäjän on pystyttävä osoittamaan, että kyseinen henkilötiedon käsittely todella on perusteltua.

Euroopan unionin uusi tietosuoja-asetus (EU 2016) tuli täysimääräisenä voimaan siirtymäajan päätyttyä toukokuussa 2018. Asetus on kaikissa jäsenvaltioissa suoraan sovellettavaa lainsäädäntöä. Tietosuojaan liittyvien sääntöjen muutoksesta johtuen miltei kaikkien henkilötietoa käsittelevien toimijoiden on täytynyt suunnitella uudelleen omien järjestelmiensä toimintaa. Tämä on samalla myös merkittävä mahdollisuus muuttaa tietojärjestelmiä kohti MyDatan kaltaisia avoimempia käytäntöjä. Asetus vahvistaa jo pitkään voimassa olleita tietosuojaperiaatteita muun muassa taloudellisesti merkittävien sanktioiden myötä. Samalla ihmisten oikeudet heitä itseään koskevaan tietoon lisääntyvät ja esimerkiksi kriteerit sille, mikä on hyväksyttävä suostumus tiukentuvat aikaisempaan verrattuna.

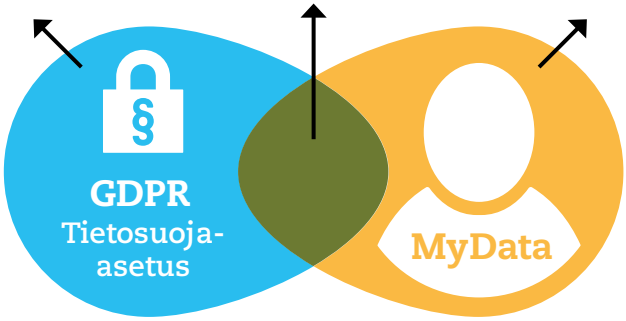
Henkilötiedon hyödynnettävyyden kannalta merkittävä muutos on, että uuden lainsäädännön myötä rekisteröidyllä on mahdollisuus tarkastusoikeuden nojalla pyytää rekisterinpitäjältä kopioita omista tiedoistaan ja saada ne yleisesti käytetyssä sähköisessä muodossa (Tietosuoja-asetus, Artikla 15). Aiemmin käytäntönä on usein ollut, että rekisterinpitäjä pyydettäessä lähettää paperitulosteena tai PDF-tiedostona otteen, josta tiedot käyvät ilmi. Tällainen toimintatapa ei edesauta henkilötiedon hyödyntämistä.

Tarkastusoikeuden lisäksi asetuksessa määritellään uusi oikeus, nimittäin oikeus siirtää tiedot järjestelmästä toiseen (Tietosuoja-asetus, Artikla 20). Tällä oikeudella pyritään varmistamaan, ettei datan keruusta tule palvelujen välistä kilpailua rajoittava tekijä, vaan että ihmisillä on mahdollisuus vapaasti valita kilpailevien palveluntarjoajien välillä ja siirtää myös tietonsa mukanaan, mikäli päättävät vaihtaa palvelua. Artiklan mukaan ihmisillä on oikeus saada tiedot jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa.

Yhdenmukaistaa lainsäädäntöä

Vahvistaa yksilön oikeuksia ja luottamusta dataa käsitteleviin organisaatioihin

Mahdollistaa uusia henkilödataan pohjautuvia palveluja



Kuva 1.2: EU:n tietosuoja-asetuksen (EU General Data Protection Regulation, GDPR) ja MyDatan tavoitteet ovat osin yhteneviä.

Tietosuoja-asetuksen lisäksi muita Euroopan tason digitaaliseen identiteettiin ja henkilötiedon liikkuvuuteen liittyviä keskeisiä lainsäädäntöuudistuksia ovat Sähköisen viestinnän tietosuoja-asetus (ePrivacy), Sähköisen tunnistamisen eIDAS-asetus sekä Maksupalveludirektiivi (PSD2). Osaltaan nämä kaikki pyrkivät luomaan Eurooppaan yhtenäistä digitaalista markkina-aluetta avaamalla pääsyä tietoon ja helpottamalla tiedon siirtymistä organisaatioiden ja maiden rajojen yli. MyData-käytännöillä pyritään siihen, että ihmisten oikeuksista tulee käytännössä helppoja ja hyödyllisiä ja että määräysten toteuttaminen on joustavaa ja helppoa organisaatioille.

Sähköisen viestinnän tietosuoja-asetus (ePrivacy): Euroopan komissio antoi tammikuussa 2017 ehdotuksensa asetukseksi yksityiselämän ja henkilötietojen suojaamisesta sähköisessä viestinnässä. Asetus koskee erilaisia sähköisten viestintäpalvelujen tarjoajia kuten teleoperaattoreita ja esimerkiksi WhatsAppin kaltaisia palveluja. Kyse on yleisen tietosuoja-asetuksen tavoin asetuksesta, joka voimaan tullessaan on suoraan sovellettavaa sääntelyä eikä edellytä jäsenvaltioilta erillistä voimaansaattamista direktiivien tavoin.

Sähköisen tunnistamisen eIDAS-asetus: Vuonna 2016 voimaan tulleen eIDAS-asetuksen (Electronic identification and trust services for electronic transactions in the internal market) tavoitteena on tarjota sähköisiä tunnistusvälineitä, joilla on mahdollista tunnistautua julkishallinnon palveluissa koko EU:ssa viimeistään 2018 syksyllä. Asetus määrää, että jäsenvaltioiden viranomaisten on tunnustettava toisen jäsenvaltion komissiolle ilmoittamat sähköisen tunnistamisen menetelmät. Esimerkiksi ruotsalaiset vahvat sähköiset tunnisteet kelpaavat suomalaisiin julkishallinnon palveluihin ja toisin päin.

Maksupalveludirektiivi (PSD2): Euroopan unioni pyrkii myös muuttamaan pankkialan kilpailuympäristöä helpottamalla uusien toimijoiden pääsyä markkinoille. Keinona tähän on tiedon liikkumisen helpottaminen. Tällä hetkellä keskeisenä rajoitteena uusien maksupalvelujen syntymiselle on se, että henkilöasiakkaiden tilejä ja maksuja koskevat tiedot pysyvät visusti heitä palvelevien pankkien hallussa. Uusi maksupalveludirektiivin (Payment Service Directive, PSD2) velvoittaa pankit avaamaan maksupalveluihin liittyviä rajapintojaan, jolloin ihmiset voivat ottaa uusia palveluja käyttöön riippumatta siitä, minkä pankin asiakkaina he ovat. Jäsenvaltioiden oli pantava toimeen direktiivi tammikuussa 2018.

Datan siirrettävyys käytännössä

Tietosuoja-asetuksen 20. artikla tuo uuden oikeuden ihmisille ladata omia tietojaan joko itselleen tai siirtää suoraan palvelujen välillä. Tämä on yksi asetuksen kohdista, mihin yritykset ovat kaikkein heikoimmin valmistautuneita. Jotkut yritykset tarjoavat jo asiakkailleen mahdollisuutta ladata omat tietonsa verkkosivuilta, mutta suurimmalle osalle tämä on kokonaan uutta ja etenkin mahdollisuus välittää tietoja suoraan kahden organisaation välillä asiakkaan pyynnöstä vaatii kehitystoimia.

20 artikla

Oikeus siirtää tiedot järjestelmästä toiseen

1. Rekisteröidyllä on oikeus saada häntä koskevat henkilötiedot, jotka hän on toimittanut rekisterinpitäjälle, jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa, ja oikeus siirtää kyseiset tiedot toiselle rekisterinpitäjälle sen rekisterinpitäjän estämättä, jolle henkilötiedot on toimitettu, jos
   a) käsittely perustuu suostumukseen artikla 6 1 kohdan a alakohdan tai artikla 9 2 kohdan a alakohdan nojalla tai sopimukseen artikla 6 1 kohdan b alakohdan nojalla; ja
   b) käsittely suoritetaan automaattisesti.
2. Kun rekisteröity käyttää 1 kohdan mukaista oikeuttaan siirtää tiedot järjestelmästä toiseen, hänellä on oikeus saada henkilötiedot siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on teknisesti mahdollista.

Kuva 1.3: Tietosuoja-asetuksen tietojen siirrettävyyttä koskeva artikla.

Tietojen siirto-oikeus (data portability) kattaa kaikki tiedot, jotka syntyvät asiakkaan toiminnan seurauksena. Tietojen pitää olla tarjolla käyttökelpoisessa koneluettavassa muodossa ja lähtökohtaisesti maksutta. Tämä oikeus ei liity oikeuteen tulla unohdetuksi, eikä datan siirtäminen automaattisesti käynnistä datan poistamista alkuperäislähteestä. Euroopan tietosuojaviranomaisten työryhmä on antanut selkeät ohjeistukset tietojen siirto-oikeuden tulkinnasta (European Commission 2017), mutta tästä on kuitenkin vielä matkaa käytännön toteutuksiin organisaatioissa.

Ranskalaisessan Dataccess[3] -projektissa teleoperaattori on koonnut avoimen työryhmän kehittämään määrittelyjä, ohjeistuksia, avoimesti lisensoituja designelementtejä ja avoimen lähdekoodin toteutuksia, joilla pyritään tarjoamaan yhteinen helposti käytettävä malli henkilötiedon siirrettävyyden käytännön toteutukseen organisaatioissa. Työryhmässä on mukana Ranskan tietosuojavaltuutettu (CNIL) sekä energiayhtiöitä, pankki- ja vakuutusalan toimijoita ja kaupunkeja.

Dataccess on ottanut mallia Yhdysvaltalaisista Green- ja Blue Button[4] -käytännöistä, jotka edistävät kuluttajien mahdollisuutta saada energiankulutus- (green button) ja terveysdataansa (blue button) itselleen. Toimialakohtaisten ratkaisujen sijaan Dataccess pyrkii vähentämään datan siirrettävyyteen liittyviä haasteita kaikissa organisaatioissa ja sen myötä mahdollistamaan käyttäjille eri palveluissa yhteneväisen ja helpon käyttökokemuksen omien tietojen siirtämiseen. Tavoitteena on, että käytännöllisen toteutusmallin myötä lain vaatimus muuttuu pakollisesta pahasta mahdollisuudeksi kehittää luottamukseen perustuvia asiakassuhteita ja edistää innovaatioita.

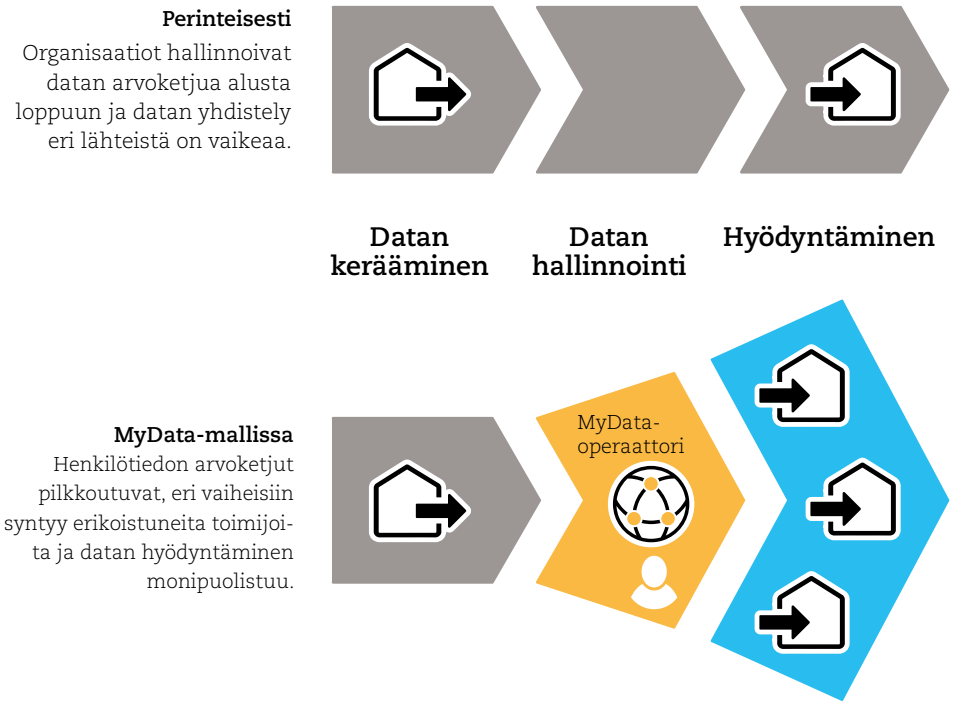
Ensimmäisessä vaiheessa Dataccess on julkaissut määrittelyjä kolmesta toisiaan täydentävästä käyttötapauksesta: 1) tietojen lataaminen omalle koneelle 2) tietojen siirtäminen sovellusten välillä ja 3) tietojen siirtäminen omaan datalompakkoon (personal cloud). Lisäksi Dataccess-julkaisussa on hahmoteltu tyypillinen tiedon siirrettävyyden toteutusprojekti ja jaettu se helposti hallittaviin osiin.

3 http://mesinfos.fing.org/wp-content/uploads/2018/03/PrezDataccess_EN_V1.21.pdf
4 http://energy.gov/data/green-button ja http://www.healthit.gov/bluebutton

1.3 Avoin liiketoimintaympäristö

Merkittävä seuraus MyData-periaatteiden toteuttamisesta on henkilötiedon arvoketjujen pilkkoutuminen ja tiedon hallinnan keskittyminen sen ihmisen ympärille, jonka tiedoista on kysymys. Tämä avaa mahdollisuuksia uusille toimijoille ja rikkoo perinteisiä sektoreiden ja toimialojen rajoja.

Yhtenä MyData-ajatteluun sisältyvänä tavoitteena on henkilötietoon liittyvän liiketoiminnan avautuminen kehitykselle, kilpailulle ja yhteistoiminnalle niin, etteivät monopolistiset skenaariot (Newman 2013) tietoyhteiskunnan tulevaisuudesta toteutuisi. Toimivassa palvelujen kokonaisuudessa halutaan välttää sitä, että mikään yksittäinen organisaatio olisi infrastruktuurin tarjoajana monopoliasemassa, että kaikki henkilötieto sijaitsisi yhdessä palvelussa tai että palveluja voisi toteuttaa vain yhdellä teknologialla.



Kuva 1.4: MyData-mallissa henkilötiedon arvoketjut pilkkoutuvat ja muodostavat arvoverkostoja. Avoimissa arvoverkostoissa eri vaiheisiin voi syntyä erikoistuneita toimijoita. MyData-operaattorit olisivat hallinnointiin erikoistuneita toimijoita, jotka tarjoavat tietosuoja-asetuksen mukaista henkilötiedon hallinnointia ja luvittamiseen liittyviä toimintoja palveluna.

Henkilötiedon jalostuksen arvoketju koostuu henkilötiedon lähteistä (luominen, kerääminen), välittämisestä (hallinta) ja hyödyntämisestä. Perinteisesti koko arvoketju on yhden organisaation sisällä. Esimerkiksi kun pankin järjestelmiin syntyy tieto henkilön kaikista tilitapahtumista, pankki jalostaa ja välittää tietoa ja tuottaa tiliotteet ja verkkopankkinäkymät asiakkailleen. MyDatan myötä siirrytään yksittäisten organisaatioiden toteuttamista arvoketjusta kohti avointa ja hajautettua arvoverkostoa, jossa syntyy eri vaiheisiin erikoistuneita toimijoita. Esimerkiksi yhdysvaltalainen mint.com-palvelu hyödyntää pankkisektorilla henkilötietoa arvoketjun loppupäässä ja tarjoaa käyttäjille tavallista verkkopankkia kattavamman oman talouden näkymän.

Perinteisessä datan jalostusketjussa yritys tai palvelu, jossa data syntyy, on portinvartija. Esimerkiksi kauppaketjun kanta-asiakaskortilla tehdyistä ostoksista syntyy dataa, jonka käytöstä päättää kanta-asiakasjärjestelmän ylläpitäjä. Mikäli palvelulla on MyData-periaatteiden mukainen henkilötietorajapinta, niin portinvartijana toimiikin palvelun käyttäjä; hän päättää itse, mille tahoille hänen tietojaan saa luovuttaa.

Henkilötiedon arvoketjun pilkkominen on strategisesti merkittävä muutos. Se murentaa joitain nykyisin tyypillisiä liiketoimintamalleja. Esimerkiksi käyttäjistä kerättyyn tietoon ja ilmaisen palvelun avulla käyttäjämäärien kasvattamiseen perustuva liiketoiminta ei toimi ympäristössä, jossa asiakkaat voivat halutessaan nopeasti siirtää tietonsa toisiin palveluihin. Toisaalta arvoketjun pilkkoutuminen luo puitteet uudenlaiselle liiketoiminnalle ja palveluyritysten pitäisikin nähdä se mahdollisuutena solmia entistä läpinäkyvämpiä ja syvempään luottamukseen perustuvia asiakkuuksia. Yritykset voisivat myös kehittää liiketoimintamallejaan vahvemman asiakasymmärryksen perusteella ja hyödyntää asiakkaita palvelujen osatuotannossa ja suunnittelussa.

Tärkeä rooli hajautetussa arvoverkostossa on henkilötiedon välittämisen ja hallinnan palveluja tuottavilla tahoilla. Näitä voidaan kutsua MyData-operaattoreiksi (ks. luku 2). Pitkällä tähtäimellä datan välittämisen infrastruktuurin tarjonta tulisi hajauttaa samalla tavalla kuin pankki- tai teleoperaattoripalvelut. Joku voi luottaa talousdatansa pankille ja terveysdatansa terveysalan MyData-operaattorille, kun taas toinen ei luota muuhun kuin omalla koneellaan olevaan avoimen lähdekoodin ohjelmistoon. Hajautettujen peruspalvelujen pitäisi toimia kuitenkin yhteen – vastaavasti kuin pankkikortilla maksaminen toimii pankista riippumatta ja kännykkäpuhelut yhdistyvät eri teleoperaattorien verkosta toiseen. Asiakkaan kannalta tämä tarkoittaisi, että palveluja on helppo vaihtaa myös niin, että henkilön omat tiedot kulkevat mukana. Vaihtamisen mahdollisuus lisää kilpailua sekä luottamusta palveluihin ja siten kiihdyttää palvelujen kehitystä.

1.4 MyDatan hyötyjä

Mihin MyDatalla pyritään ja mitä hyötyä siitä on? Tässä luvussa on kuvattu MyDatan myönteisiä vaikutuksia ihmisten, yritysten ja yhteiskunnan kannalta. Hyödyt ihmisille ja organisaatioille ovat käyttövoima muutoksessa, joita ilman mitään ei tapahtuisi. Alusta alkaen on tärkeää löytää MyData-sovelluksia, jotka palvelevat konkreettisesti ihmisiä heidän arjessaan. Oikeuksien toteutuminen tai kestävämmät datatalouden periaatteet saattavat kiinnostaa joitakuita, mutta jokapäiväiset hyödyt saavat suuret joukot liikkeelle. Positiivisia yhteiskunnallisia vaikutuksia taas voidaan pitää suuntaa määrittävinä tavoitteina. Henkilötiedon infrastruktuuriin ja sääntelyyn tehtävien ratkaisujen pitää olla sellaisia, että ne lisäävät käyttövoimaa, mutta samalla ohjaavat suuntaan, joka mahdollistaa kollektiivisten hyötyjen toteutumisen pitkälle tulevaisuuteen.

1.4.1 Ihmisille

Suurinta osaa ihmisistä ei kiinnosta data itsessään, eivätkä he jaksa nähdä vaivaa oman datansa hallinnoinnissa. Myöskään oikeuksien vahvistuminen tai parempi tietosuoja ja yksityisyys eivät ole ensisijaisia motiiveja uudenlaisten palvelujen tai toimintamallien käyttöönottoon. Tarvitaan loppuun asti tuotteistettuja ja helppokäyttöisiä palveluja, jotka datan avulla auttavat ihmisten arkea.

Datan siirrettävyyden ansiosta palvelujen tarjoajia voi vaihtaa ketterästi ja oman tiedon hallinnoinnin taakka pienenee. Kun tiedon saatavuus helpottuu, voivat yritykset erikoistua tarjoamaan tuotteita monipuolisesti pienillekin asiakasryhmille.

Mahdollisuus jakaa hallitusti ja vaivattomasti omia tietoja eri organisaatioiden kanssa vaikuttaa ihmisten ja organisaatioiden välisiin suhteisiin, olivat ne sitten asiakassuhteita tai muita vuorovaikutussuhteita. Jos esimerkiksi työntekijät jakavat omasta hyvinvoinnista keräämäänsä tietoa työnantajansa kanssa, voi yrityksillä olla parempia keinoja työympäristön parantamiseen.

- **Uudenlaiset palvelut:** Kokonaan uudenlaisten palvelujen tuottamiselle avautuu mahdollisuuksia, kun eri lähteistä tulevaa tietoa voi hyödyntää ja yhdistää nykyistä helpommin. Ihmisten arkea helpottaisivat esimerkiksi entistä osuvammat suositusjärjestelmät, kohdistetut terveysneuvot ja oman talouden seurantaa ja kulutusvalintojen ymmärtämistä tukevat sovellukset.
- **Valinnanvapaus ja palvelujen vaihdettavuus:** Datan helppo siirrettävyys suojaa asiakkaita yksittäiseen palveluun lukittumiselta. Ihmiset voivat vaihtaa palveluntarjoajaa ja samalla siirtää omat tietonsa uuteen paikkaan. Tilanne on verrattavissa siihen, että teleoperaattorin vaihtaminen helpottui, kun asiakas sai säilyttää vanhan puhelinnumeronsa.
- **Informaation tasapuolisuus:** Ihmisten asema suhteessa organisaatioihin vahvistuu, kun heille on tarjolla paremmat keinot ymmärtää ja hallita organisaatioiden heistä keräämää tietoa. Lisääntyvän läpinäkyvyyden myötä kansalaisjärjestöjen ja viranomaisten on helpompi puuttua yksityisyyttä loukkaaviin väärinkäytöksiin

1.4.2 Yrityksille ja muille organisaatioille

MyData vastaa liiketoimintamallien tasolla muutokseen, jossa siirrytään nyt vauhdilla siiloista arvoverkostoihin muun muassa datan jakamisen, rajapintojen ja hajautetun luottamuksen mahdollistavien lohkoketjuteknologioiden avulla. Sääntely, kuten tietosuoja-asetus ja PSD2 ohjaavat samaan suuntaan. Ihmiskeskeinen henkilötiedon hallinta ja uudentyyppiset hajautetut digitaalisen identiteetin ratkaisut ovat välttämättömiä verkostomaisten digitaalisen talouden liiketoimintamallien mahdollistajia.

Kaikki henkilötietoa käsittelevät organisaatiot edistävät MyDataa avaamalla henkilötietorajapintoja. Ensi näkemällä motivaatio tämän tekemiseen voi olla epäselvä, ovathan asiakastiedot monelle yritykselle merkittävä kilpailutekijä. Tiettyyn rajaan asti lainsäädäntö edellyttää datan siirrettävyyttä kaikilta, ja tässä uudessa sääntely-ympäristössä proaktiivinen tietojen vaihtoon osallistuminen voi tarjota edelläkävijän aseman. Tietovarantoja keräävät tahot hyötyvät, jos muut tuottavat heidän tarjontaansa täydentäviä palveluja saman tiedon pohjalta. Esimerkiksi jos kanta-asiakaskortilla kerättyä dataa voi käyttää laajasti eri palveluissa, niin kortista tulee asiakkaille arvokkaampi ja sillä on positiivinen vaikutus kortin käyttöön ja asiakastyytyväisyyteen. Avoimiin toimintatapoihin sitoutuneille toimijoille voi myös kertyä näkyvyyttä ja brändin parantumista, jos ne erottautuvat eettisinä ja reiluina toimijoina.

- **Verkostomaiset liiketoimintamallit:** Ihmiskeskeinen henkilötiedon hallinta mahdollistaa saumattomien palvelukokonaisuuksien tuottamisen useiden organisaatioiden verkostoissa ilman keskitettyä alustatoimijaa. Ihmisten mahdollisuus itse päättää, ketkä heidän dataansa voivat käyttää, tarjoaa myös kotimaisille ja pienille toimijoille tasavertaisen pääsyn tietoon, johon nyt pääsevät käsiksi vain suuret kansainväliset toimijat.
- **Kuluttajien luottamus:** Luottamuksella on yhä merkittävämpi arvo yrityksille. Asiakkaat haluavat tietää, mitä heidän datallaan tehdään. MyData lisää organisaation läpinäkyvyyttä, auttaa luottamuksen rakentamisessa ja tuottaa mainehyötyjä.
- **Pienempi käyttäjämäärä riittää:** Nykyään verkkopalvelujen menestystä määrittää usein niin sanottu voittaja saa kaiken -ilmiö (winner takes all) ja moni hyvä palvelu kuolee, koska ei saavuta kriittistä käyttäjämäärää. MyData-palvelut ovat yhteentoimivia ja keskenään vaihdettavia datan helpon siirrettävyyden ansioista. Tämän ansiosta myös pienet niche-palvelut hyötyvät verkostovaikutuksista.

1.4.3 Yhteiskunnalle laajemmin

Henkilötietojen käytöstä puhutaan useimmiten vain joko yksilöiden tai organisaatioiden näkökulmasta. Yhteiskunnallinen vaikutus voi olla kuitenkin muutakin kuin vain summa yksittäisille toimijoille koituvista hyödyistä ja haitoista.

Ihmisoikeuksien ja tietotekniikan kehitys ovat kulkeneet pitkälti toisistaan erillään. MyData on ihmiselle keino ottaa digitaaliset oikeudet haltuunsa. Ihmisellä on oltava oikeus ja mahdollisuus hallita omaa digitaalista identiteettiään siinä missä hänellä on oikeus ajattelun ja ilmaisun vapauteen kansalaisena. MyData tarjoaa henkilötiedon organisoinnille pitkäjänteisen mallin, joka toimii kestävänä pohjana tietoyhteiskunnalle.

Ihmiskeskeiset henkilötiedon hallintamallit voivat parhaimmillaan tukea esimerkiksi yhteiskunnallista tiedonkeruuta, sosiaalista oikeudenmukaisuutta, osallistumista ja kollektiivista vastuullista toimintaa. Lisäksi ihmiset saisivat arkea helpottavia palveluja ja yrityksille avautuisi uusia liiketoimintamahdolli-

suuksia. Tärkeitä kysymyksiä ovat mm. kuinka kollektiivista toimintaa voitaisiin käyttää datatalouden tasapainottamiseen ja kuinka ihmiset voivat henkilötietojaan jakamalla luoda yhteiskunnallista ja yhteisöllistä arvoa sen lisäksi, että osallistuvat taloudellisen arvon tuotantoon?

- **Yhteiskunnallinen tiedon käyttö:** Vaikeiden ongelmien ratkaiseminen helpottuu, kun tutkijat ja päätöksentekijät saavat työkaluja kattavampaan tiedonkeruuseen. Ihmiset voivat esimerkiksi antaa lupia omien tietojensa hyödyntämiseen tutkimuskäytössä.
- **Lainsäädäntö yksinkertaistuu:** Tarve säätää lailla käyttötapauskohtaisia tiedonsaantioikeuksia eri tarkoituksiin vähenee, kun henkilö voi luvittaa tietojensa luovuttamisen julkishallinnon tietovarannoista yksityisten palveluiden käyttöön.
- **Valinnan vapaus ja datan vapaa liikkuminen:** Ihmiset käyttävät yhä enemmän digitaalisia palveluja normaalissa arjessaan. Datan siirrettävyys mahdollistaa palvelujen vapaan vaihtamisen ja ihmisten ja palvelujen liikkumisen globaalisti ilman rajoja.

Avoin data, big data ja MyData

Viime vuosina erityisesti julkishallinnon toimijat ovat julkaisseet tietovarantojaan avoimena datana niiden hyötykäytön lisäämiseksi. Myös henkilötiedon alueella selkeillä datan hallinnan periaatteilla, paremmalla yhteentoimivuudella ja datan siirrettävyydellä voidaan saavuttaa mittavia hyötyjä. Tällä hetkellä henkilötieto on rajusti alikäytetty raaka-aine uusille palveluille.

MyData on avoimen tiedon kanssa rinnakkainen ideologia, joka korostaa tiedon hyödynnettävyyttä esimerkiksi tietojen helpon siirrettävyyden ja koneluettavuuden kautta. Molemmissa tarvitaan yhteisistä periaatteista sopimista, viisasta sääntelyä sekä rajapintoja, standardeja ja palveluja tiedon hallittuun siirtämiseen, varastointiin, käsittelyyn ja analysointiin.

Opendefinition.org määritelmän mukaan avoin aineisto on teknisesti ja juridisesti kenen tahansa vapaasti ja uudelleen käytettävissä ja jaettavissa. Vastaavasti MyData voitaisiin määritellä niin, että se on teknisesti ja juridisesti datan kohteen itsensä vapaasti ja uudelleen käytettävissä ja jaettavissa.

Massadatalla (big data) viitataan suureen ja nopeasti karttuvaan tiedon määrään, jonka kerääminen, tallennus ja analyysi vaativat uusia käsittelymenetelmiä. Toisaalta massadatan voi käsittää myös tiedon paradigman muutoksena. Sen myötä yrityksissä ja hallinnossa voidaan yhä useammin tehdä päätöksiä, jotka perustuvat suoraan kerättyyn tietoon. Tutkimuksessa on mahdollista muodostaa teoriaa uusilla tavoilla, kun datamassojen analysointi ja yhdistely on entistä helpompaa. (LVM, 2014)

Suuria datamääriä syntyy mm. internetiin kytketyistä laitteista, anturijärjestelmistä, sosiaalisesta mediasta, verkon yli tehtävistä transaktioista, yritysten liiketoimintaan liittyvistä ohjaus- ja raportointijärjestelmistä jne. Suuri osa massadatasta on ihmisten käyttäytymisdataa. Massadata-keskustelussa korostetaan henkilötietojen analysoinnin ja hyödyntämisen mahdollisuuksia organisaatioiden näkökulmasta. Ihmisten näkökulma on supistettu usein vain vaatimukseen siitä, että yksityisyydensuoja säilytetään. Asiakkaan kiinnostusta saati oikeutta omiin tietoihinsa ei massadata-keskustelussa juurikaan ole tuotu esille.

Henkilöihin liittyvässä tiedossa MyData ja massadata ovat kaksi toisiaan täydentävää näkökulmaa, “ihmisnäkökulma” ja “yritysnäkökulma”. MyData tuo läpinäkyvyyttä ja sitä kautta hyväksyttävyyttä henkilöihin liittyvien datamassojen käsittelyyn ja antaa konkreettisia keinoja yksityisyydensuojan toteuttamiseen. Ilman tätä ihmisnäkökulmaa monet massadatan hyödyntämismahdollisuudet katoavat, koska ne eivät ole yksityisyyden suojan kannalta hyväksyttäviä.

Olennaista on, että kontrolli omaan dataan on ihmisillä itsellään, infrastruktuuripalvelujen tarjoajia on useita ja palvelut ovat yhteentoimivia ja vaihdettavissa.

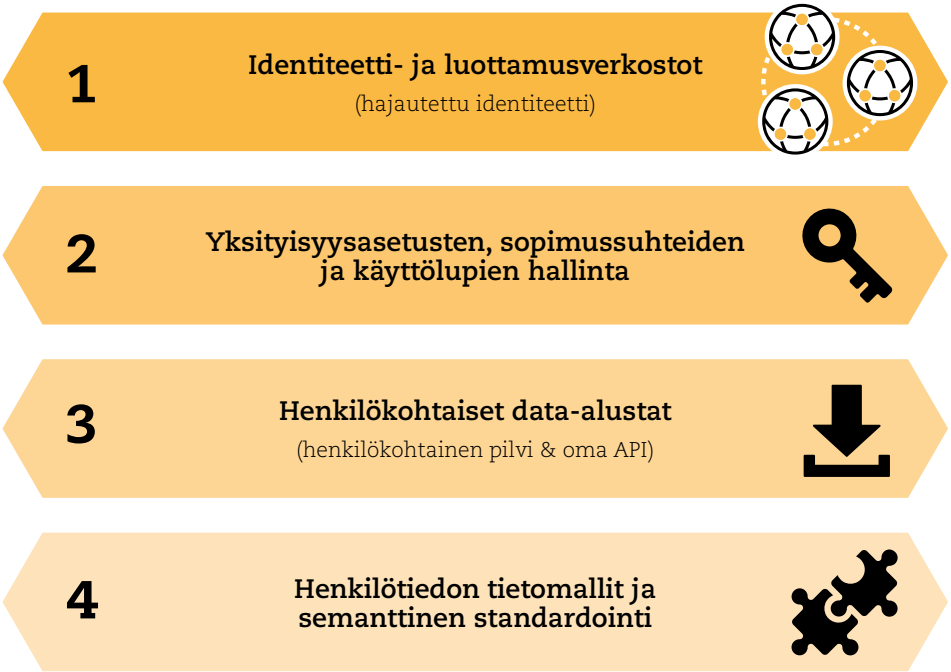
2. MyData-infrastruktuuri

Tässä luvussa kuvataan teknologinen visio globaalista ihmiskeskeisen henkilötiedon jakamisen infrastruktuurista, joka pohjautuu alustojen sijaan verkostoihin. Organisoitumistapa vaikuttaa siihen, kuinka helposti hyödynnettävää henkilötieto on, kuinka läpinäkyvää tiedon käyttö on, kuinka hyvin rakenteet tukevat avointa kilpailua sekä kuinka ihmiskeskeistä henkilötiedon hyödyntäminen tulevaisuudessa on. Olennaista on, että kontrolli omaan dataan on ihmisillä itsellään, infrastruktuuripalvelujen tarjoajia on useita ja palvelut ovat yhteentoimivia ja vaihdettavissa.

Tämä on yksi näkemys siitä, millaisilla teknisillä ja organisatorisilla ratkaisuilla MyData-periaatteet voitaisiin toteuttaa laajassa mittakaavassa ja kestävästi. Tavoitteena on luotettava ja pelkistetty palveluinfrastruktuuri, joka on avoin uusille toimijoille ja uusille innovaatioille. Palvelut olisivat laajennettavissa, ja niitä voisi helposti vaihtaa, koska data liikkuisi sujuvasti rajapintojen ja operaattorien välisen yhteentoimivuuden ansiosta. Ihmisille tämä tarkoittaisi muun muassa helppokäyttöisiä palveluja yksityisyysasetusten etähallinnointiin, oman tiedon säilytyspalveluja ja omien profiilien ylläpitopalveluja.

Visio on synteesi maailmalla tapahtuvasta kehityksestä. Sellaisenaan visio ei tule toteutumaan, koska kehitys on vielä varhaisessa vaiheessa. Jotkut ajatukset kuten ekosysteemin roolit ja hajautettujen tunnisteiden merkitys ovat laajasti tuettuja. Kehitykseen vaikuttavat uudistuva lainsäädäntö, teknologian ja standardien kehitys, henkilötiedon hallinnan alalla toimivat yritykset liiketoimintamalleineen sekä muuttuva yleinen mielipideilmasto ja datatalouden nykyisiin rakenteisiin kohdistuva kritiikki.

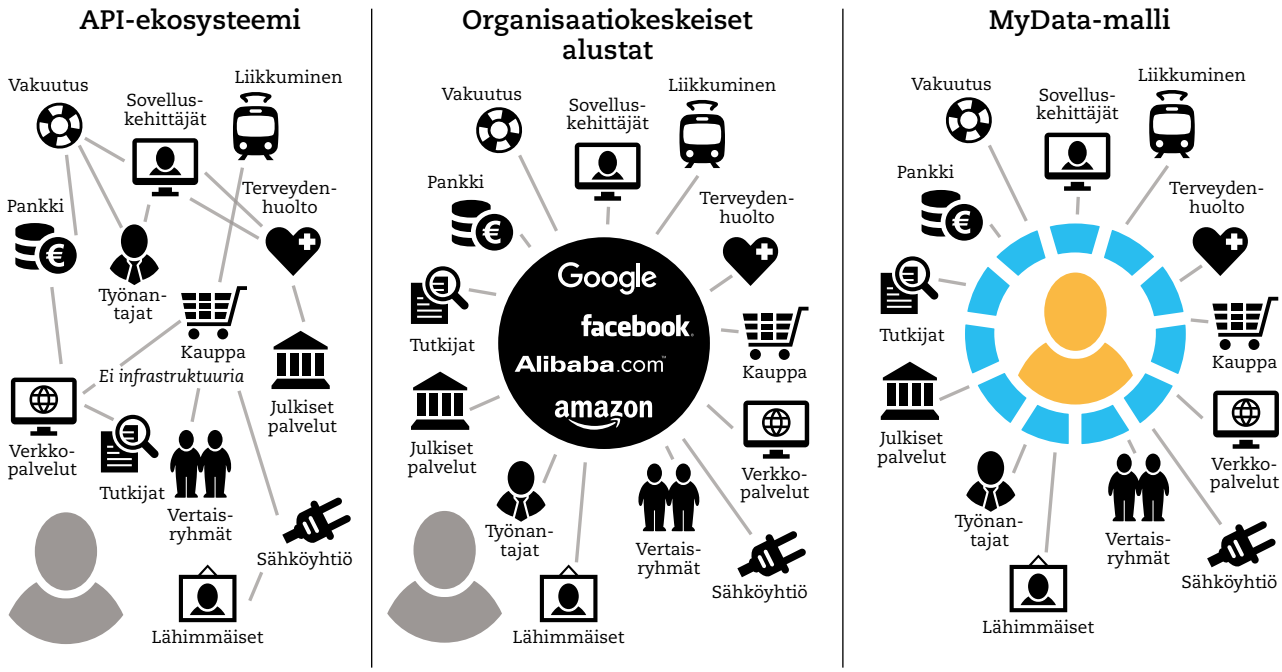
Kuvattua visiota ei kannata ajatella yhtenä suurena kokonaisuutena, joka pitäisi rakentaa kerralla valmiiksi. Luvun lopussa on esitetty, miten eri kerroksia MyData-infrastruktuurista ollaan jo kehittämässä.



Kuva 2.1: MyData-infrastruktuurin eri kerrokset täydentävät toisiaan. Kunkin kerroksen teknologioita kehitetään itsenäisesti myös MyDatasta riippumatta.

2.1 Alustoista verkostoihin

Tarvitaanko henkilötiedon organisointiin infrastruktuuria ylipäänsä? Eikö olisi helpompaa, jos rajapinnat ja sovellukset keskustelisivat suoraan keskenään ilman välissä olevaa tiedonvälittämisen infrastruktuuria? Monin paikoin kehitys on vienyt tällaisen orgaanisesti laajentuvan infrastruktuurittoman, niin sanotun API-ekosysteemin suuntaan. Toisaalla taas on syntynyt alustoja, joissa yksittäinen toimija kerää ja harmonisoi dataa useasta lähteestä ja jakelee sitä eteenpäin. MyData-mallissa henkilötiedon hallinnan palveluja tarjoavat toimijat ovat keskenään kilpailevia, mutta muodostavat yhteentoimivan verkoston ja yhdessä tarjoavat infrastruktuurin henkilötiedon välittämiseen. Nykykehityksessä näkyy viitteitä näistä eri organisointitavoista, jotka tulevaisuudessa eivät välttämättä sulje pois toisiaan.



Kuva 2.2: Nykyisessä infrastruktuurittomassa API-ekosysteemissä, jos palvelujen määrä kasvaa, niin yhteyksien määrä kasvaa vielä nopeammin (vasen). Datan hallinnan keskittäminen helpottaa sovellusten kehittämistä, mutta eri alustatoimijoilla ei ole lähtökohtaisesti motiivia pyrkiä alustojen väliseen yhteentoimivuuteen (keskellä). Alustamalliin verrattuna MyData-infrastruktuuri on kestävä ja joustava, koska se ei ole riippuvainen yksittäisestä organisaatiosta (oikealla).

2.1.1 API-ekosysteemi

Ohjelmointirajapintojen eli APIen avulla yhteyksiä eri palvelujen välille voidaan luoda ketterästi. Näin syntyvä API-ekosysteemi edistää tiedon virtaamista, luo uutta liiketoimintaa ja nopeuttaa digitaalista palvelukehitystä. Yleensä APIn kehittämisen motiivi on tehdä omasta palvelusta mahdollisimman keskeinen osa laajempaa palvelukokonaisuutta. Toteutettujen rajapintojen ominaisuudet vaihtelevat kuitenkin merkittävästi, mikä tekee eri palveluntarjoajien APIen yhdistämisestä työlästä.

Rajapintojen tekninen yhdisteltävyys varmasti paranee ajan myötä. Henkilötiedon ihmiskeskeisen hallittavuuden kannalta API-ekosysteemin ongelma on palvelujen ja niiden välisten yhteyksien suuri määrä ja ylläpidon monimutkaisuus. Ainoa tapa saada kokonaiskuva omien tietojen liikkumisesta palvelujen välillä on kirjautua jokaiseen palveluun erikseen, ja etsiä paikka, jossa näytetään,

mille kaikille muille palveluille on myönnetty lupa lukea dataa rajapinnan kautta. Muutaman palvelun erillinen hallinta on vielä mahdollista, mutta digitalisaatio myötä jokainen brändi ja palvelu haluaa muodostaa kuluttajan kanssa oman digitaalisen asiakkuussuhteen, johon liittyy datan keruuta ja jakamista. Hallittavia suhteita voi tulevaisuudessa olla kymmenien sijaan satoja tai tuhansia, ja silloin tiedon ja digitaalisten vuorovaikutussuhteiden hallintaa helpottavan infrastruktuurin tarve on jo ilmeinen.

2.1.2 Organisaatiokeskeiset alustat

Avoimiin standardeihin perustuvan henkilötiedon hallinnan ja välittämisen infrastruktuurin puuttuessa yksittäiset globaalisti toimivat yritykset laajentavat kukin omaa henkilötiedon ekosysteemiään ja pyrkivät suuren käyttäjämäärän voimalla de facto -standardin asemaan. Yhteistä näiden alustatalouden jättiläisten luomissa organisaatiokeskeisissä ekosysteemeissä on, että tieto siirtyy saumattomasti keskusyrityksen tarjoaman alustan ja käyttäjäidentiteetin ympärille rakentuneen ekosysteemin sisällä, mutta vain rajoitetusti sen ulkopuolelle. Riskinä on, että uusien toimijoiden tulo markkinoille estyy tai ne joutuvat alihankkijan asemaan ilman valinnan tai vaikuttamisen mahdollisuuksia.

Alustamallia hyödynnetään myös eri sektoreilla mahdollistamaan useiden toimijoiden keräämän tiedon yhteiskäyttöä. Terveyssektorilla on tästä useita esimerkkejä eri maissa, kuten sveitsiläinen Health bank, brittiläinen Patients Know Best ja Suomen valtion Kanta-palvelu. Tällaisessa rakenteessa yritykset tai julkishallinnon toimijat perustavat yhteisen alustapalvelun tiedon välittämiseen. Keskittäminen edistää tiedon yhdistämistä ja uusien käyttötapojen kehittämistä, mutta samalla järjestelmä tulee riippuvaiseksi yksittäisestä toimijasta, joka määrittää toiminnan tavoitteet ja tekemisen tavat.

Ihmisten mahdollisuudet omien tietojensa käyttöön ja hallintaan eivät välttämättä toteudu alustoissa, jotka on ensisijaisesti toteutettu joko tukemaan keskusyritysten liiketoimintamalleja tai ekosysteemissä mukana olevien organisaatioiden välistä tietojen vaihtoa. Esimerkiksi verkkomainonnan yritykset toimivat verkostoissa, joissa muutamat aggregaattoriyritykset edesauttavat henkilötiedon liikkumista, mutta eivät ihmisten omien tarpeiden vaan verkostossa mukana olevien yritysten tarpeiden täyttämiseksi.

2.1.3 MyData-malli

Ihmiskeskeisessä mallissa ihminen voi itse toimia oman datan yhdistävänä tekijänä. MyData-tilin kautta ihminen voi hallinnoida omien tietojensa käyttöä eri palveluissa antamalla tai eväämällä tiedon käyttölupia tai antamalla palveluille toimeksiantoja omien tietojensa suhteen. Osa ihmisistä voisi ylläpitää MyData-tiliään tietoturvallisesti itsekin, mutta todennäköisesti suurin osa haluaa nojautua ulkopuolisiin palveluntarjoajiin. Palveluntarjoajat tarjoavat ihmisille ja myös organisaatioille henkilötietojen hallintaan yleiskäyttöisiä sovelluksia ja työkaluja, jotka toimivat useamman tiedon tyypin ja tietolähteen kohdalla.

Keskeinen ero alustamalliin on, että MyData-mallissa henkilötiedon hallinnan palveluja tarjoavat toimijat muodostavat verkoston, jossa henkilötietoa jaetaan luotettavalla tavalla. Infrastruktuuri ei perustu siihen, että käyttäjien tietoja keskitettäisiin yksittäiseen palveluun kuten alustamallissa. Sen sijaan verkostoon osallistuvilla on yhteiset standardit ja toimintatavat, jotka mahdollistavat yhteentoimivuuden. Tätä voisi verrata vaikkapa pankkien verkostoon. Sen sijaan, että pankki pystyisi välittämään maksuja vain omien asiakkaittensa välillä (alustamallinen pankki) pankit muodostavat kansainvälisen verkoston, missä maksuja voidaan välittää eri pankkien asiakkaiden välillä.

2.2 Ihmislähtöinen tiedonvaihdannan ekosysteemi

MyDatan kilpailua ja avointa ekosysteemiä korostava visio pohjautuu oletukseen siitä, että henkilötiedon välittämisen ja hallinnan palveluja tarjoavia toimijoita tulee olla lukuisia ja niiden tulee olla keskenään yhteensopivia ja vaihdettavissa. Kilpailevat palveluntarjoajat yhdessä luovat globaalin verkoston ihmiskeskeiseen henkilötiedon välittämiseen vastaavalla tavalla kuin pankit luovat verkoston maksujen välittämiseen, puhelinoperaattorit puhelujen välittämiseen ja sähköpostipavelimet sähköpostien välittämiseen.

2.2.1 Pääsy verkostoon MyData-tilin kautta

Sekä ihmisillä, datan lähteillä että dataa hyödyntävillä palveluilla tulee olla tiedonvaihdannan verkostoon kytketty digitaalinen identiteetti, jotta tiedon välittäminen eri toimijoiden välillä on mahdollista. Digitaalisia identiteettejä hallinnoidaan MyData-tilien kautta. Tili on metaforana tuttu pankkitileistä, sähköpostitileistä ja asiakastileistä. MyData-tilit tarjoavat keskitetyn näkymän omiin tietoihin sekä siihen, kuka näitä tietoja tällä hetkellä käyttää. Tilien kautta voidaan hallita annettuja tiedon käyttölupia ja tiedon käsittelyn toimeksiantoja.

Keskitetty näkymä ja hallinnointipaikka omiin tietoihin ja eri sovellusten ja palveluntarjoajien kanssa muodostettuihin yhteyksiin on tarpeellinen, vaikka jokapäiväinen asiointi pääosin tapahtuukin muualla. Päätöksiä tiedon käytöstä tehdään esimerkiksi sovellusten käyttöönoton yhteydessä tai myöhemmin yksityisyysasetuksia vaihtamalla. MyData-mallissa kaikki annetut luvat ja erilaiset yksityisyysasetukset kuitenkin tallentuvat käyttäjän MyData-tilille riippumatta siitä, missä ne on tehty. Samalla tavalla esimerkiksi verkkopankki on keskitetty näkymä omiin raha-asioihin ja maksutapahtumiin, vaikka suurin osa maksuista tehdään pankkikortilla aivan muualla kuin verkkopankin käyttöliittymässä.

Teknisesti MyData-tili on tiedonvaihdannan verkostoon kytkeytynyt ohjelmistoagentti (software agent), joka voi olla asennettuna käyttäjän päätelaitteelle tai pilvipalveluun. MyData-tiliä käytetään yhdessä identiteetilompakon kanssa, joka puolestaan on turvattu moduuli (tyypillisesti laitteiston ja ohjelmiston yhdistelmä), missä on tallennettuna identiteetin haltijan yksityiset kryptoavaimet. Tavoitteena on sellainen MyData-infrastruktuuri, missä jaetut standardit mahdollistavat erilaisten MyData-tilien ja identiteettilompakkojen keskinäisen yhteentoimivuuden.

Kuten aiemmin mainittiin, niin ei ole teknistä estettä sille, etteikö käyttäjä voisi itse ylläpitää omaa MyData-tiliään (siihen vaadittavaa ohjelmistoa) ja siten itsenäisesti kytkeytyä verkostoon. MyData-mallin skaalautuessa suurille käyttäjämäärille on kuitenkin oletuksena, että suurin osa turvautuu palveluntarjoajiin, jotka ylläpitävät MyData-tilejä loppukäyttäjien puolesta. Yhtenä keskeisenä suunnitteluperiaatteena MyData-infrastruktuurissa on, että MyData-tilin tulisi olla siirrettävissä palveluntarjoajalta toiselle vaivattomasti ilman, että tilin sisältö katoaa tai tilin kautta annetut luvat ja kytkennät lakkaavat toimimasta. Tilin siirrettävyys lisää luottamusta verkostoon ja avaa markkinoita kilpailulle. Luonnollisesti tietosuoja ja yhteensopivuus eri toimijoiden välillä on haaste siirrettävyyden toteuttamisessa.

MyData-tilien ominaisuuksia:

- “Tiliotteet” oman tiedon käytöstä: selkeät näkymät tiedon käytön kokonaisuudesta.
- Ihmisillä voi olla useita MyData-tilejä ja osa niistä voi olla usean henkilön yhteisiä.
- Tileillä on erilaisia tunnistautumisen tasoja. Jotkut niistä on vahvasti kytketty ihmisen henkilöllisyyteen, osa on pseudonyymitilejä, joihin tunnistaudutaan esimerkiksi vain sähköpostiosoitteen perusteella.
- MyData-tili osaa hallita tiedon luovuttamista ja pitää automaattisesti rekisteriä siitä, mitä tietoa on luovutettu minnekin.
- MyData-tilejä ja niihin linkitettyjä identiteettejä voi yhdistää ja linkittää toisiinsa.
- Tilejä voi hallinnoida suoraan tai erillisten käyttöliittymien kautta (vertaa sähköpostiohjelmat, joilla voi hallita useita sähköpostitilejä).

Muita toimintoja, joita palveluntarjoajat voivat tarjota:

- Yksityisyysasetusten etähallinta
- Oman suostumuksen kumoaminen ja tiedon poistaminen sitä käyttävistä palveluista (huom. lakisääteisistä rekistereistä ihmisellä ei ole oikeutta poistaa omia tietojaan)
- Erilaisten datan lähteiden ja palvelujen löytäminen ja yhdistäminen
- Rajapintoihin liittyminen ja sen vaatima tunnistautuminen sekä yksilöille että organisaatioille
- Henkilötiedon tallennus käyttäjän niin halutessa (ks. 2.3.3 Henkilökohtaiset data-alustat)
- Työkaluja datan muuntamiseen, yhteensopivuuden varmistamiseen ja omien tietojen hyödyntämiseen

MyData-operaattorin referenssiarkkitehtuuri

Yksi käyttäjäkeskeisen pääsynhallinnan malli on kuvattu Aalto-yliopiston, Tampereen yliopiston ja Oulun yliopiston yhteistyönä tuottamassa ns. MyDatan referenssiarkkitehtuurissa, joka hahmottelee MyData-tilin ja suostumustenhallinnan toteutusmalleja. Tämä arkkitehtuuri ja siihen liittyvä kehitys- ja kokeiluympäristö on avattu ja saatavilla osoitteesta **sandbox.mydata.fi**.

Malli vastaa pitkälle tietosuoja-asetuksen asettamia vaatimuksia henkilötiedon käytön läpinäkyvyydestä ja henkilötiedon käsittelyn hallintamahdollisuuksien kirjosta. Se ei ota infrastruktuuritasolla kantaa identiteetinhallintaan eikä tilien siirrettävyyteen. Arkkitehtuuri kuvaa yksittäisen MyData-operaattorin toteuttamisen ja palvelujen liittämisen operaattorilla ylläpidettävään käyttäjän tiliin, joka sisältää käyttäjän antamat luvat, tiedonsiirtoilmoitukset ja käsittelykiellot.

Referenssiarkkitehtuuri on teorian mutta ei käytännön tasolla yhteensopiva IT-järjestelmissä vakiintumassa olevien käyttövaltuushallinnan teknologioiden kanssa, ja tämä on yksi sen suurimpia haasteita. Lähes sama rajapintojen luvittamiseen liittyvä toiminnallisuus voidaan saavuttaa yhdistelemällä väljästi standardipohjaisia toteutuksia kuten OAuth 2.0:n eri profiileja (erityisesti UMA 2.0) luvittamiseen, XACML (eXtensible Access Control Markup Language) käyttäjän hallintapolitiikkojen kuvaukseen ja Kantaran suostumuskuittia dokumentointiin.

Luodun mallin eduksi voi katsoa sen luvitusmekanismien sitomisen vahvasti tietosuojatun ja pääsyoikeudet dokumentoivan suostumustenhallinnan alle. Teoriassa suostumukset ovat myös siirrettävissä operaattorilta toiselle. Käytännössä tarvittava käyttäjien PKI-avainten luotettava siirtäminen olisi kuitenkin haastavaa – kuten on käyttäjien avainten hallinta osana operaattorin palvelua jo itsessään.

2.2.2 Ekosysteemin roolit

Henkilötiedon jakamisen ekosysteemissä on neljä roolia: ihminen, datan lähde, dataa käyttävä palvelu sekä operaattori. Toimijat voivat olla samanaikaisesti useammissa rooleissa. Esimerkiksi yritykset ovat tyypillisesti sekä datan lähteitä että dataa hyödyntävien palvelujen tarjoajia. Myös muissa rooleissa olevat toimijat voivat ottaa lisäksi operaattorin roolin ja ylläpitää itse MyData-tiliä, jota kautta ne kytkeytyvät verkostoon.

	**Ihminen** on verkostossa identiteetin haltija ja se henkilö, jonka datasta on kyse. Ihminen hallinnoin, mitkä tahot saavat hänen dataansa ja mihin käyttötarkoituksiin.
	**Datan lähde** kerää, käsittelee ja mahdollistaa henkilötiedon jakelun muille toimijoille verkostossa.
	**Dataa käyttävä palvelu** voi henkilön valtuuttamana hakea ja käyttää henkilötietoa yhdestä tai useammasta datan lähteestä.
	**Operaattori** mahdollistaa henkilötiedon käyttölupien digitaalisen hallinnan ja varmentamisen tarjoamalla MyData-tilipalveluja.

Kuva 2.3: Roolit henkilötiedon jakamisen ekosysteemissä.
Huom. sama toimija voi olla useammassa roolissa.

Datan välittämisen verkostossa voidaan henkilötiedon lisäksi välittää myös esimerkiksi yrityksiin tai esineisiin liittyvää tietoa. Teknisesti ei ole merkittävää eroa, onko dataa hallinnoiva taho ihminen vai esimerkiksi organisaatio, mutta lainsäädäntö on erilainen silloin, jos käsitellään henkilötietietoa.

Luonnollisesti ekosysteemin toimintaan vaikuttavat muutkin toimijat kuten sääntelevät viranomaiset, standardointiorganisaatiot, rahoittajat, media jne. Nämä yhdessä luovat toimintaympäristön ja reunaehdot, missä henkilötiedon jakamisen ekosysteemi ja markkinat kehittyvät.

2.2.3 Erikoistuneet dataoperaattorit

Operaattorin roolin voi ekosysteemissä ottaa mikä tahansa toimija ja ainakin ensimmäisissä käyttötapauksissa tämän roolin toteuttaa useimmiten joko datan lähde tai dataa hyödyntävä palvelu. Liiketoiminnallisesti henkilötiedon hallinnoinnin ja välittämisen ja siihen liittyvien palvelujen tulisi olla erotettu tai ainakin erotettavissa datan hyödyntämiseen liittyvästä liiketoiminnasta. Erottelu mahdollistaa datan hyödyntämistapojen suhteen neutraalin ja erilaisille toimijoille avoimen tiedonvaihdannan ekosysteemin kehittymisen. Myös ihmislähtöisten periaatteiden toteuttaminen on helpompaa liiketoiminnallisessa ympäristössä, jossa datan hyödyntäjäorganisaatioiden motiivit eivät ohjaa datan välittämiseen liittyvän infrastruktuurin kehittymistä.

Tämä nostaa keskusteluun mahdollisuuden erikoistuneista MyData-operaattoreista, jotka lähtökohtaisesti pyrkivät rakentamaan henkilötiedon välittämisestä kestävää ja kannattavaa liiketoimintaa. Jokaisella voisi olla luotettuja MyData-operaattoreita eri tiedoilleen: terveystiedot, omaisuustiedot, kuluttajaprofiilitiedot, liikkumisprofiilitiedot jne. Jotkut operaattoreista voivat erikoistua tiettyihin toimialoihin ja toiset voivat olla yleisluontoisia. Halutessaan ihminen voisi hallita kaikkia tietojaan myös vain yhden operaattorin kautta.

MyData-malli helpottaa myös henkilödataa hyödyntävien palvelujen toteuttamista, kun sovellusten kehittäjien ei tarvitse toteuttaa yleisiä ominaisuuksia, kuten vaikkapa henkilötiedon käyttölupien hallintaa erikseen palveluihinsa. Sovelluskehittäjille operaattorien muodostama verkosto tarjoaa riittävän suuren asiakaspotentiaalin, eikä yksilöitä palvelevilla operaattoreilla ole intressiä sulkea markkinoita esimerkiksi tukemalla vain tiettyjä sovelluksia.

Keskittäminen tuo etuja, mitä vikaa siinä on?

MyDatan tavoitteisiin kuuluu henkilötiedon hallinnointi- ja hyödyntämispalvelujen organisointi ihmiskeskeisesti ja käytettävästi. Operaattorimalli jossain määrin monimutkaistaa asioita. Ei olekaan enää yhtä pistettä, jonka kautta kaikki tieto yhdistyy, vaan on useita rinnakkain toimivia operaattoreita.

Tällaisen avoimen yhteentoimivuutta korostavan operaattorikentän synnyttäminen on kova urakka. Miksi ei vain tyydyttäisi kansainvälisten, keskenään kilpailevien, mobiiliviestintää tai sosiaalisen median palveluja tarjoavien yhtiöiden walled-garden tyyppisiin ekosysteemeihin MyData-tiedon säilytys- ja kehityspaikkoina – tai tavoiteltaisi yhtä, vaikkapa kansallista, alustatoimijaa henkilötiedon välittämiseen?

Yhden organisaation mallissa koko järjestelmän riippuvuus tästä yhdestä toimijasta tekee järjestelmästä haavoittuvaisen (single point of failure). Jos on vain yksi taho, niin ongelmat syntyessään koskevat kaikkia, jolloin seuraukset voivat olla katastrofaalisia.

Useampi operaattori mahdollistaisi myös ketterän ja monipuolisen palvelukehityksen ja vaihtoehtoisten kilpailevien infrastruktuuripalvelujen rinnakkaisen kehittymisen. Toiset kaipaavat enemmän suojaa, kun taas toiset arvostavat järjestelmän keveyttä ja vapautta tehdä asioita itsenäisesti. Yhden organisaation malli saattaa helposti muuttua jäykäksi ja hitaaksi eikä sovellu kevyiden käyttötapausten ketterään toteuttamiseen.

Monessa muussa maassa kansalaisilla on huomattavasti vähemmän luottamusta hallintoon kuin Suomessa. Näissä maissa kansallisesti organisoitu tietojärjestelmä ei soveltuisi arkielämää ja yksilönvapautta korostavien sovellusten alustaksi. On verrattain poikkeuksellista, että Suomessa osa alan asiantuntijoista uskoo kansallisesti keskitetyn mallin mahdollisuuksiin. MyDatan kannalta on keskeistä, että toimintamalleilla on mahdollisuus kansainvälisesti laajamittaiseen vaikuttavuuteen.

2.3 MyDataan liittyvien teknologioiden kerrokset

MyDatassa ei ole kyse yksittäisestä teknologiasta vaan viitekehyksestä, joka koostuu toisiaan täydentävistä ja tukevista kerroksista (kuva 2.1 luvun alussa). Eri kerroksilla on kullakin itsenäinen arvo ja omat kehityspolkunsa. Esimerkiksi hajautettujen tunnisteiden identiteettiratkaisut, luottamusverkostot, henkilökohtaiset datavarastot, koneluettava datan jakamisen kirjanpito (ehdot, suostumukset, toimeksiannot, sopimukset, lokitiedot, jne.), ihmiskeskeinen profilointi, ihmisten, organisaatioiden ja esineiden välisten suhteiden hallinta jne. ovat kaikki asioita, joita kehitetään joka tapauksessa MyData-infrastruktuurista riippumatta.

2.3.1 Identiteetti- ja luottamusverkostot

Taso 1: Luottamusverkostot

Liittyy muihin tasoihin: Identiteetti- ja luottamusverkostot tarjoavat yhteentoimivuuden kerroksen sopimussuhteiden ja käyttölupien hallintaan (2.3.2) sekä henkilökohtaisiin datalustoihin (2.3.3).

Haasteita: Nykyiset identiteetti- ja luottamusverkostot mahdollistavat yksittäisten melko muuttumattomien identiteettiattribuuttien jakamisen, mutta eivät ratkaise päivittyviin tapahtumavirtoihin liittyviä datan hallinnan haasteita, kuten rajapintojen käytön luvittamista.

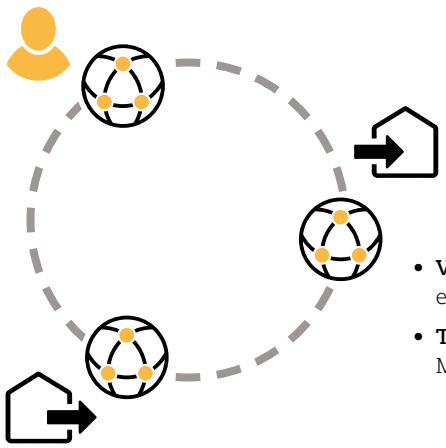
Teknologioita ja standardikehitystä: W3C hajautetut tunnisteet (Decentralized Identifiers DID), Oasis hajautettu kryptoavainten hallinta (Decentralized Key Management System DKMS), hajautettuihin tunnisteisiin pohjautuva autentikointi (DID-Auth), W3C vahvistettavissa olevat identiteetti-attribuutit (Verifiable Credentials)

Referenssejä: Hyberledger Indy ja Sovrin, uPort, Veres One ja Blockstack.

Liittyviä konsepteja: Itsehallittava identiteetti (self sovereign identity), identiteettiledger, mainejärjestelmät ja luottamuksen verkosto (web of trust), luottamusverkostojen hallintomallit (governance and rule books).

Sähköinen luotettava ja helposti käytettävä identiteetti on tärkeä mahdollistaja toimivalle henkilötiedon ekosysteemille. Yksittäisistä identiteetintarjoajasta riippumattomat hajautetut identiteettiratkaisut mahdollistavat MyData-mallissa palvelujen vaihdettavuuden sekä tunnistautumis- ja käyttöoikeusratkaisujen yhteentoimivuuden eri palvelujen välillä.

Tiedon luovutus rajapintojen kautta edellyttää, että ihmiset ja organisaatiot pystyvät tunnistautumaan ja antamaan lupia tietojensa siirtoon. Mikäli luottamus toisen osapuolen sähköiseen identiteettiin puuttuu, organisaatiot eivät uskalla luovuttaa mitään tietoja rajapintojen kautta. Tämä ei kuitenkaan tarkoita, että kaikissa tapauksissa pitäisi käyttää esimerkiksi pankki- ja mobiilitunnisteisiin pohjautuvaa vahvaa tunnistautumista. Toisiin tarkoituksiin riittää tavanomainen käyttäjätunnus-salasana-tunnistautuminen, joka voi toimia vahvaa tunnistautumista joustavammin ilman että käyttäjän henkilöllisyys paljastuu. MyData-ekosysteemin tulee ehdottomasti tukea useita tunnistautumisen tapoja ja tasoja.



- **Verkostovaikutukset:** kaikki toimijat eivät tule kytkeytymään yhteen alustaan!
- **Tilin siirrettävyys:** mahdollisuus vaihtaa MyData-tili palveluntarjoajalta toiselle

Kuva 2.4: MyData-malli on verkostopohjainen, eikä siinä oleteta, että kaikki ihmiset, datan lähteet ja dataa käyttävät palvelut kytkeytyisivät yhteen datan jakamisen alustaan.

MyData-mallin yksi keskeinen ajatus on, että ihmisille on tarjolla useita yhteentoimivia, mutta kilpailevia tilipalveluja. Tämä edellyttää, että identiteetinhallinnan, tunnistautumisen ja tilitietoon liittyvän tietoturvan kysymykset ratkaistaan tiettyyn tasoon saakka yhteisen mekanismin mukaisesti, muutoin MyData-tilin vaihtaminen palveluntarjoajalta toiselle ja yhteentoimivuus ei ole mahdollista. Yhteinen perusta voi kuitenkin olla ohut, mikäli se mahdollistaa tarkemmin määriteltyjen luottamuspalvelujen rakentamisen perustan päälle.

Itsehallittava identiteetti ja lohkoketjuteknologiat

Lohkoketjut ja laajemmin ns. hajautettujen tilikirjojen teknologiat (distributed ledger technologies) ovat olleet viime aikoina erittäin aktiivisia teknologian kehitysalueita. Tunnetuimpia esimerkkejä lohkoketjuteknologioista ovat virtuaalivaluutta Bitcoin ja niin sanottuja ohjelmoitavia älysopimuksia (smart contracts) tukeva Ethereum.

Lohkoketjuteknologialla on toteutettu myös hajautettuja sähköisen identiteetin järjestelmiä, joissa identiteetin omistaja voi hallita omaa digitaalista identiteettiään itsenäisesti ulkoisista identiteetintarjoajista riippumatta. Itsehallittavan identiteetin (self sovereign identity) mallissa luonnollinen henkilö tai organisaatio hallinnoi itse omia tietojaan ja niiden jakamista.

Itsehallittavan identiteetin kehittäjiä ovat muiden muassa Sovrin, uPort, Veres One ja Blockstack. Eri kehittäjien toteutukset poikkeavat toisistaan, mutta yhteistä kaikille on, että luotettavuus itsehallittaviin henkilötietoihin toteutetaan lohkoketjuteknologialla. Henkilötietoja ei talleta lohkoketjuun, vaan lohkoketjua ja krytografisia tunnisteita käytetään siihen, että tiedon vastaanottaja voi varmistaa muuta kautta lähetetyn tiedon paikkansapitävyyden ja voimassaolon.

Itsehallittavan identiteetin malli nähdään keskeisenä teknisenä mahdollistajana tulevaisuuden MyData-infrastruktuurissa, mutta toistaiseksi (kesällä 2018) tarjolla olevat teknologiat eivät ole vielä kypsiä laajamittaisiin toteutuksiin.

Lohkoketjuteknologioihin pohjautuvien hajautettujen identiteettiratkaisujen yhteensopivuutta EU:n tietosuoja-asetuksen kanssa on joissain keskusteluissa kyseenalaistettu, mutta ainakin Sovrin-teknologiaan keskittyneen tutkimuksen (Pitkänen 2018) perusteella näyttäisi siltä, että itsehallittava identiteetti on yhteensopiva myös EU:n yleisen tietosuoja-asetuksen kanssa.

2.3.2 Yksityisyysasetusten, sopimussuhteiden ja käyttölupien hallinta

Taso 2: Käyttölupien hallinta

Liittyy muihin tasoihin: Sopimussuhteiden ja käyttölupien hallintaan pohjautuva henkilötiedon hallinnointi, missä dataa ei tallenneta ja kerätä yhteen paikkaan täydentää henkilökohtaisiin data-alustoihin (2.3.3) pohjautuvaa mallia.

Haasteita: Ei kata identiteettiratkaisuja, minkä johdosta hallinnointipalvelun tarjoajan vaihtaminen ei ole mahdollista.

Teknologioita ja standardikehitystä: UMA 2.0 (User Managed Access), XACML (eXtensible Access Control Markup Language), Kantara Consent Receipt

Referenssejä: MyData-operaattorin referenssiarkkitehtuuri (ks. Infolaatikko aiemmin)

Liittyviä konsepteja: suostumuksen hallinta (consent management), sopimuksiin (ei suostumus) pohjautuva tiedon jakamisen hallinta, toimittaja- ja sopimussuhteiden hallinta, älysopimukset, varmennettavissa oleva loki (tamper proof logging), yksityisyysasetusten etähallinta

Ihmiset kokevat käyttöehtoihin perehtymisen ja yksityisyysasetusten hallinnan työläänä. Jos ihmisten pitää tulevaisuudessa hallita yhä enemmän myös omien tietojensa luovutusta ja käyttölupia, niin yksityisyysasetusten, sopimussuhteiden ja henkilötiedon käyttölupien hallittavuutta on kehitettävä merkittävästi.

Parhaiten tämä toteutuisi, jos palvelujen käyttöehdot ja henkilödatan käyttöselosteet olisivat koneluettavia ja yksityisyysasetuksia voisi muuttaa rajapintojen kautta. Tämä mahdollistaisi ratkaisut, missä käyttäjää ei välttämättä tarvitse rasittaa kaikilla valinnoilla. Sopimisen yhdenmukaistaminen ja hallittavuus lisäisi henkilökohtaisten digitaalisten palvelujen kokonaisuuden ymmärrettävyyttä ja käytettävyyttä.

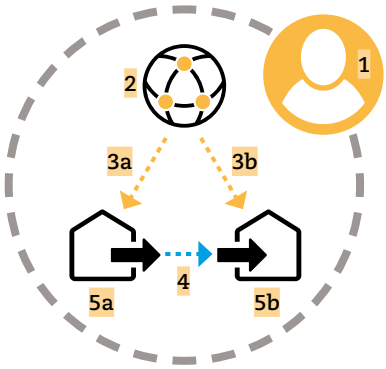
Kehitteillä on standardeja, jotka pyrkivät tarjoamaan yleisesti tunnistettuja ja avoimia tapoja käyttöehtojen ja käyttäjien antamien suostumusten (Kantara 2017) esittämiseen. Puhelinsovellusten yksityisyysasetusten lista on konkreettinen esimerkki siitä, miten henkilötiedon keräämiseen ja käyttöön voidaan muodostaa yhteinen malli, jonka mukaan eri sovellukset toimivat.

Ideaalitapauksessa eri palvelujen yksityisyysasetuksia voisi muuttaa myös rajapintojen kautta etänä kirjautumatta itse palveluun. Käyttäjällä olisi yksi paikka, josta hän voi kerralla määritellä yksityisyyteen ja datan käyttöön liittyvät asetukset useassa käyttämässään palvelussa. Nykyiset palvelut eivät vielä mahdollista yksityisyysasetusten hallintaa rajapintojen kautta, vaan asetukset tehdään kunkin yksittäisen palvelun sisällä. Sujuva palvelujen etähallinta edellyttää yhteisiä käytäntöjä siitä, millaisia yksityisyysasetuksia ja -valintoja eri palveluissa on.

Tyypillisesti yksityisyysasetuksissa voi hallita muun muassa sitä, mitä tietoa palvelu:

- saa käyttöönsä: esimerkiksi mobiililaitteesta sijainti- tai yhteystiedot
- voi näyttää muille käyttäjille: esimerkiksi sosiaalisen median viestien näkyvyys
- voi hyödyntää kaupallisesti: esimerkiksi kohdennettuun markkinointiin
- voi hyödyntää vain reaaliaikaisesti: esimerkiksi sijaintitiedon hyödyntäminen hetkellisesti ilman sijaintihistorian tallentamista
- voi tarjota rajapinnan kautta muille sovelluksille: esimerkiksi sykemittarin tietojen jakaminen ulkopuoliseen liikuntasovellukseen.

Yksi tulevaisuuden malli on, että osan omasta valintojen taakasta voisi siirtää jollekin sovellukselle tai tekoälylle, joka ymmärtää kunkin ihmisen omia mieltymyksiä ja elämäntapoja. Carnegie Mellon -yliopisto on kehittänyt Android-sovelluksen, joka kysyy joukon kysymyksiä siitä, millaisen tiedon jakamiseen käyttäjä on valmis, ja muokkaa sovellusten yksityisyysasetuksia vastaavasti (Goode 2017).



Ihminen 1 hallinnoi **MyData-operaattorin** 2 kautta, mitkä palveluntarjoajat saavat hänen dataansa ja mihin käyttötarkoituksiin. MyData-operaattori mahdollistaa henkilötiedon käyttölupien (consent) digitaalisen hallinnan ja varmentamisen.

Kun **lupa datan luovuttamiseen** 3a ja **hyödyntämiseen** 3b on varmennettu, niin data **voi virrata** 4 **datan lähteiden** 5a ja **dataa käyttävien palveluntarjoajien** 5a välillä suoraan.

Kuva 2.5: Operaattorimallissa ihmiset voivat hallinnoida yksityisyysasetuksiaan, sopimussuhteitaan ja tiedon käyttölupia etänä MyData-operaattorikäytööliittymän kautta.

2.3.3 Henkilökohtaiset data-alustat

Taso 3: Henkilökohtaiset data-alustat

Liittyy muihin tasoihin: Henkilökohtaiset data-alustat täydentävät sopimussuhteiden ja käyttölupien hallintaan (2.3.2) pohjautuvaa mallia.

Haasteita: Kaikkea dataa ei ole mahdollista säilyttää paikallisesti. Ei ole mekanismeja hallinnoida tietoa käsitteleviä organisaatioita (data processors).

Teknologioita ja standardikehitystä: Decentralized Identity Foundation (**http://identity.foundation**) kehittää niin sanottua Identiteetti Hubin (Identity Hub) standardia.

Referenssejä: Cozy Cloud, Digi.me, Meeco

Liittyviä konsepteja: Henkilökohtainen pilvipalvelu (personal cloud), henkilötiedon hallintapalvelu (Personal Information Management Service PIMS)

Vaikka käyttölupien hallinnan avulla tieto voisi, yksilön luvalla, siirtyä suoraan palvelusta toiseen ilman, että sitä tallennetaan välillä, niin on myös monia käyttötapauksia, missä on hyödyllistä, jos ihminen voi tallentaa ja arkistoida tietoa itselleen ja toimia itse sen jakelijana edelleen muille palveluille.

Palveluja tiedon tallentamiseen kutsutaan henkilökohtaisiksi data-alustoiksi (personal data storage PDS). Nämä data-alustat ovat tyypillisesti käyttäjän omassa laitteessa toimivia tai yksilön hallinnassa olevia pilvipalveluja, joissa hänen henkilötietonsa ovat tallennettuna ja erilaiset sovellukset voivat paikallisesti ja hallitusti päästä käsiksi dataan ilman, että dataa tarvitsee siirtää muualle. Tämä malli kääntää tiedon hallinnoinnin organisaatio-keskeisestä ihmiskeskeiseksi.

Mikäli henkilökohtaisessa tietovarastossa on rajapinta, jota kautta sieltä voi jakaa dataa muille sovelluksille, niin tällaista rajapintaa voidaan kutsua omaksi APIksi (API of Me) erotuksena muiden organisaatioiden ylläpitämistä rajapinnoista. Tämä erottelu oman APIn ja muiden henkilötietorajapintojen välillä on merkityksellinen sopimussuhteiden kannalta. Mikäli ihminen esimerkiksi lehtitilausta tehdessään antaa pääsyn omaan kontaktiprofiiliinsa, jota hän ylläpitää omassa tietovarastossaan, on kyseessä kahden välinen transaktio lehtitalon ja tilaajan välillä. Vastaavat osoitetiedot voisivat hypoteettisesti olla tarjolla myös esimerkiksi väestötietojärjestelmästä ja tilaaja voisi antaa lehtitalolle luvan niiden käyttöön. Tällöin kyseessä olisi kuitenkin kolmen keskinen transaktio, jossa osapuolina olisi lehtitalon ja tilaajan lisäksi myös väestötietojärjestelmän ylläpitäjä. Lehtitalolle varmasti kelpaa ihmisen itse ylläpitämä kontaktitieto, mutta joissain tapauksissa tiedon käyttäjä saattaa edellyttää virallisen rekisteristä löytyvän osoitetiedon käyttämistä.

Henkilökohtaisten alustojen ominaisuuksia:

- Alustalle voi kerätä ja tallentaa omat tiedot eri lähteistä ja rajapinnoista.
- Varastossa voi olla oma API (API of Me), jonka kautta ihminen voi jakaa sovelluksille pääsyn joihinkin osiin omista tiedoistaan.
- Varaston yhteyteen voi asentaa ja siellä voi käyttää sovelluksia (vrt. appsit puhelimessa) datan muokkaamiseen, kuvaamiseen ja analysointiin.
- Varaston yhteydessä toimivat sovellukset voivat jalostaa dataa ja tuottaa esimerkiksi profilointeja ilman raakadatan eteenpäin luovutusta.
- Varasto voi sijaita omassa laitteessa (puhelin, tietokone tai erityinen tarkoitusta varten tehty laite) tai palveluntarjoajan tarjoamassa ns. henkilökohtaisessa pilvessä (personal cloud).
- Varasto voi olla kryptattu, jolloin tallennuspalvelun tuottajalla ei ole pääsyä informaatiosisältöön.

Paikalliset sovellukset

Paikallisilla sovelluksilla[5] tarkoitetaan ohjelmia, jotka eivät lähetä käyttäjän dataa eteenpäin toiselle verkkopalvelimelle vaan toimivat siten, että sovellus tai dataa käsittelevä koodi ladataan verkosta datan luo. Paikalliset sovellukset voivat toimia esimerkiksi käyttäjän päätelaitteella tai henkilökohtaisessa pilvessä olevan oman tietovaraston yhteydessä. Esimerkiksi ranskalainen Cozy Cloud[6] tarjoaa avoimen lähdekoodin alustaa henkilökohtaisen pilvipalvelun toteuttamiseen ja tämä alusta mahdollistaa erilaisten paikallisten sovellusten käyttämisen.

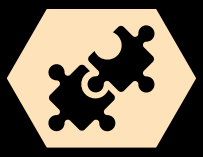
Paikallisten sovellusten toimintalogiikka on käänteinen verrattuna sovelluksiin, joiden luo data lähetetään. Paikallista sovellusta käytetään selaimella tai mobiililaitteella kuten mitä tahansa muuta sovellusta, eikä käyttökokemus eroa perinteisistä verkkopalvelimilla toimivista palveluista. Päätelaitteiden ja selaimien ominaisuudet ovat kehittyneet niin paljon, että moni toiminnallisuus, jonka toteuttaminen aiemmin oli mahdollista vain palvelimella, voidaan nykyisin tehdä päätelaitteessa.

Yksityisyydensuojan kannalta on merkittävästi parempi yhdistellä ja analysoida tietoja paikallisesti, kuin lähettää laajat henkilötiedot piilaakson startupien pilvipalveluihin. Myös silloin, kun datan määrä on suuri, niin on käytännöllisempää tuoda ohjelmakoodi datan luokse.

5 Unhosted https://unhosted.org
6 https://cozy.io

2.3.4 Henkilötiedon tietomallit ja semanttinen standardointi

Taso 4: Tietomallit



Liittyy muihin tasoihin: Henkilötiedon tietomallit tarjoavat yhteiset datan standardoinnin viitekehyksen sopimussuhteiden ja käyttölupien hallintaan (2.3.2) sekä identiteettiattribuuttien välittämiseen identiteetti- ja luottamusverkostoissa (2.3.1).

Haasteita: Yhteisten tietomallien sopiminen ja levittäminen laajamittaisesti käyttöön on hidasta.

Teknologioita ja standardikehitystä: W3C:n ylläpitämät RDF (Resource Description Framework), OWL (Web Ontology Language) ja myös JSON-LD (Javascript Object Notation for Linked Data). Lohkoketjuteknologiat standardoitujen skeemojen jakamiseen

Referenssejä: HL7, Mobile Connect -profiilit

Liittyviä konsepteja: data-ontologiat, profiilit, rooliprofiilit, identiteettiattribuutit

Semanttisella standardoinnilla tarkoitetaan tietosisällön merkitysten kuvaamista niin, että eri lähteistä tuleva samaa asiaa koskeva tieto on yhdistettävissä ja ymmärrettävissä helposti. Usein käytettyjen henkilötiedon tyyppien semanttinen yhtenäistäminen on tärkeää sekä loppukäyttäjien että tietojärjestelemien kehittäjien kannalta. Se tukee tiedon siirrettävyyttä eri palvelujen välillä ja luo pohjan käyttäjien kannalta ymmärrettävälle henkilötiedon hallinnalle.

Henkilötiedon ihmiskeskeinen hallinta ei voi toteutua, jos kaikki organisaatiot kysyvät samoja tietoja, kuten vaikkapa yhteystietoja hieman eri muodossa. Jos jokaisella palvelulla on hieman toisistaan eroavat tietomallit ja käsitteet, niin organisaatiorajat ylittävän tiedon jakamisen ja siihen liittyvä tiedon käyttölupien hallinnan toteuttaminen on kömpelöä ja kallista.

Yhteisten tietomallien kehittäminen ja kansainvälisesti laajaan käyttöön saaminen on hidasta. MyData-ekosysteemin kannalta on tärkeää tunnistaa yläkategoriat, joissa yhteiset tietomallit ovat kaikkein tärkeimpiä. Jos voidaan kuvata keskeiset tietomallit muutamille hyvin tunnistetuille yläkategorioille, niin silloin tiedon hallinnan käyttöliittymiä ja yhteisiä toimintamalleja esimerkiksi datan löydettävyyteen ja käyttölupien hallintaan voidaan tehokkaasti kehittää juuri näiden tietomallien ympärille. Palvelut voivat ilmoittaa selkeämmin omat tietotarpeensa ja käsittelyn perusteensa standardeihin tietomalleihin nojautuen.

MyDatan kannalta keskeisiä henkilötiedon yläkategorioita:

- Vahvistettavissa olevat identiteetti-attribuutit ja muut suhteellisen staattiset identiteettiin liittyvät tiedot kuten täysi-ikäisyys, opintosuoritukset, kansalaisuus jne.
- Jatkuvat aikasarjat kuten osto- ja maksutapahtumat, palvelujen käyttö ja verkkojalanjälki, fysiologiset aikasarjat, sijaintitietovirta, kalenteritapahtumat jne.
- Tiedon hallintaan liittyvät lokitiedot kuten luvitustapahtumat, käyttölupien perumiset, sopimukset jne.
- Monikäyttöiset profiilit kuten kontaktiprofiili (yhteystiedot), preferenssiprofiili (kiinnostustiedot) ja sovellusalakohtaiset profiilit (esim. esteettömyys-, sijainti- ja terveysprofiili)

Standardointi eri alueilla tapahtuu erilaisten prosessien kautta. On olemassa toimialakohtaisia organisaatioita, jotka edistävät standardointia, ja toisissa tapauksissa standardointi tapahtuu de facto -prosessin kautta. Usean erilaisen ja samaan aihepiiriin liittyvän semanttisen standardin tukeminen ei ole tavoiteltavaa, mutta joissain tapauksissa välttämätöntä. Tulevaisuudessa koneoppimista voitaneen hyödyntää semanttisen yhteentoimivuuden luomiseen eri toimijoiden välille. Edellytys tälle on tietomäärittelyjen (keskenään yhteensopimattomienkin) tarjoaminen avoimesti esimerkiksi Open API -dokumentaatioformaatissa.

Customer Commons – yhdenmukainen malli käyttöehtoihin

Jotta palvelujen käyttäjien olisi helppo ymmärtää henkilötiedon jakamiseen liittyviä ehtoja, niiden pitäisi olla mahdollisimman selkeät ja rakenteeltaan yhtenäiset eri palveluissa. Nykyisin palvelujen ehdot poikkeavat toisistaan rakenteellisesti, joten niitä on mahdotonta esittää yksinkertaisina valintoina tai visualisointeina. Jatkossa voisimme kehittää yhtenäisiä standardeja rakenteisessa muodossa julkaistaville käyttöehdoille.

Customercommons.org -projekti pyrkii yhdenmukaistamaan ja yksinkertaistamaan kuluttajien ja yritysten väliset sopimusmallit vastaavalla tavalla kuin Creative Commons yksinkertaisti teosten ja julkaisujen lisensoinnin. Creative Commons -lisenssiä valitessaan tekijänoikeuksien haltijan tarvitsee vastata vain muutamaan kysymykseen, kuten saavatko muut muokata sisältöä tai käyttää ja levittää sitä kaupallisesti. Henkilötiedon käyttöehdoissa voitaisiin kysyä esimerkiksi, saako dataa myydä tai luovuttaa eteenpäin, miten kauan dataa säilytetään jne. Vakiomuotoiset käyttöehdot voitaisiin visualisoida vaihtoehtoja kuvaavilla ikoneilla. Suomessa Digital Health Revolution -hanke on luonut “Consent Commons” -kuvakkeet keinoksi selkeyttää tiedon jakamiseen liittyviä lupia ja sopimuksia ihmisille. Toistaiseksi mikään joukko kuvakkeita ei ole tarttunut laajempaan käyttöön.

Kuva 2.6: Digital Health Revolution -hankkeessa luodut “Consent Commons” -kuvakkeet, joilla kuvataantietosuoja-asetuksesta löytyviä kuutta lainmukaista henkilötiedon käsittelyperustetta, sekä neljää tyypillistä henkilötiedon käyttötarkoitusta. Kuvakkeiden avulla tiedon jakamiseen liittyvät luvat ja sopimukset voidaan visualisoida käyttöliittymissä.

Avoimet standardit ja yhteentoimivuus

Datasta saatavien hyötyjen toteutuminen vaatii avoimia kansainvälisiä standardeja, joita useat toimijat tukevat. Standardien välillä vallitsee jatkuva kilpailu. Esimerkiksi yritykset pyrkivät edistämään omia tai itselleen edullisia standardeja.

MyDatan suunnittelussa on olennaista, että toiminnan ytimessä olevat standardit ovat selkeitä ja yksinkertaisia ja että niiden kehitystyö ja käyttö on avointa ja maksutonta. On hyvä ymmärtää standardien kehityksen tila ja tehdä olemassa olevia standardeja silloittavia kokeiluja, joiden avulla selviävät eri standardien mahdollisuudet ja yhteensopivuuden ydinongelmat. Uusien standardien kehityksessä on pyrittävä laajennettavuuteen, jotta vältytään tilanteelta, jossa vanhanaikainen ja jäykkä standardi estää innovaation.

Yhteentoimivuudesta puhuttaessa usein keskitytään ensisijaisesti tietomallien harmonisointiin niin, että eri järjestelmät pystyvät käsittelemään ja ymmärtämään tietosisältöä samalla tavalla. Toinen keskeinen näkökulma on järjestelmien välinen yhteentoimivuus tiedonsiirrossa niin, että data ylipäätään saadaan siirtymään paikasta toiseen. Mitä sujuvampaa on henkilötietojen siirtäminen ja jakaminen, sitä suurempi merkitys tulee olemaan myös uudelleenkäyttöä helpottavilla yleisillä tietomalleilla.

Tiedon rakenteen pitää olla riittävän kattavasti ja selkeästi kuvattu, jotta esimerkiksi eri lähteistä saatavat aikasarjat voidaan vaivattomasti yhdistää toisiinsa. Toinen edellytys yhteentoimivuudelle on, että datan mukana siirtyvät myös kuvailutiedot siitä, mitä datassa olevat eri käsitteet merkitsevät. Esimerkiksi käsite “palkka” voi järjestelmästä riippuen tarkoittaa bruttopalkkaa, nettopalkkaa tai jotakin muuta.

Nykyisin organisaatioiden käyttämät henkilötiedon tietomallit on suunniteltu suurelta osin niiden omien tarpeiden ympärille. Tietomallit eivät ole yhtenäisiä kilpailijoiden saatikka muiden toimialojen organisaatioiden kanssa. Tarvelähtöisesti organisaatiot siirtyvät käyttämään standardeja itse kehittämiensä tietomallien sijaan. Tämä voi hyödyttää organisaatiota tulevien tietojärjestelmien määrittelyssä ja toteuttamisessa.

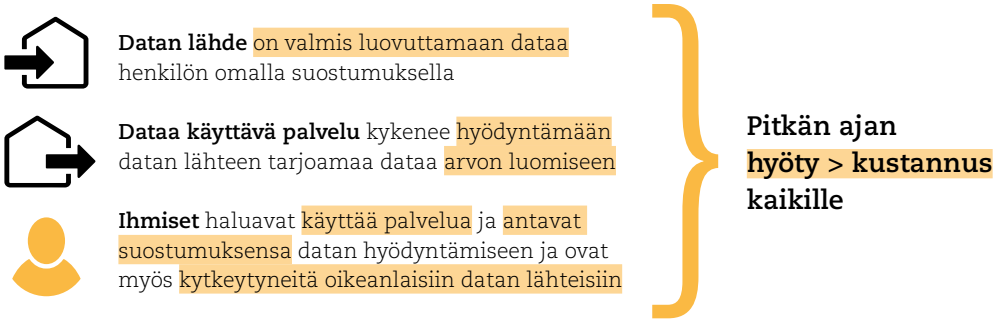
Markkinat toimivat, jos datan lähteillä, dataa hyödyntävillä palveluilla, ihmisillä itsellään ja infrastruktuurin tarjoajilla on kullakin pitkässä juoksussa omia kustannuksiaan suuremmat hyödyt.

3. Esimerkkejä MyDatan sovellusalueista

MyDatan toteuttaminen ja ylläpito vaatii investointeja ja muuttaa henkilötiedon hyödyntämiseen liittyvää liiketoimintaa. Kuka maksaa kustannukset ja kenelle menevät hyödyt? Ovatko ihmiset oikeasti kiinnostuneita MyData-palveluista?

Kypsän MyData-markkinan kokonaishyödyt on melko laajasti tunnistettu ja tunnustettu. Esimerkiksi päällekkäisen tiedonkeruun vähentyminen, saumattomasti toimivien digitaalisten palvelujen syntyminen, avoin kilpailuympäristö ja ihmisten vahvempi oikeudellinen asema kannustavat MyDatan kehittämiseen organisaatioissa ympäri maailmaa.

Puolikkaalla MyDatalla ei kuitenkaan saa puolta hyödyistä. Markkinat toimivat, jos datan lähteillä, dataa hyödyntävillä palveluilla, ihmisillä itsellään ja infrastruktuurin tarjoajilla on kullakin pitkässä juoksussa omia kustannuksiaan suuremmat hyödyt. Mikäli jokin osapuoli ei ole mukana, ei data liiku eikä kukaan hyödy. Jos kannustimet saadaan kohdalleen ja ekosysteemi syntyy, niin verkostovaikutukset voivat kiihdyttää sen kasvua nopeastikin.



Kuva 3.1: Elinvoimaisessa MyData-käyttötapauksessa kaikki osapuolet saavat enemmän hyötyjä, kuin niille koituu kustannuksia pitkässä juoksussa. Vaikka käyttötapauksen kokonaishyödyt olisivat kokonaiskustannuksia suuremmat, niin se ei vielä riitä, mikäli hyödyt ja kustannukset jakautuvat niin, ettei mukaan lähteminen ole kaikille osapuolille kannattavaa. MyData-operaattorien verkosto voi toimia arvon välittämisen verkostona ja jakaa hyötyjä esimerkiksi, niin, että datan lähteille korvataan niille syntyvät kustannukset.

Kustannukset ja hyödyt eivät luonnostaan jakaudu tasaisesti eri roolien ja toimijoiden kesken. Vahva oletus on, että henkilötiedolle ylipäätään on kysyntää, eli henkilötietoa hyödyntäviä palveluja on ja syntyisi lisääkin, jos dataa olisi vaivattomammin saatavilla. Sen sijaan datan lähteille MyDataan siirtyminen voi merkitä kustannuksia ja riskejä. Esimerkiksi julkisen rekisterin sisältämä tieto voi olla erittäin kysyttyä, mikä vaatisi panostuksia tietovarantojen laadun ja rajapintojen ylläpitoon, mutta kyseinen virasto ei välttämättä merkittävästi hyötyisi henkilötietojen tarjoamisesta MyDatana tai saattaisi jopa menettää datasta saamiaan myyntituloja.

Esitetty MyData-infrastruktuuri on paitsi datan välittämisen, niin myös arvon tuotannon ja arvon välittämisen verkosto. MyData-operaattorit voisivat ylläpitää datan välittämiseen liittyviä älysopimuksia, joilla hyötyjä ja kustannuksia verkostossa voidaan tasata automaattisesti. Esimerkiksi jos datan hyödyntäjä maksaa datasta, niin verkoston kautta tulot voitaisiin jyvittää MyData-operaattorien ja rajapintaa ylläpitävän datan lähteen kesken. Näitä operaattoriverkoston maksumalleja ei vielä ole kokeiltu MyDatassa, mutta muista verkostoista kuten vaikkapa pankki- ja telealalta voidaan ottaa mallia.

Ihmisille MyData lupaa muun muassa parempaa käyttökokemusta digitaalisissa palveluissa. Samoja tietoja ei tarvitse syöttää ja päivittää moneen paikkaan, palvelut ovat automaattisempia ja yksilöidympiä jne. Tämä riippuu toteutuksien käytettävyydestä. Ei ole vaikea kuvitella päinvastaista skenaariota, missä MyData ei toisi helppoutta, vaan vaatisi ihmisiltä nykyistä enemmän ajankäyttöä ja viitseliäisyyttä oman datansa hallinnoinnissa. Operaattoriverkoston maksumallien pitäisi myös toimia kannustimena datan hallinnan käytettävyyden kehittämiseen. Operaattorit, joilla on helpot palvelut, saavat asiakkaita ja suuremman markkinaosuuden. Edellytyksenä tietenkin on, että operaattorin vaihtaminen itsessään on riittävän vaivatonta, eikä siitä tule kilpailun estettä.

Kuva 3.2: Tyypillisiä tarpeita, joita henkilötiedon ekosysteemissä eri rooleissa olevilla toimijoilla voi olla.

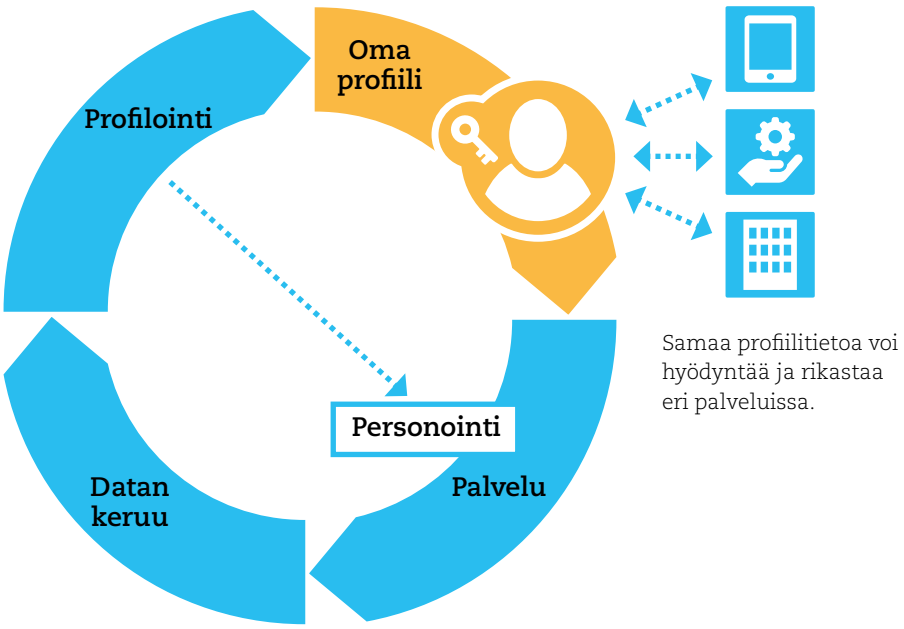
Seuraavaksi kuusi esimerkkiä tavoista, joilla MyData voi muuttaa käyttäjien, datan tuottajien ja palveluntarjoajien välisiä suhteita ja tarjota hyötyjä eri osapuolille. Esimerkit on valittu ajatuksen herättelijöiksi MyDatan erilaisista hyödyntämismahdollisuuksista.

3.1 Itse kootut profiilit: Siirrettävä mediaprofiili

Heikosti kohdennetut suositukset ja verkkomainokset ovat arkipäivää, mutta joskus suositukset osuvat hämmästyttävän hyvin. Sama hyvin osuva suositus voi olla asiakkaan näkökulmasta loistavaa digitaalista palvelua tai sitten se voi olla luottamusta heikentävää pelottavaa seurantaa. Tätä kutsutaan niin sanotuksi puistattava-siisti-rajaksi (creepy-cool line). Kummalle puolelle rajaa profiloinnin pohjalta tehty palvelu sijoittuu riippuu siitä, onko asiakkaalle ymmärrettävää, mihin suositus perustuu ja miten yritys tietää hänestä niin paljon.

Ihmisten itse hallinnoimat profiilit mahdollistaisivat tarkempia suosittelujärjestelmiä ja läpinäkyvyys lisäisi luottamusta yrityksiä kohtaan. MyData-profiilit voivat olla yhden yrityksen tuottamia profiileja monipuolisempia ja kuvaavampia, koska niihin voidaan yhdistää tietoa eri lähteistä. MyDatan myötä ihminen voisi myös käyttää samoja rikkaampia profiilitietoja eri palveluissa sen sijaan, että jokainen palvelu tekisi erillisen profiloinnin hänestä asiakkaana.

Esimerkiksi siirrettävä mediaprofiili mahdollistaisi omien mediamieltymysten välittämisen ja hyödyntämisen useissa palveluissa. Parhaimmillaan käyttäjä voisi esimerkiksi jatkaa yhdessä mediapalvelussa kesken jääneen ohjelman katselua samasta kohdasta toisessa palvelussa ja näiden molempien palvelujen kerryttämä tieto rikastaisi samaa mediaprofiilia, jonka avulla molemmat palvelut voisivat tarjota jatkossa paremmin sopivia suosituksia. Vastaavasti liikkumisprofiili voisi olla jaettu niin sanottujen liikkuminen palveluna (Mobility as a Service, MaaS) -tarjoajien kanssa ja terveysprofiili helpottaisi vuorovaikutusta erilaisten terveyden ja hyvinvoinnin palveluntarjoajien kanssa. Muita mahdollisia omia profiileja olisivat esimerkiksi kontaktiprofiili ja yksityisyysasetusten profiili.

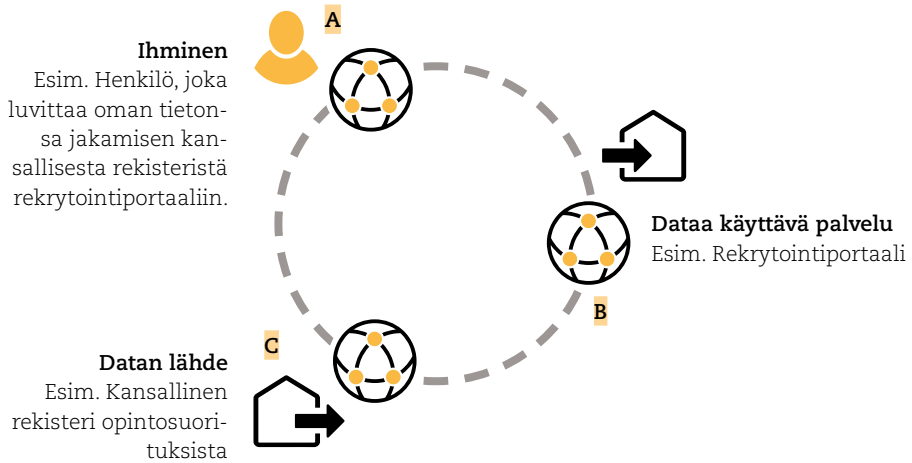


Kuva 3.3: Perinteisesti käyttäjädatan keruuseen ja analysointiin pohjautuva profilointi ja palvelun personointi tapahtuvat yksittäisen palvelun sisällä (siniset nuolet), eikä kertynyttä profiilitietoa voi tällöin hyödyntää muualla, eikä toisaalta profiilin muodostamiseen ole käytettävissä muissa palveluissa syntynyttä käyttäjädataa. MyData-mallin mukainen ihmisen itse hallitsema profiilitieto (oranssi) mahdollistaisi tiedon koostamisen useista lähteistä ja saman profiilin hyödyntämisen eri palveluissa.

3.2 Varmennettu tieto: CV 2.0

MyData antaa ihmisille mahdollisuuden päästä käsiksi omiin tietoihinsa ja käyttää niitä toisaalla alkuperäisestä datan tuottajasta riippumatta. Tämä lisää joustavuutta, kun dataa hyödyntävien palvelujen ei tarvitse olla suorassa yhteydessä tai sopimussuhteessa datan lähteiden kanssa. Monissa käyttötapauksissa pelkästään tiedon joustava siirtyminen ei riitä, vaan on tarpeen myös varmistaa tiedon alkuperä ja oikeellisuus. Tällainen tiedon sertifiointi on mahdollista sähköisten allekirjoitusten avulla.

Esimerkiksi tulevaisuuden rekrytointipalvelut ja työnantajien henkilöstöhallinnon palvelut voisivat toimia ihmisten MyDatana välittämien osaamisprofiilien avulla. Osaamisprofiilia on luontevaa ajatella uudenlaisena digitaalisena CV:nä, jossa oma osaaminen on paitsi kuvattu koneluettavassa muodossa, niin myös opinto- ja tutkintotiedot sekä muut pätevyydet olisi mahdollista tarvittaessa varmistaa sähköisesti. Esimerkiksi rekrytointipalvelu voisi vahvistaa, että tieto suoritetusta tutkinnosta todella on peräisin oppilaitosten rekistereistä eikä sitä ole peukaloitu. Opintohistorian ja tutkintotietojen lisäksi myös vaikkapa ajokortti, kielitodistukset, hygieniapassit, tulityöluvat, erilaiset kurssit ja vastaavat olisi mahdollista varmistaa sähköisesti, jos siihen soveltuva MyData-infrastruktuuri on tietoa tuottaville organisaatioille riittävän helppo ottaa käyttöön.

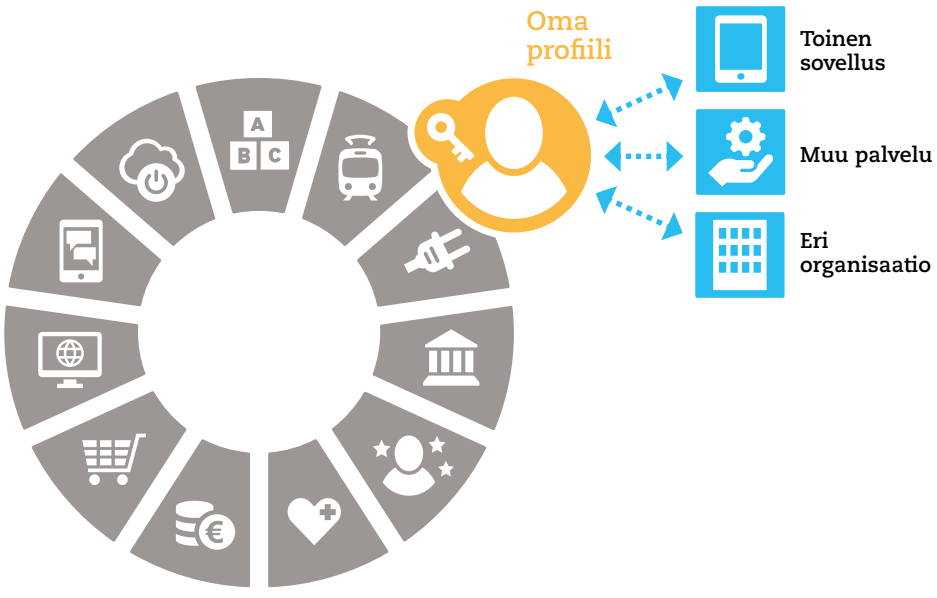


Kuva 3.4: Esimerkkitapauksessa työnhakija [**A**] täydentää osaamisprofiiliaan (esimerkiksi CV-tiedot) rekrytointiportaalissa [**B**], johon on mahdollisuus tuoda koneluettavassa muodossa kansallisesta rekisteristä [**C**] varmennettu tieto omasta opintohistoriasta. Keskitetyn alustaratkaisun sijaan verkostomaisen MyData-mallin mukaisesti tämän voisi toteuttaa niin, että sekä datan lähde, dataa käyttävä palvelu että ihminen itse kytkeytyvät verkostoon eri palveluntarjoajien kautta.

3.3 Käyttäjätietojen hajautettu hyödyntäminen: Tiedot kanta-asiakaskortilta

Neljällä viidestä suomalaisesta kotitaloudesta on kanta-asiakaskortti. Ihmiset hyötyvät niiden käytöstä ennen kaikkea bonusten ja alennusten muodossa, mutta mahdollisesti myös osuvampien palvelujen muodossa. Kauppaketjut, kuten monet muutkin palvelut, käyttävät keräämäänsä tietoa logistiikan optimoinnissa, tarjonnan kohdentamisessa ja markkinoinnissa. Kauppaketjut kehittävät uutta sähköistä palveluntarjontaa, joka nojaa myös ostostietoihin, mutta samalla ne toimivat portinvartijoina sen suhteen, kuka voi hyödyntää niiden keräämää tietoa. Kanta-asiakasohjelmien tieto on käytettävissä vain yritysten omissa palveluissa.

MyDataan kuuluu ajatus palveluketjujen hajautumisesta, missä eri toimijat erikoistuvat palveluketjun eri osiin. Mikäli ihmiset voisivat helposti siirtää omat ostotietonsa kanta-asiakasjärjestelmistä muidenkin sovellusten käyttöön, mahdollistaisi se nykyistä ketterämpää palvelukehitystä. Joku yritys voisi esimerkiksi luoda sovelluksia, jotka opastavat allergioista tai kroonisista sairauksista kärsiviä asiakasryhmiä heidän ruokaostoksissaan ja toinen yritys voisi koota asiakkaan ostodataa laajasti henkilökohtaisen taloushallinnan näkymiin. Näiden yksityiskohtaisten asiakastarpeiden palveleminen ei välttämättä ole kauppaketjun kanta-asiakasohjelman prioriteeteissa kovin korkealla, mutta näiden palvelujen toteutuminen lisäisi kuitenkin kanta-asiakaskortin hyödyllisyyttä asiakkaille ja olisi siten myös kauppaketjun edun mukaista.



Kuva 3.5: Käyttäjän suostumuksella yritykset voivat saada käyttäjästä rikasta profiilitietoa, jonka pohjalta ja vastineeksi yritys pystyy tuottamaan käyttäjälle parempaa palvelua ja palveluun liittyvää viestintää.

Yritysten ja asiakkaiden tieto toisistaan

Asiakastiedon hallinta on osa yritystoimintaa. Yritysasiakkaiden tiedot ovat yleensä jollain tavoin hallittavissa ja asiakastietoa voi ostaa muun muassa hakemistoyrityksistä. Mitä pienemmistä ja monilukuisemmista asiakkaista asiakaskunta koostuu, sitä haastavampaa on asiakastiedon hallinta. Kuluttajakaupassa ajantasaisen asiakasrekisterin ylläpito lähestyy jo mahdottomuutta. Monet yritykset haluaisivat ehkä päästä eroon oman asiakasrekisterin jatkuvasta ylläpidosta. Niille riittäisi, että asiakaskontaktin syntyessä ne saisivat ajantasaiset tiedot suoraan sähköisesti asiakkaalta omaan järjestelmäänsä tai jopa niin, ettei asiakastietoa edes tallennettaisi, sitä vain käytettäisi sillä hetkellä, kun sitä tarvitaan.

Kuten nykyisin kuluttajasta on tietoja useiden yritysten asiakastietojärjestelmissä (Customer relationship management CRM), niin vastaavasti ihmisellä itsellään voisi olla työkalut omien yrityskontaktien hallintaan aina autokorjaamoista parturikampaamoihin (Vendor Relationship Management VRM). Tällainen oma tavaroiden ja palvelujen toimittajarekisteri voisi sisältää sopimuksia, takuukuitteja ja historian yhteydenpidosta kunkin yrityksen kanssa. Esimerkiksi kun ihminen muuttaa asunnosta toiseen, hän voisi jakaa automaattisesti uudet yhteystiedot kerralla kaikille niille yrityksille, joiden kanssa haluaa jatkaa yhteydenpitoa. Asiakkaiden hallitsema VRM ja yrityksen CRM-järjestelmä voisivat täydentää toisiaan ja vaihtaa tietoa tarpeen mukaan.

Omassa hallinnassa olevan asiakasprofiilin ja toimittajarekisterin avulla kuluttaja-asiakkaatkin voivat nykyistä helpommin kilpailuttaa yrityksiä. Sen sijaan, että asiakas käyttää aikaa parhaiden tarjousten metsästämiseen, hän voikin ilmaista aikomuksensa liittämällä julkiseen profiiliinsa ostotarjouksen. Nykyisin asiakkaan ostotarjouksiin pohjautuvia järjestelmiä on joillain yksittäisillä toimialoilla. Esimerkiksi **tilausajot.net**-palvelussa asiakas täyttää tiedot tarvitsemansa kyydin ajankohdasta ja reitistä, ja saa sen jälkeen kuljetusyrityksiltä tarjouksia sähköpostiinsa. Tällaista käänteistä mallia kutsutaan nimellä aikomustalous (Searls 2012).

3.4 Yhteiskunnallinen tiedonkeruu: MyData tutkimuskäytössä

Yhteiskunnallisesti merkittävä tutkimus edellyttää usein tietojen keräämistä suuresta joukosta ihmisiä ja usein myös useammasta tietolähteestä. Suomen lainsäädäntö on verrattain salliva sen suhteen että julkisia rekistereitä on saatavilla tutkimuskäyttöön. Keinot tiedon hankkimiseen ovat kuitenkin tarkkaan säädeltyjä. Tutkimukselle hyödyllisiä tietovarantoja, kuten esimerkiksi teleoperaattorien tietoja ihmisten liikkeistä ja sijainneista, kertyy myös yksityisen sektorin pitämiin rekistereihin. Tulevaisuudessa tutkimus ja muu yhteisten ongelmien ratkaiseminen vaatii uudenlaisia keinoja tiedonkeruuseen.

Näihin keinoihin kuuluu myös ihmisten osallistuminen niin, että he antavat suostumuksensa tietojensa käyttöön tai vaikuttavat tiedon käyttöön liittyviin yhteisiin päätöksiin. Esimerkiksi suomalainen Biopankki[7] kokoaa näytteitä ja tietoja ihmisten antamien lupien pohjalta terveystutkimukseen. Tietoa välittäviin organisaatioihin voi myös liittyä useita erilaisia tapoja jakaa tutkimuksen kautta syntyvää arvoa. Esimerkiksi sveitsiläinen Midata.Coop[8] on osuuskunta, jonka jäsenet yhdessä päättävät datan jakamisesta syntyvien tulojen käytöstä esimerkiksi lisätutkimukseen tai koulutukseen.

Kuva 3.6: Suomalaisten biopankkitoimijoiden kanssa tehty biopankkiluovuttajan MyData-kuvaus. Esimerkissä ihmiset ovat aktiivisia biopankkinäytteen luovuttajia ja henkilökohtainen terveystili toimii tiedon hallinnan alustana ja mahdollistaa analysoidun tiedon palauttamisen luovuttajalle. (Kuva: Digital Health Revolution **digitalhealthrevolution.fi**)

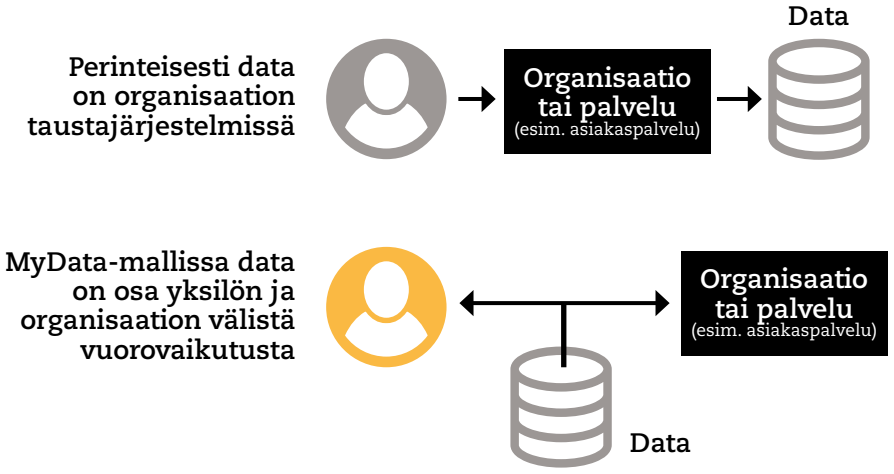
7 http://www.biopankki.fi
8 https://midata.coop

3.5 Data osaksi vuorovaikutusta: Julkisten palvelujen läpinäkyvyys

Ihmisten omaa dataa hyödyntämällä palveluja voidaan automatisoida ja tarjota oikeaan aikaan niitä tarvitseville. Palveluja automatisoitaessa on tärkeää tehdä niistä läpinäkyviä. Käyttäjillä pitää olla tehokkaat keinot korjata mahdollisia taustatiedoissa olevia virheitä tai puutteita, jotka voisivat johtaa automatisoidussa prosessissa vääriin johtopäätöksiin.

Perinteisesti data on organisaatioiden taustajärjestelmissä, jonka vuoksi asiakkaan ja asiakaspalvelijan näkymät tietoihin poikkeavat toisistaan. Tiedon määrän ja näkyvyyden epäsymmetrisyyden takia asiakkaan voi olla hankala ymmärtää häntä koskevia päätöksiä ja niiden perusteita (esim. pankin lainapäätös). MyData-lähestymisessä data on osa henkilön ja organisaation välistä vuorovaikutusta. Ihmisellä on yhtäläinen pääsy häntä koskeviin tietoihin kuin organisaatiollakin. Tällöin ihmiset voisivat helposti tarkistaa tietojensa oikeellisuuden, mutta myös MyData-periaatteiden mukaan siirtää omat tiedot muihin sovelluksiin. Julkisten palvelujen tapauksessa kansalaisella voisi olla sama näkymä tietoihin kuin heistä päätöksiä tekevällä virastolla. Opintotukea hakeva voisi esimerkiksi suoraan viraston verkkopalvelusta nähdä, mihin tulotietoihin nykyinen opintotukipäätös perustuu ja kuinka lisätienestit vaikuttaisivat tilanteeseen.

Yksi MyDatan hyödyntämismahdollisuus on niin sanottu proaktiivinen palvelutarjonta, jossa henkilödataa hyödyntämällä palveluja kohdennetaan, muutetaan ennakoivammiksi ja automatisoidaan. Palvelun tuottajan näkökulmasta proaktiivisella palvelutarjonnalla voidaan lisätä asiakastyytyväisyyttä ja tehostaa prosesseja muun muassa tasaamalla ruuhkahuippuja. Siirtyminen veroilmoituksista verottajan automaattisesti tuottamiin veroehdotuksiin on hyvä esimerkki proaktiivisesta palvelutarjonnasta. Siinä hyödynnetään verottajan hallussa olevaa ihmisten omaa dataa. Veroehdotus toimintamallina sekä helpottaa ihmisten arkea että tehostaa verottajan toimintaa. Vastaavasti ihmisille, joiden passi on vanhentumassa voitaisiin aktiivisesti tarjota sähköistä palvelua passin uusimiseen. Tämä tasoittaisi lomakausia edeltäviin aikoihin kohdistuvia ruuhkahuippuja passin uusimisissa.



Kuva 3.7: MyData-mallissa henkilötieto on jaettu resurssi ja osa yksilön ja organisaation välistä vuorovaikutusta.

3.6 Esineiden keräämä data: Ovatko autoni tiedot minun?

Dataa ei kerry pelkästään verkkopalveluihin ja matkapuhelinten sovelluksiin. Yhä useammat arjessa käyttämämme laitteet myös tallentavat tietoja, ovat kytkeytyneet internetiin ja viestivät keskenään. Tätä trendiä kutsutaan esineiden internetiksi (Internet of Things tai IoT). IoT-laitteet synnyttävät runsaasti reaaliaikaista dataa, josta osa on luokiteltavissa henkilötiedoksi. Sensorien ja datan virtaan perustuvien toiminnallisuuksien yleistyminen kuluttajatuotteissa nostaa kysymykset datan hallinnoinnista ja käytöstä ajankohtaisiksi. Onko hyväksyttävää, että kerätyt tiedot ovat käytettävissä vain valmistajan alustalla?

Esimerkiksi uudet autot tallentavat ja jakavat runsaasti tietoa ajoneuvon sijainnista ja toiminnasta sekä kuljettajan ajotavasta. Tällä hetkellä tämä tieto on autonvalmistajien hallussa, jotka määrittelevät, kenellä on pääsy tietoon. Rajoituksilla on käytännön merkityksiä muun muassa sen kannalta, kuka pystyy huoltamaan autoa. MyData-periaatteiden toteutuminen ajoneuvojen kohdalla tarkoittaisi, että ihmisille olisi selvää, mitä tietoa ajoneuvo kerää ja mihin tarkoituksiin sitä jaetaan. Kun tieto siirtyisi palveluntarjoajille ihmisten valinnan mukaan, pystyisivät nämä itse valitsemaan, miten huoltavat omaa autoansa.

Dataa useilta henkilöiltä, yrityksiltä ja laitteilta

MyData-ajattelu rajautuu helposti luonnollisiin henkilöihin. Tietoa syntyy ja hyödynnetään kuitenkin yleensä kahden tai useamman tahon vuorovaikutuksessa. Mukana voi olla ihmisiä, organisaatioita ja yhä enemmän myös esineitä ja fyysisiä tiloja. Tällöin samaan tietoon tulee olla pääsy erilaisin oikeuksin useilla eri ihmisillä ja tahoilla. Usein on hankala määritellä vain yhtä henkilöä, jota tieto koskee. Esimerkiksi autoon asennetun anturin data koskee kaikkia auton käyttäjiä. Ostoksia tehdään usein koko perheelle, vaikka maksaja onkin yksi ihminen, ja puhelinliittymän todellinen käyttäjä voi olla joku muu kuin liittymän omistaja.

Jako henkilötietoon ja ei-henkilötietoon ei ole datan teknisen hallinnan kannalta välttämätöntä. Koneille ei ole merkitystä, onko kyseessä henkilötieto vai organisaatiota koskeva ei-henkilötieto. Eroavaisuudet tulevat lainsäädännön vaatimuksista, mutta selkeät mekanismit tiedon luvittamiseen ovat tarpeellisia myös yritysten tietojen hallinnassa, vaikkei laki siihen velvoitakaan.

Organisaatiot voisivat myös hyötyä, mikäli saisivat itseään koskevan datan helposti käytettävässä muodossa. Esimerkiksi taloyhtiöiden on nykyisin hankalaa vaihtaa isännöitsijää, koska taloyhtiöiden data on yleensä isännöitsijätoimistojen tietojärjestelmissä (Ympäristöministeriö 2014). Myös julkishallinnon kanssa asioidessaan, kuten veroilmoitusta täyttäessään, yritykset kerryttävät yritysten omaa dataa, jolla voisi olla paljon hyödyllisiä jatkokäytön mahdollisuuksia.

Identiteetti, johon hallittavat tiedot kytkeytyvät, saattaa siis olla henkilö tai organisaatio, mutta se voisi yhtä hyvin olla esine tai fyysinen tila. Laite voisi esimerkiksi kantaa mukanaan omaa historiaansa ja tietoa esimerkiksi siihen tehdyistä korjauksista. Olisi perusteltua, että pääsy laitteen “omaan” dataan siirtyisi myös omistussuhteiden muutosten mukana.

Yksinkertaistetut tapaukset, joissa on selkeää, että kyseessä on yhden ihmisen henkilötieto, eivät välttämättä varsinkaan tulevaisuudessa ole yleisimpiä. Usean ihmisen yhteisen datan, organisaatioiden datan ja esineiden sekä tilojen datan asettamat vaatimukset datan jakamisen ja hallinnoinnin infrastruktuurille ovat haastavampia, mutta toisaalta yleiskäyttöiset ratkaisut leviävät nopeammin. Selkeyden vuoksi tässä selvityksessä termillä MyData viitataan ensisijaisesti luonnollisten henkilöiden dataan, mutta huomioidaan mahdollisuus, että MyData-infrastruktuurin toteutumisen ajurina saattavat hyvinkin toimia ratkaisut, jotka palvelevat muutakin kuin henkilötiedon jakamista.

4. Uhat, esteet ja hidasteet

Aiemmissa luvuissa on esitetty MyData-malli, sen tavoitteiden kautta. Maailmalla vastaavia visioita on paljon. Ne kaikki jakavat suurelta osin näkemykset siitä, mitä hyötyjä ja tulevaisuuden vaikutuksia systeeminen muutos kohti ihmiskeskeistä henkilötiedon hallintaa toisi tullessaan. Vielä ei kuitenkaan olla tilanteessa, että edes Suomessa saatikka globaalilla tasolla olisi toimiva infrastruktuuri ja markkinat ihmiskeskeiselle henkilötiedon jakamiselle ja hallinnalle.

MyDatan vieminen visioista ja konsepteista todellisuudeksi etenee useiden löyhästi toisiinsa liittyneiden toimijoiden tekemisten tuloksena. Mukana niin Suomessa kuin kansainvälisestikin on alati laajeneva joukko tekijöitä erikokoisista yrityksistä, julkishallinnon organisaatioista, tutkimuslaitoksista, kansalaisjärjestöistä ja muista organisaatioista – kukin omista motiiveistaan. Konseptit ja käytännön teot luovat tulevaisuudenodotuksia ja tuovat kentälle lisää toimijoita, rahoitusta ja sitä myöten lisää toimintaa. Pienet ja isot teot luovat uusia tulevaisuuden odotuksia, jotka ruokkivat edelleen lisää toimintaa. Kehityssykli voi eri syistä myös kuihtua kasaan tai jäädä jonkun toisen voimakkaamman kehityskulun jalkoihin.

Jos kehitys kuitenkin jatkuu, niin ennen pitkää kenttä kypsyy ja tapahtuu lukkiutumista. Esimerkiksi tietyt teknologiastandardit yleistyvät käyttöön, jotkut toimijat saavuttavat merkittävän markkina-aseman, "killer app" näyttää toimivan liiketoimintamallin tai verkoston hallinnointiin syntyy kansainvälisesti hyväksytty toimintamalli ja instituutiot. Lukittumiset vakauttavat toimintaympäristöä ja mahdollistavat MyDatan leviämisen laajasti käyttöön, mutta lukittunutta tilannetta ei voi helposti enää muuttaa. Miten voidaan välttää sellaisia lukittumisia, jotka vesittäisivät MyDatan tavoitteita ja johtaisivat yhteiskunnallisesti negatiivisiin tuloksiin? Tässä luvussa käsitellään hidasteita, jotka voivat pahimmillaan kuihduttaa MyDatan kehityssyklin, sekä uhkakuvia, jotka toteutuessaan tarkoittaisivat sitä, että kehityssykli lukittuu väärään asentoon.

Kuva 4.1: Kansainvälisen MyData-verkoston slogan "make it happen make it right" (toteutetaan se ja tehdään se oikein) kuvaa kehityksen kahta puolta. Yhtäältä pitää huolehtia, että kehityssykli kohti todellista ja toimivaa MyDataa pysyy vauhdissa eikä kuihdu kasaan. Toisaalta pitää ymmärtää, että kehitys voi eri toimijoiden ja toiminnan tuloksena muuttaa suuntaa ja pahimmillaan lukittua joltain osin ei toivottuun tilaan.

4.1 Hidasteet tai esteet

4.1.1 Mitä voimme tehdä nyt heti käytännössä?

Olemme nyt pisteessä 1. Kaikki näkevät, että pisteessä 3., kun kaikki toimii, niin kaikki voittavat, mutta epäselvää on, mitä on ykkösen ja kolmosen välillä. MyData-ajattelu on idealistista ja siksi joillekin myös innostavaa, mutta tekeminen onkin eri juttu. MyData ei vain käytännössä toimi; jos toimisi, niin se olisi jo kehitetty, moneen kertaan koestettu ja laajasti käytössämme.

MyData-kehityksen jatkuminen maailmanlaajuisesti suotuisasti edellyttää, että suuri joukko toisistaan riippumattomia toimijoita näkee MyDatan tulevaisuudenlupaukset riittävän kiinnostavina ja tavoittelemisen arvoisina ja toisaalta myös mahdollisuuksien rajoissa olevana. Mahdottoman tavoittelu ei innosta.

Lupaukset ihmisten digitaalisista oikeuksista ja voimaantumisesta, avoimesta ja kilpailua suosivasta liiketoimintaympäristöstä sekä teknisesti kitkattomasta ja yhteentoimivasta infrastruktuurista ovat laajasti hyväksyttyjä. Ainakaan julkisesti niitä ei vastusteta. Toimintaa kiihdyttävän motivaation lähde tai käänteisesti sen puute kiteytyy monesti siihen, kuinka mahdollisena muutos nähdään.

MyDatasta kiinnostunut digipalvelun kehittäjä kysyy, miten voimme liittyä Mydata-infrastruktuuriin tai operaattori-toiminnasta kiinnostunut kysyy, mikä on operaattorien ansaintamalli. Pettymys on karvas, jos kysyjä olettaa, että olemme jo pisteessä, missä kaikki on valmista. Toiset näkevät tämän kehityshaasteena, johon kannattaa tarttua, ja toiset jäävät passiivisesti odottelemaan tai kääntävät kokonaan selkänsä MyDatalle.

Vaikka epävarmuus polusta ykkösen ja kolmosen välillä väistämättä passivoi osan toimijoista, niin myös liian varhainen “selkeän polun” alleviivaaminen voi olla kehitykselle vaarallista. Esimerkiksi jonkun tietyn teknologiavalinnan, arkkitehtuurimallin tai liiketoimintamallin osoittaminen valittuna MyData-mallina saattaa karkottaa toimijoita, jotka jakavat MyDatan vision, mutta syystä tai toisesta näkevät valitun kehityspolun vääränä. Mahdollisia polkuja on lukemattomia; kyse ei siis ole vain jonkin piilossa olevan yhden totuuden selvittämisestä. Erilaiset esitetyt konseptualisoinnit, toteutetut kokeilut, tekniset arkkitehtuurit ja yrityskentässä kypsyvät liiketoimintamallit ovat mahdollisia polkuja tai polun osia. Kaikkia ei saa eikä voi pakottaa yhteen ajattelutapaan, vaan eri tekniikoita ja liiketoimintamalleja pitää kokeilla ja kehittää rinnakkain.

4.1.2 Data on keino pitää asiakas

MyData-rajapintojen avaamisesta ei ole edelläkävijöille etua.

Yritys tai palvelu, joka on onnistunut pitämään asiakkaan pitkään, on voinut myös kerryttää ison datahistorian. Esimerkiksi vuosikausia kestäneen pankkiasiakkuuden myötä pankin järjestelmiin on kertynyt henkilön tilitapahtumien historia koko tältä ajalta, mikä on arvokasta tietoa mm. luottopäätöstä tehtäessä. Monessa tapauksessa data ja historia myös sitovat henkilöä kyseisen palvelun käyttäjäksi. Esimerkiksi Facebookista irtautuminen olisi kivuliasta vaikka markkinoille tulisi parempi palvelu, koska Facebookissa on tuttavaverkostoja, viestintähistoriaa, valokuvia yms. jo pitkältä ajalta.

Asiakkaiden kannalta helppo mahdollisuus vaihtaa palvelua tuntuu luonnolliselta ja oikeutetulta, mutta yrityksen näkökulmasta liiketoimintariski voi kasvaa suureksi, jos kuka tahansa uusi tulokas markkinoilla voi kaapata koko asiakaskunnan datoineen hetkessä.

Markkinatilanne, jossa suurin osa yrityksistä toimisi MyData-periaatteiden mukaisesti, ohjaisi todennäköisesti loputkin yritykset ja uudet tulokkaat toimimaan samalla periaatteella. Ihmiset eivät valitsisi yritystä, joka haluaa lukita asiakkaan ja hänen datansa. Nykytilanteessa edelläkävijäyritysten ongelmana (first mover problem) on, että muut yritykset olisivat kyllä halukkaita hyödyntämään asiakkaan dataa, mutta eivät luovuttamaan sitä asiakkaalle vapaasti käytettäväksi.

4.1.3 Yritykset näkevät itsensä mieluiten kaiken keskellä

Ajatus rajapintojen kautta liikkuvasta datasta, joka mahdollistaisi ketterän organisaation ulkopuolisen sovelluskehityksen, toivotetaan usein tervetulleeksi. Se lisäisi palvelutarjontaa yrityksen asiakkaille, kun muut toimijat voivat tarjota täydentäviä palveluja. Yritysekosysteemejä kuvaavilla PowerPoint-kalvoilla oma organisaatio on yleensä keskellä ja kolmansia osapuolia on reunoilla rikastamassa palveluja, mutta ihminen saattaa puuttua kuvista kokonaan. Toimivasta ekosysteemistä on merkittävää arvoa, vaikkei oma organisaatio olisikaan sen keskiössä. Erikoistumalla kukin voi tehdä sitä, mitä parhaiten osaa, ja tukeutua ulkopuolisiin toimijoihin niissä asioissa, joita ei ole rahkeita toteuttaa riittävällä laadulla itse. Jos joku on henkilötiedon arvoverkon keskiössä, niin sen tulisi olla ihminen, joka hallinnoi omaa dataansa.

Tekniset ja strategiset ratkaisut, joita tehdään esimerkiksi henkilötietorajapintojen toteuttamiseksi, ovat pitkälti samoja riippumatta siitä, nähdäänkö yrityksen olevan keskellä vai reunalla. Mielen mallina organisaatiokeskeinen ajattelu on kuitenkin ristiriidassa MyDatan ihmiskeskeisen näkökulman kanssa. Se saattaa estää näkemästä yrityksen kannalta merkityksellisiä MyDatan mahdollisuuksia, jotka aukeavat nimenomaan ihmisten ollessa keskiössä. Vaikka oman yrityksen näkeminen kaiken keskellä ei ole varsinaisesti vaarallista, niin suuressa osassa tapauksia se on epärealistista. Vain muutamat yritykset kerrallaan voivat olla ekosysteemien napoina. Avoin ekosysteemi ei nojaudu yhteen keskusyritykseen, vaan jaettuun toimintamalliin ja standardeihin. Se antaa huomattavan suurelle määrälle yrityksiä tilaa olla tasapainoisesti mukana.

4.1.4 Meidän datasta ei ole muille iloa

Vaikka MyDataan suhtauduttaisiinkin myönteisesti eikä organisaatioilla olisi liiketaloudellisia esteitä toimia sen mukaisesti, niin usein juuri oman organisaation hallinnoimiin henkilötietoihin saatetaan suhtautua protektionistisesti. Datasta ei nähdä olevan mitään hyötyä alkuperäisen käyttötarkoituksen ulkopuolella.

Esimerkiksi hoitotyössä on ehdottoman tärkeää, että potilastieto on oikeaa. Lääkäri luottaa laboratoriotestien ja mittausten tuloksiin, jos hän tietää, että ne on tehty oikein ja oikeissa olosuhteissa. Tiedon oikeellisuuden voi taata virallinen sähköinen potilastietokanta, mutta siitä otettu MyData-kopio olisi altis tahalliselle tai tahattomalle manipuloinnille. Hoitotyön kannalta siis virallinen järjestelmä on luotettavin ja MyDatalle ei välttämättä nähdä tarvetta.

Datan saaminen ulos potilastietojärjestelmistä antaisi ulkopuolisille tahoille mahdollisuuden kehittää sovelluksia eri päätelaitteille ja eri kohderyhmille kuten näkövammaisille, kielitaidottomille, diabeetikoille jne. Potilas voisi esimerkiksi ajaa oman lääkityksensä validaattorisovellukseen ja saada tietoa, onko lääkityksessä mahdollisia päällekkäisyyksiä tai tarkastella verikokeissa mitattua hemoglobiiniarvoa ja verrata sen kehittymistä ruokavalionsa muutoksiin.

Alkuperäiseen käyttötarkoitukseen lukkiutuminen on hyvin tavallista. Vaikka ei itse heti keksikään mitään mielekästä ulkopuolista käyttöä oman organisaation hallinnoimalle henkilötiedolle, olisi hyvä asennoitua avoimen uteliaasti siihen, mitä ihmiset itse ja heidän valtuuttamansa muut oman alan ulkopuoliset toimijat voisivat keksiä.

4.1.5 Suojellaan tietoa ihmiseltä itseltään

Henkilötietojen käsittelyyn liittyvät lainsäädännölliset velvoitteet ovat yrityksille tuttuja. On yllättävää, kuinka usein tietosuojaan liittyvät vastuut nostetaan mahdollisten MyDataa estävien asioiden listalle, vaikka kysymys on siitä, että yksilölle itselleen vain annetaan pääsy omiin tietoihinsa koneluettavassa muodossa.

Esimerkiksi pankit eivät ole avanneet henkilöasiakkaille pääsyä omiin pankkitietoihin rajapintojen kautta ennen pakottavaa lainsäädäntöä, vaikka yritysasiakkaat ovat voineet kytkeä taloushallinto-ohjelmistonsa pankin järjestelmiin jo pitkään. Toimintatapaa on perusteltu henkilöasiakkaiden tietosuojalla. Verkkopankissa henkilöasiakkaat voivat manuaalisesti ladata tilitapahtumat omalle koneelleen. Tietosuojamielessä omalle koneelle lataaminen ei ole sen turvallisempaa, kuin että pankkitunnuksilla tunnistautunut henkilö antaisi luvan tietojensa siirtämiseen rajapinnan kautta vaikkapa omaan henkilökohtaiseen taloushallinto-ohjelmaansa.

Toisaalta tiukan tietosuojan ympäristössä datan säilyttämiseen liittyy paljon vastuita ja velvoitteita, joiden toteuttaminen ei ole ilmaista. MyData-periaatteilla voitaisiin kääntää tilanne sekä teknisesti että juridisesti niin, ettei palveluntarjoajan tarvitsisi välttämättä säilyttää dataa ja siten kantaa rekisterinpitäjän velvollisuuksia. Sen sijaan palvelulla olisi yksilön luvalla pääsy lukemaan ja tarvittaessa käyttämään tämän dataa.

4.1.6 Keskustelujen vaikeus

Avoimen dialogin puute marginalisoi ilmiön. MyData-keskustelut erkaantuvat todella syvään päähän ja toisaalta populistiseen päähän. Ei riitä, että asiat määritellään hyvin, keskustelulle pitää löytää yhteinen sanoitus vaikkapa politiikkaa varten.

MyData-keskusteluihin liittyy monia käsitteitä: Data, oikeudet, kontrolli, toimijuus, liiketoimintamallit, markkinamallit, kilpailu, ekosysteemit, yhteentoimivuus, luottamusverkot, hallintomallit, instituutiot, palvelumuotoilu, käytettävyys, profilointi, sääntely, suostumus, rahoitus, investointikyky, kansalliset tietoinfrastuktuurit, standardit, APIt, datamallit, ihmisten käyttäytyminen, arvot, ajankäyttö, datalukutaito, kulttuurierot, tietoturva, yhteiskunnalliset vaikutukset, politiikka, luottamus, yksityisyys, kansainväliset verkostot, jne. Käsitteiden moninaisuus johtaa siihen, että keskustelut ovat vaikeita.

MyDatan toteutuminen on tyypillinen kompleksinen ilmiö, kuten laajat yhteiskunnalliset muutokset usein ovat. Siihen liittyy paljon tuntemattomia seikkoja ja toistensa kanssa ristiin vaikuttavia tekijöitä. Kompleksinen ilmiö erotuksena monimutkaisesta tarkoittaa, ettei sitä lähtökohtaisesti ole mahdollista ratkaista tai määritellä, vaan järjestys syntyy itseorganisoitumisen kautta. Mikäli monimutkaista ongelmaa sinnikkäästi tutkii, niin se alkaa työn edistyessä yleensä selkiytymään.

MyDatan sanoittamisessa pitää vastustaa kiusausta pyrkiä tarkkuuteen. Tarkkuus on yleensä tulkittu hyveeksi, mutta kompleksisen ilmiön tapauksessa se johtaa terminologian räjähdykseen, mikä vie pohjan pois laajan yhteisymmärryksen muodostumiselta. Syntyy asiantuntijakultti, joka porautuu yhä syvemmälle yksityiskohtiin kykenemättä kommunikoimaan aiheesta kultin ulkopuolisille. Pian tarvitaan kolmipäiväinen MyDatan peruskurssi ennakkotietona ennen kuin voi osallistua keskusteluihin tulematta nauretuksi pihalle. Tarkkuuden sijaan pitää pyrkiä avaintermien laaja-alaisuuteen niin, että peruskonseptit on ymmärrettävissä ja merkityksellisiä eri taustoista tuleville osallistujille.

MyData ei ole kenenkään hallussa tai hallinnassa, se ei ole projekti tai ratkaisu, jonka mikään yksittäinen taho tai ryhmä voisi toteuttaa. Sen kehitystä ei voi ohjata, mutta sen toteutumiselle voidaan luoda mahdollisuuksia tukemalla itseorganisoitumista, altistamalla ajatukset muiden edelleen kehitettäviksi ja olemalla vastaanottavainen sille, mitä muut tekevät. Ratkaisujen vaatimisen ja ratkaisuista palkitsemisen sijaan tulisi luoda tiloja yhdessä oppimiselle ja dialogille ja palkita vuorovaikutuksesta. Maailma on täynnä kompleksisia ilmiöitä, eikä MyData ole mitenkään erityislaatuinen. Hierarkiatonta vuorovaikutusta ruokkiva asenne auttaa monien muidenkin asioiden ratkaisemisessa.

4.2 Uhkakuvat

4.2.1 Frankensteinin MyData

Henkilötiedon välittäminen, yhdistäminen ja analysointi on kitkatonta ja tapahtuu näennäisesti ihmisten hallinnoimana. Ihmisillä ei kuitenkaan ole aitoja valinnan mahdollisuuksia, sillä laajoja suostumuksia henkilötiedon käyttöön kysytään kaikkialla. Normaali arki ei suju, ellei omaa dataansa luovuta – halusi tai ei.

Vaikka ihmisellä olisi tekninen mahdollisuus hallita tietojaan tarkasti, se ei kuitenkaan automaattisesti johda siihen, että hänellä on mahdollisuus tehdä vapaasti päätöksiä. Tiedon helppo saatavuus voi entisestään kiihdyttää suuntausta, jossa ihmisiltä vaaditaan jatkuvasti enemmän henkilötietoja. Esimerkiksi lupa kerätä kattavia tietoja voi olla jonkin suositun palvelun edellytys. Ihmiset antaisivat rutiininomaisesti lupia liittyäkseen palveluun, jota syystä tai toisesta täytyy käyttää, jotta olisi yhteiskunnan normaali jäsen. Kuulostaako tutulta?

Voiko olla esimerkiksi niin, että tulevaisuudessa kohtuuhintaista vakuutusta on mahdotonta saada antamatta ensin kattavaa ja rikasta profiilidataa vakuutusyhtiölle? Lupa MyData-tilin penkomiseen voisi olla maahan pääsyn edellytyksenä rajalla tai ehtona pankkitilin avaamiseen, asunnon vuokraamiseen, työhaastatteluun pääsemiseen, työttömyyskorvauksen saamiseen jne. Mitä ikinä jokin sellainen taho keksii kysyä, jolle on vaikea tai mahdoton sanoa ei.

Se, että palveluntarjoajat ja muut pääsevät nykyään käsiksi vain epätäydellisiin ja heikkolaatuisiin tietoihin, tuottaa tehottomuutta, mutta myös suojaa ihmistä. Samalla kun tehottomuutta ratkotaan paremmalla yhteentoimivuudella tulee kehittää myös uusia keinoja ihmisten suojaamiseksi ja aitojen valinnan mahdollisuuksien varmistamiseksi.

Valvovien viranomaisten ja myös kansalaisjärjestöjen tehtävä on pitää huolta, etteivät organisaatiot väärinkäytä yksilöiden suostumusta henkilötiedon käyttöön, ja tarvittaessa reagoida väärinkäytöksiin ja nostaa niitä julkisuuteen. Näillä viranomaisilla ja järjestöillä pitää olla riittävät toimintaedellytykset, jotta ne pystyvät tämän tärkeän tehtävän hoitamaan.

EU:n uudessa tietosuoja-asetuksessa onkin kirjattu tietojen minimoinnin periaate, jonka mukaan suostumus ei yksin riitä henkilötiedon keräämiseen, vaan keruun pitää olla myös perusteltua ja tarpeellista. Myös alakohtaista sääntelyä tulee kehittää, esimerkiksi mitä tietoa vakuutuksenottajilta saa pyytää. Sääntely tuo markkinoille yhteiset pelisäännöt. Muutoin datan keruu helposti laajenee, jos yksi yritys tekee irtioton ja saa laajemmalla datalla kilpailuetua, johon muiden on vastattava pysyäkseen bisneksessä.

4.2.2 Laki ja teknologia tohtori Jekyllin ja Mr. Hyden käsissä

Tietosuoja-asetuksen kaltaiset aloitteet hyvässä tarkoituksessa pakottavat yritykset ja organisaatiot avaamaan järjestelmänsä ja tuomaan tiedot ihmisten itsensä saataville. Teknologian ja lainsäädännön kehitys ei pysähdy. Kvanttitietokoneilla murretaan nykyiset salausteknologiat, ja turvallisuuslainsääntö kehittyy suuntaan, joka pakottaa yritykset antamaan pääsyn ihmisten dataan myös viranomaisille ja niiden alihankkijoille. Se, mikä oli tarkoitettu ihmiselle itselleen, onkin teknologian ja pakottavan sääntelyn myötä myös muiden saatavilla.

Osa suomalaislukijoista nostaa kulmakarvojaan ja suosittelee yllä kuvatun skenaarion kirjoittajaa päästämään irti foliohatustaan. Kvanttitietokoneet kuulostavat scifiltä ja jos valtio säätää turvallisuuslainsäädäntöä, niin siihen on varmasti hyvä syy ja viranomaiset kyllä hoitavat hommansa niin, ettei kansalaisten yksityisyys tai muut oikeudet vaarannu.

Maailman mittakaavassa on poikkeavaa, että viranomaisiin luotetaan esimerkiksi henkilötietojen käsittelyssä niin paljon kuin Suomessa. Historiankuvaukset siitä, kuinka Natsi-Saksa hyödynsi viranomaisrekisterejä ja IBM:n tuottamaa reikäkorttiteknologiaa joukkovainojen työkaluina eivät Suomessa saa ihmisiä epäluuloisiksi hallintoa tai hallinnon ja yritysten yhteistyötä kohtaan. Meillä on paljon normaalimpaa puhua uhkakuvista, jotka liittyvät esimerkiksi suuryritysten vallankäyttöön. Koska MyData-kehityksessä pyritään globaaliin yhteentoimivuuteen, niin kulttuurierot ihmisten asennoitumisessa sekä todelliset riskit valtioiden kansalaisiinsa kohdistamasta valvonnasta on otettava tosissaan.

Kvanttitietokoneet eivät myöskään ole scifiä, niitä kehitetään kiihtyvällä vauhdilla ja esimerkiksi IBM tarjoaa jo nyt kvanttitietokoneensa käyttömahdollisuutta pilvipalveluna. Ennusteiden mukaan yleiskäyttöiset kvanttitietokoneet leviävät laajempaan käyttöön 2030-luvulla. Kryptografian asiantuntijat ovat jo pitkään tiedostaneet, että nykyiset julkisen avaimen salausmenetelmät menettävät tulevaisuudessa tehonsa, koska salaukset ovat purettavissa kvanttitietokoneiden laskentakapasiteetilla. Kehitteillä on uusia kvantinkestäviä salausmenetelmiä, mutta niiden standardointi ja käyttöönotto vie aikaa. Mikäli kvanttitietokoneiden kehitys voittaa nopeudessa uusien salausmenetelmien kehityksen ja käyttöönoton, niin silloin MyData on kenen tahansa luettavissa.

Teknologian ja lainsäädännön kehitys yhdessä ja erikseen voivat muuttaa yhteiskuntaa ja toimintaympäristöä hyvinkin radikaalisti. Se, mikä tänään ei ole mahdollista tai laillista, voi tulevaisuudessa olla. Arkisesti näin radikaaleja muutoksia ja niihin liittyviä riskejä ei huomioida teknologian kehityksessä ja käyttöönotossa.

4.2.3 Taistelu valtasormuksesta

Datataloudessa suurilla on etulyöntiasema teknologian ja käyttäjämassan ansiosta. Ihmiset, pienemmät yritykset ja valtiotkin ovat altavastaajina. MyData luo valinnanvapautta ihmisille ja tasapainottaa kilpailua. Kun data ei ole lukossa, ihmiset valitsevat erilaisia, pieniä tai kotimaisia palveluntuottajia. Jätit eivät luovuta, ne ostavat MyData-startupit pois kuljeksimasta, tekevät käytettävyydeltään ylivertaiset ja ilmaiset operaattoripalvelut, miehittävät standardointifoorumit, miinoittavat kentän teknologiapatenteilla ja lobbaavat lainsäätäjät puolelleen. Lopulta jätit palauttavat vallan itselleen entistä vahvempana. MyData on niille keino saada massoittain korkealaatuista tietoa yksilöistä.

Professori Lawrence Lessigin sanonta "koodi on laki" (code is law) kuvaa osuvasti digitalisoituvan yhteiskunnan dynamiikkaa. Tätä täydentää lausahdus "arkkitehtuuri on politiikkaa" (architecture is politics), jonka on tehnyt tunnetuksi yksi Electronic Frontier Foundationin perustajista Mitch Kapor. Siinä, missä laki määrittelee, mitä saa ja mitä ei saa tehdä, niin koodi määrittelee, mitä voi ja mitä ei voi tehdä. Jos lainsäätäjä ei uskalla konkretisoida kirjoittamaansa lakimuutosta, niin viime kädessä sen konkretisoi koodari. Vastaavasti jos politiikka ohjaa lainsäädännön kehittämistä, niin arkkitehtuuriratkaisut ohjaavat sitä, millaista koodia ja palveluja loppujen lopuksi tehdään.

Pystyäkseen hallinnoimaan ja hyödyntämään omaa dataansa ihmiset tarvitsevat palveluja. Jotta MyData-toimintamalli voisi skaalautua, niin palvelut tarvitsevat yhteentoimivuuden infrastruktuuria. Henkilödatan jakamisen ja hallinnan infrastruktuuri määrittelee, millaisten palvelujen tekeminen on mahdollista tai kannattavaa ja palvelut puolestaan määrittelevät, mitä voimme niiden sisällä tehdä. Millaiseen arkkitehtuuriin eli politiikkaan nojautuvan MyData-infrastruktuurin haluamme? Millaisia teknologioita ja standardeja käytetään, miten infrastruktuuria operoidaan, millaiset rakenteet, instituutiot ja säännöt ovat taustalla?

Riskinä on, että yksittäinen vahva toimija toteuttaa infrastruktuurin riittävän hyvin ja nopeammin kuin muut. Se pystyy tarjoamaan helppoa integroitavuutta sovelluskehittäjille sekä maksuttomuutta ja hyviä käyttöliittymiä ihmisille. Verkostovaikutukset vahvistavat sitä ja se saavuttaa monopoliaseman MyDatan ytimessä. Tällaisen toimijan politiikkana ei välttämättä ole tietosuojan vahvistaminen tai yksilön oikeudet saatikka kilpailun lisääminen.

Usein markkinat johtavat luonnostaan monopolien syntymiseen. Nyt dominoivassa asemassa olevat datajätit ovat päässeet asemiinsa internetin uusilla markkinoilla kuten esimerkiksi Standard Oil öljyteollisuuden syntyessä tai Bell System sekä valtioiden telemonopolit puhelinalalla. Kilpailulainsäädännön kautta öljyteollisuus ja teleala toimivat nykyisin avoimilla markkinoilla. Eri maiden kilpailuviranomaiset tutkivat jo, ovatko esimerkiksi Google ja Facebook tulkittavissa monopoleiksi, ja tulisiko markkinoita avaaviin toimenpiteisiin ryhtyä kansalaisten hyödyksi.

Kysymys on siis siitä, onko mahdollista kehittää avoimiin standardeihin nojautuvaa infrastruktuuria, joka johtaisi MyDatan alueella kilpailtuihin markkinoihin ilman monopolin syntymisen ja purkamisen välivaihetta.

4.2.4 Datavastuu lyyhistää ihmisiä

MyData tuo kauan kaivattuja digitaalisia oikeuksia ja valtaa ihmisille. Samalla lisääntyy yksilön vastuu; hänen on huolehdittava omasta yksityisyydestä ja siitä, mihin dataansa jakaa. Markkinat täyttyvät huijaripalveluista ja datapuoskareista: ensimmäiset kalastelevat henkilötietoja harhalupauksilla ja jälkimmäiset antavat ihmisten dataan pohjautuen valheellisia, vääriä tai jopa haitallisia tulkintoja ja "neuvontaa". Ihmisten kyvyt ja mahdollisuudet omien data-asioiden hoitoon jakautuvat epätasaisesti: toiset pärjäävät ja toiset eivät. Individualismia korostavassa yhteiskuntakehityksessä jokainen on kuitenkin oman onnensa seppä ja yksin datansa kanssa.

Omien tietojen hallinta on uusi asia, vaikka se tehdään käytettävyydeltään helpoksi ja tarjolla on apuja, kuten vaikkapa yksityisyysasetuksia vahtiva henkilökohtainen tekoäly-assistentti. Loppujen lopuksi ihmisen pitää kuitenkin vähintään ottaa tällaisia palveluja käyttöön ja tehdä erilaisia valintoja pitkin matkaa. Tämä edellyttää osaamista, viitseliäisyyttä, ajankäyttöä, työkaluja ja mahdollisesti taloudellisia resursseja.

Paljon on puhuttu ylijakamisen riskistä. Kaikki eivät ole kiinnostuneita tai osaa huolehtia yksityisyydestään. Ihmiset jakavat vahingossa dataansa laajemmin kuin ymmärtävät tai jakavat ymmärtäen, mutta laajemmin kuin olisi tarpeellista tai heille itselleen hyväksi. Datan jakamisen negatiivinen vaikutus saattaa paljastua vasta vuosien päästä, kun esimerkiksi terveystiedoista paljastuu nuoruuden humalahaaveri, joka haittaa vakuutuksen saantia.

Kokonaan toinen asia on datasta tehtävät tulkinnat ja niiden vaikutus ihmisten elämään. Kuka tulkintoja tekee ja kenen tulisi kantaa vastuu, jos tulkinnat ovat vääriä? Jotkut terveydenhuollon ammattilaiset ovat esittäneet huolensa siitä, että ihmiset alkavat liiaksi itse tulkita omaa terveysdataansa eivätkä hae ammattilaisen apua. Vääriä tulkintoja voi syntyä myös sen takia, että tiedon konteksti katoaa. Esimerkiksi tutkija saattaa ”tykätä” Facebookissa natsisivuista tutkimuksen tekemisen tarkoituksessa, mutta kontekstista tietämättä tehty profilointi saattaa johtaa väärään päätelmään.

Aina oikeakaan tulkinta datasta ei ole välttämättä haluttu. Pitäisikö joissain tilanteissa ihmistä suojella hänestä kerätyltä tiedolta? Omasta datasta saattaa paljastua asioita, joiden käsittelyyn ihminen ei ole valmistautunut. Esimerkiksi geenitiedon pohjalta voidaan arvioida kohonnutta alttiutta sairauksille, joista osaan ei ole parannuskeinoa. Kansalaisen pitäisi itse pystyä päättämään, haluaako hän esimerkiksi tietää, onko hänellä kohonnut riski sairastua johonkin vakavaan tautiin kuten Alzheimeriin.

Ylipäätään korostunut data- ja yksilökeskeisyyden yhdistelmä teknologiavetoisessa yhteiskuntakehityksessä on huolestuttavaa. Riskinä on, että ihmisnäkökulma kaventuu datanäkökulmaksi, eikä kollektiivisia ja sosiaalisia näkökulmia oteta huomioon lainkaan. Holhoamista ei tarvita, mutta datan välittämisen infrastruktuurin kehittämisen ohella tulisi varmistaa, että ihmisille on tarvittaessa tarjolla tukea tiedon käsittelyssä ja tulkinnassa. Tukea voivat tarjota esimerkiksi valmentajat, opettajat tai vertaiset.

5. MyData Suomessa

Paradigman muutos organisaatiokeskeisestä ihmiskeskeiseen henkilötiedon hallintaan on luonteeltaan globaali ja siksi aiemmissa luvuissa on kuvattu MyDatan mahdollisuuksia ja toteutumisen edellytyksiä ottamatta kantaa erityisesti kansallisiin kysymyksiin. Yksi selvityksen päämääristä on kuitenkin hahmottaa Suomen roolia MyDatan kehittämisessä kansainvälisesti. Tähän viimeiseen lukuun on koottu kansallisia kehityskulkuja, joilla on selkeästi liittymiä MyData-ajatteluun.

Kotimaisessa kehitystyössä tulee jatkuvasti korostaa, että MyData tarjoaa mahdollisuuksia ratkaista henkilötiedon hallinnan haasteita kansallista tasoa laajemmin. Suomen kokoisessa maassa on houkuttelevaa pyrkiä kehittämään kaikkia suomalaisia palvelevaa kansallista infrastruktuuria. Tällainen infrastruktuuri ei kuitenkaan automaattisesti toimi muissa maissa. Suomi voi kuitenkin toimia yhteentoimivuutta korostavien MyData-sovellusten kokeilumarkkinana. Pienessä, korkeasti koulutetussa maassa yhteisistä käytännöistä on helpompi sopia kuin suuremmissa maissa. Mikäli henkilötiedon hallinnan globaalien haasteiden ratkaisemista ja laajasti skaalautuvaa palvelujen yhteentoimivuutta pidetään tietoisesti tavoitteena, niin Suomessa kokeillut ratkaisut voidaan viedä maailmalle.

MyData ei ole suomalainen ilmiö, vaan avauksia ihmiskeskeisen datan hallinnan toteuttamisessa on tehty useissa maissa. EU:n tietosuoja-asetus lisää entisestään kiinnostusta uusiin toimintamalleihin ja eurooppalaisten kilpailuvalttien löytämiseen datan käytön saralla. MyData-periaatteiden noudattaminen edesauttaa asetuksen vaatimusten täyttämisessä mm. suostumusten hallinnassa ja datan siirrettävyydessä ja voi siten tuoda kilpailuetua periaatteita noudattaville yrityksille.

Globalisaatio muuttaa suomalaista yhteiskuntaa ja palveluja myös sellaisilla perinteisillä aloilla, jotka ovat yleensä olleet kotimaisten toimijoiden hallussa. Pelko isojen monikansallisten yritysten liiketaloudellisen vallan kasvamisesta on ajankohtaista ja osin aiheellista. Tietoinfrastruktuurin organisoiminen avoimuuden periaatteilla voi parantaa kotimaisten toimijoiden kilpailukykyä suhteessa kansainvälisiin yrityksiin, joiden kilpailuetu perustuu pääasiassa suljettuihin järjestelmiin ja suuren kokoon. Nyt on aika toimia, jotta suomalaiset pysyvät kärkijoukoissa kehittämässä henkilötiedon hyödyntämisen käytäntöjä. Suomeen on mahdollista rakentaa vahva MyData-osaamisen keskittymä ja sitä kautta tuoda suomalaisille yrityksille kansainvälistä kilpailuetua.

MyDatan kehittymiseen tarvitaan avoimuutta, yhteistoimintaa ja luottamusta ihmisten ja organisaatioiden välille. Suomalaisesta yhteiskunnasta löytyy näitä ominaisuuksia. Suomessa on vahvat perinteet avoimessa tietoteknisessä kehityksessä esimerkiksi avoimen datan ja avoimen lähdekoodin alueilla. Myös yritysten ja valtion yhteistyöllä on saatu tuloksia. Esimerkiksi GSM-standardin nopea omaksuminen ja sitä seurannut mobiiliteollisuuden kehittyminen on esimerkki siitä, miten Suomi voi olla aktiivisesti mukana kansainvälisesti, yhteiskunnallisesti ja kaupallisesti merkittävän uuden teknologian kypsyttämisessä ja maana hyötyä edelläkävijyydestään. Mobiiliteollisuuden kehittymisessä avainasemassa oli avoimiin standardeihin perustuva verkostomainen toiminta. Verkostotoimintamalli on myös MyData-rakenteiden kehittymisen keskeinen mahdollistaja.

Henkilötiedon alueella ratkaistavat kysymykset ovat erilaisia, eikä vanhoihin teleoperaattori-maailman esimerkkeihin ja menestystarinoihin pidä tuudittautua liian syvälle. Toiminnan edistämiseksi on syytä luoda rohkea mutta uskottava visio siitä, miten Suomi voi kehittää uusia toimintamalleja. Tämä edellyttää, että yritykset lähtevät varhaisessa vaiheessa mukaan kehittämään uutta liiketoimintaa – soveltuvin osin yhdessä julkisen sektorin kanssa.

5.1 MyDatan toteutunut kehitys Suomessa

Tämän selvityksen ensijulkaisun (2014) jälkeen Suomessa on tapahtunut paljon kehitystä MyData-ajattelussa ja myös kansainvälinen huomio on kasvanut. Liiketoimintamallien osalta kehitys on vielä varhaisessa vaiheessa, mutta kansainvälisesti vertailtuna suomalainen MyData-työ on edistyksellistä erityisesti siinä, miten täällä painotetaan toimijoiden välistä yhteentoimivuutta (vastakohtana ns. winner-takes-all-malli). Suomalainen MyData-kehitys on saanut paljon positiivista huomiota maailmalla ja esimerkiksi Euroopan komissio on nostanut sen esille osana datatalous-tiedonannon valmistelutyötä (EU 2017). Kansainvälistä tunnettuutta Suomen MyData-toiminnalle on saatu myös Helsingissä ja Tallinnassa järjestettyjen vuotuisten suurten MyData-konferenssien myötä (**mydata2018.org**).

Vuonna 2015 Sipilän hallitus nosti aiheen hallitusohjelmaan seuraavalla linjauksella: *"Vahvistetaan kansalaisten oikeutta valvoa ja päättää itseään koskevien tietojen käytöstä"* (Valtioneuvosto 2015). Samana vuonna liikenne- ja viestintäministeriö yhdessä Aalto-yliopiston kanssa käynnistivät MyData-palvelupilotteja kehittävien suomalaisten yritysten foorumina toimivan MyData-allianssin. Allianssissa on mukana noin 40 suomalaista organisaatiota: suuria toimijoita kuten kauppaketjuja, pankkeja ja teleoperaattoreita, MyDataan liittyviä startupeja sekä tutkimuslaitoksia ja julkishallintoa (**mydata.fi**).

Eräiden MyData-allianssissa mukana olevien yritysten ja tutkimuslaitosten yhteistyössä käynnistettiin syksyllä 2017 yritysten ja Business Finlandin rahoittama TrustNet-hanke (**trustnet.fi**). Hankkeen tavoitteena on luoda Suomessa luotettava hajautetun digitaalisen identiteetin verkosto ja kestävä yhteentoimivuuden malli henkilötiedon hallintaan, joka olisi skaalattavissa muualle. Tekes on rahoittanut myös muita MyDataa edistäviä tutkimus- ja yrityshankkeita kuten Digital Health Revolution (2014–2018) ja Personal Data Management Platforms (2016–2018). Vuonna 2016 Teknologiateollisuus yhdessä jäsenyritysten sekä liikenne- ja viestintäministeriön kanssa järjesti Maankoodauskurssin, jonka aiheena oli MyData-operaattoritoiminnan kiihdyttäminen.

Hallituksen kärkihankkeista: "Digitaalisen liiketoiminnan kasvuympäristön rakentaminen (Digi2-hanke)[9]" ja "Yhteisen tiedon hallinta (YTI-hanke)[10]" edistävät MyDataan liittyvää kehitystä sekä julkisella että yksityisellä sektorilla. Digi2 toteuttaa valtioneuvoston periaatepäätöstä datan hyödyntämisestä liiketoiminnassa[11], jossa omadatan toimet on linjattu ja viety toteutukseen verkostotoimintana sekä vaikutettu EU:n datatalouden politiikka-alueella. Liikenne- ja viestintäministeriö on lisäksi sisällyttänyt MyData-periaatteita liikennepalvelulakiin. YTI-hankkeen yksi työpaketti käsittelee omadataa ja sen tavoitteena on toteuttaa Kosken (opintojen tietovaranto) yhteyteen ensimmäinen tuotantoversio suostumustenhallinnasta sekä tuottaa viitearkkitehtuuri, jonka avulla omadata saadaan jatkokehitettyä ja skaalattua laajemmin julkisen hallinnon käyttöön. YTI hanketta ohjaa Valtiovarainministeriö ja sen toteuttaa Väestörekisterikeskus, josta tulee vuoden 2020 alusta julkista hallintoa palveleva Digi ja väestötietovirasto.

Toteutusvaiheeseen edenneiden hankkeiden lisäksi MyData on huomioitu vahvasti strategisella tasolla valtionhallinnossa ja suurissa kaupungeissa. Työ- ja elinkeinoministeriön tekoälyohjelman julkaisussa (TEM 2017) esitetään omadatan vapauttamista kansalaisten käyttöön sekä dataoperaattoripilotointia keinoina suomalaisten datavarantojen joustavampaa hyödyntämiseen. Tekesin julkaisemassa digitaalisen alustatalouden tiekartastossa (Viitanen et al. 2017) ehdotetaan, että käynnissä oleva MyData-yhteistyö erityisesti julkisella sektorilla hankkeistettaisiin yhdeksi, yhteiseksi MyData-palvelujen kehityshankkeeksi. Päämääränä olisi kehittää suomalainen alusta-arkkitehtuuri ja sen päälle

9 Digitaalisen liiketoiminnan kasvuympäristön rakentaminen – https://www.lvm.fi/digitalisaatio
10 YTI Yhteisen tiedon hallinta -hanke – http://vm.fi/yhteinen-tiedon-hallinta
11 Valtioneuvoston periaatepäätös: Datan hyödyntäminen liiketoiminnassa https://valtioneuvosto.fi/paatokset/paatos?decisionId=0900908f804c23c7

sovellettava liiketoimintakonsepti. Myös Valtioneuvoston kanslia on julkaissut MyData muutosvoimana -vaikutusarvioinnin (Knuutila et al. 2017) ja Helsingin kaupunki on sitoutunut noudattamaan MyData-periaatteita palvelujensa uudistamisessa[12].

Nämä ovat lupaavia askeleita kohti ihmiskeskeisen tiedonhallinnan toteutumista, mutta kehitys on kuitenkin vielä varhaisessa vaiheessa. Tarvitsemme edelleen tutkimusta ja tuotekehitystä, toimintatapojen ja asenteiden uudistamista sekä ennen kaikkea tiivistä vuorovaikutusta eri tahojen ja sektoreiden välillä. Ratkaisevia ovat innokkaat ihmiset ja organisaatiot, jotka ovat valmiita kokeilemaan ja oppimaan kokeiluista. Nyt on syytä myös katsoa maailmalle ja pyrkiä houkuttelemaan esimerkiksi henkilödatan välittämiseen keskittyneitä kansainvälisiä toimijoita Suomeen, jotta voimme kiihdyttää omaa oppimistamme.

2014 Yhteisen näkemyksen muodostuminen Kehitysvisio hajautetusta, mutta yhteentoimivasta henkilötiedon hallinnan infrastruktuurista kiteytyi useiden yritysten, julkishallinnon toimijoiden, tutkijoiden ja kansalaisaktiivien yhteistyönä, ja tuloksena syntyi MyData-selvityksen ensimmäinen versio.
2015 Kansallinen sitoutuminen ja kansainvälisten yhteyksien luominen Hallitusohjelman linjaus toi Suomessa selkänojan jatkotyölle, joka konkretisoitui MyData Allianssin perustamiseen yhteistoimintamallin kehittämisen foorumiksi. MyData-selvityksen englanninkielisen version julkaiseminen toi kansainvälisiä yhteyksiä ja kytki suomalaisen MyData-kehitystyön kansainväliseen toimintaan.
2016 Kansainvälinen profiloituminen Julkishallinnon kärkihankkeet ja ensimmäinen kansainvälinen MyData-konferenssi
2017 Toimintamallin leviäminen ja periaatteiden kirkastuminen Kansainvälisessä yhteistyössä kirjoitetaan MyData julistus (**mydata.org/declaration**), joka kirkastaa yhteiset ihmiskeskeisen henkilötiedon hallinnan periaatteet. Suomessa MyData-toimintamalli huomioidaan strategisella tasolla esimerkiksi valtionhallinnossa, suurissa kaupungeissa ja joissain yrityksissä. (Valtioneuvoston kanslian ja Helsingin kaupungin omat MyData-esiselvitykset, Alustatalouden tiekartasto ja Tekoälystrategia)
2018 Käytännön toteutukset pilottihankkeissa MyData-mallia demonstroidaan yksittäisissä kaupallisissa ja julkishallinnon piloteissa (YTI MyData-pilotit ja TrustNet-hanke). Pilottihankkeissa on mukana myös kansainvälisiä toimijoita.

Taulukko 5.1: Nostoja MyData-kehityksestä Suomessa vuosilta 2014–2018.

12 https://www.hel.fi/uutiset/fi/kaupunginkanslia/helsinki-sitoutuu-edistamaan-mydataa

5.2 MyData-visio seuraaville vuosille

MyData Allianssin vuoden 2017 viimeisessä kokoontumisessa käynnistettiin visiokeskustelu, jolla pyrittiin hahmottamaan suuntaa seuraaville vuosille. Yhteistä tulevaisuudenkuvaa on sen jälkeen työstetty muun muassa yritysten, Sitran IHAN®-avainalueen[13] ja valtionhallinnon toimijoiden kanssa. Avoimissa verkostoissa tapahtuva visiotyö ei oikeastaan tule koskaan valmiiksi, vaan eri toimijat tulkitsevat ja muokkaavat tulevaisuuden näkemystään jatkuvasti yhdessä ja erikseen. Alla oleva on yksi kiteytys siitä, miten Suomen MyData-kehityksessä aktiiviset toimijat keskustelevat tulevaisuudesta.

MyData-kehittämisen lähtökohtina ovat EU:n arvopohja, avoin kilpailu ja tiukka tietosuoja. MyData-infrastruktuuri luo toimintaedellytyksiä ihmislähtöiselle datataloudelle, jossa ihmisillä ja yrityksillä on oikeudet ja käytännön mahdollisuudet itseään koskevien tietojensa hallintaan, jakamiseen ja uusiokäyttöön. Tietoja voidaan hallitusti ja joustavasti yhdistää organisaatiorajojen yli ja siten olennaisesti parantaa palveluja ja tuottavuutta sekä edistää uudenlaisten liiketoimintamallien syntymistä. Tavoitteena ovat saumattomat arkea helpottavat ja kustannustehokkaat digitaaliset palvelut, jotka toteutetaan läpinäkyvästi ja turvallisesti niin, että ihminen voi itse hallita omaa digitaalista maailmaansa.

- **Sujuvat palvelut:** Suomessa noudatetaan laajasti MyData-periaatteita henkilötiedon käsittelyssä digitaalisissa palveluissa. Ihmisten päivittäinen elämä on helpottunut uusien MyData-periaatteita noudattavien palvelujen yleistyttyä. Henkilötietojen käytön läpinäkyvyys ja turvallinen henkilötiedon jakaminen ovat luonnollisia toimintoja käyttäjille.
- **Kokeilumarkkina suomalaisille ja kansainvälisille toimijoille:** Toimiva ja joustava toimintaympäristö mm. julkishallinnon ja yritysten yhteistyön, tutkimustoiminnan, investointien, rahoituksen ja paikallisen sääntelyn osalta edesauttaa uusien henkilötietoon pohjautuvien tuotteiden, palvelujen ja ketterien sovellusten syntyä. Tämä on houkutellut lukuisia kansainvälisiä yrityksiä ja muita toimijoita sijoittumaan Suomeen ja liittymään kumppaniksi suomalaisten organisaatioiden kanssa toteutettaviin MyData-kehitysprojekteihin.
- **Yhteistoimintamalli:** Toimijoiden ja projektien välillä on tiivistä paikallista vuorovaikutusta, joka kerryttää yhteistä jaettua osaamista Suomeen ja samalla kiihdyttää MyDatan kehitystä kansainvälisesti, koska mukana on myös kansainvälisiä toimijoita. Vahva osaaminen tuottaa kansainvälistä liiketoimintaa suomalaisyrityksille ja suomalaisasiantuntijoita kutsutaan neuvonantajiksi kansainvälisiin hankkeisiin.

5.2.1 Toimintasuunnat vision toteuttamiseksi

Vision toteuttamisen kannalta tärkeitä tunnistettuja toimintasuuntia ovat operaattoritoiminnan kiihdyttäminen, datan jakamisen liiketoimintaverkostojen käynnistäminen, kansainvälinen laajentuminen ja standardointityö. Näitä eri toimintasuuntia kannattaa edistää samanaikaisesti, ne ruokkivat toisiaan, mutta eivät ole toisistaan riippuvaisia.

13 Sitra ihmislähtöinen datatalous – https://www.sitra.fi/aiheet/ihmislahtoinen-datatalous

Operaattoritoiminta

Keskeinen pitkän tähtäimen tavoite suomalaisessa MyData-tekemisessä on MyData-palveluinfrastruktuurin synnyttäminen. MyData-operaattoritoiminta ei ole vielä Suomessa käynnistynyt, eikä täällä toimi kovin monia sellaisia yrityksiä, jotka olisivat erikoistuneet toteuttamaan henkilötiedon välittämisen infrastruktuuripalveluja (eng. Personal Information Management Services PIMS). Tämä on vaikuttanut toimintaan toisaalta niin, että mikään yritys ei ole Suomessa dominoinut MyData-kehitystä voimakkaasti ja siten täällä on voitu keskittyä enemmän verkostomaisten ja yhteentoimivuutta korostavien ratkaisujen edistämiseen. Toisaalta MyData-operaattoritoimijat olisivat luonnollisesti veturiyrityksiä, jotka omista liiketoiminnallisista intresseistään johtuen pyrkisivät aktiivisesti vahdittamaan käytännön toimintaan siirtymistä. Tällaisten veturiyritysten vähäinen määrä saattaa hidastaa suomalaisten MyData-toteutusten syntymistä. Esimerkiksi Ranskalainen monivuotinen MyData-hanke MesInfos[14] on rakentunut vahvasti infrastruktuuria tarjoavan Cozy Cloud -yrityksen ympärille ja siellä on Suomeen verrattuna hieman nopeammin siirrytty käytännön kokeiluihin, mutta toisaalta painotus hajautettuihin malleihin ja yhteentoimivuuteen on siellä ollut vähäisempää.

Liiketoimintaverkostot

Käytönnöllinen kehitysaskel kohti laajempaa yhteistoimintamallia on käynnistää pienempiä liiketoimintaverkostoja, jotka perustuvat hajautettujen identiteettien ja henkilötiedon jakamisen teknologioihin. Ensimmäiset suomalaiset kokeilut yritysverkostoista on jo lanseerattu. Esimerkiksi Asiakastieto, Nordea, OP ja Tieto ovat yhdessä viranomaisten kanssa kehittäneet lohkoketjuteknologiaan perustuvan liiketoimintaverkoston, jonka avulla osakeyhtiön voi perustaa täysin digitaalisesti[15]. Seuraavaksi on vuorossa laajemmat kokeilut uusilla alueilla.

Lohkoketjuihin perustuvat hajautetut identiteetti- ja luvitusratkaisut mahdollistavat datan jakamista sekä yritysten ja organisaatioiden välistä yhteistoimintaa uusilla tavoin. Aiemmin yhteiskäyttöisen tiedon luomiseen ja jakamiseen on tarvittu keskitetty rekisteri ja sen ylläpidosta vastaava organisaatio. Hajautetut teknologiat mahdollistavat tavoitteellisten liiketoimintaverkostojen perustamisen joustavammin ilman keskitettyä rekisteriä ja hallinnointiorganisaatiota. Tällaiset hajautetut yritysverkostot voivat kehittyä ja kasvaa nopeammin ja ne sallivat aiempaa suurempia vapauksia verkostojen liiketoimintamalleihin.

Kansainvälinen laajentuminen

Kansainvälisten tapaamisten ja MyData-konferenssien ympärille on muodostunut kasvava globaali yhteisö, jolla on paikallistoimintaa jo yli 20:ssä paikallisessa MyData-hubissa (**mydata.org**). Euroopan ulkopuolella hubeja on mm. Japanissa, Brasiliassa ja Pohjois-Amerikassa. Suurin osa hubeista on toistaiseksi vielä pieniä ja vapaamuotoisia paikallisyhteisöjä, mutta esimerkiksi Hollannissa, Ranskassa ja Tanskassa toiminta on tavoitteellista ja säännöllistä ja mukana on paikallisia yrityksiä vastaavasti kuin suomalaisessa MyData-allianssissa. Kansainvälinen verkoston tavoitteena on perustaa MyDatan edistämiseen ja yhteistoiminnan rakenteita kehittämään MyData Foundation, jonka kotipaikaksi on tulossa Suomi.

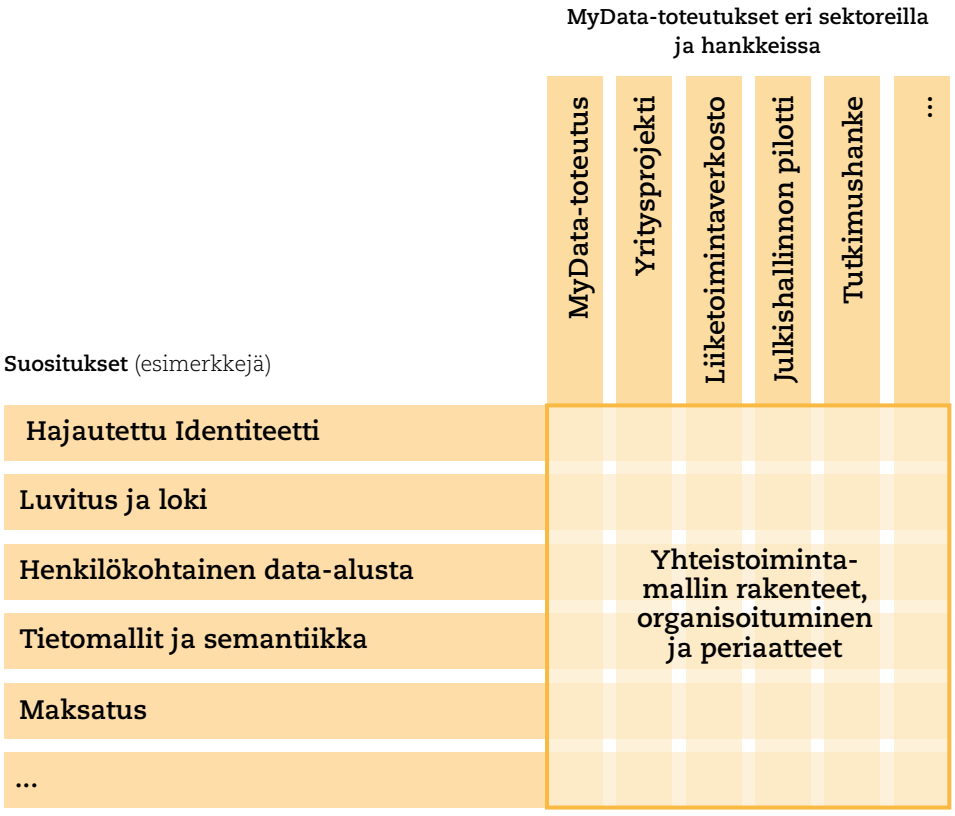
Suomella on hyvä mahdollisuus asemoitua kansainväliseksi ajatusjohtajaksi henkilötiedon hallinnan ja ihmiskeskeisen datatalouden alueilla. Tämä edellyttää aktiivista verkostoitumista ja kansainvälistymistä esimerkiksi EU-tason yhteistyöhankkeissa ja kansainvälisillä standardointi- ja teknologiafoorumeilla. Esimerkiksi Sitran IHAN®-hankkeessa on otettu lähtökohdaksi EU:n alue ja käynnistetään standardointityö CEN-CENELEC:ssä.

14 http://mesinfos.fing.org/english
15 Tieto, Lohkoketju mahdollistaa täysin digitaalisen identiteetin uusille yrityksille (15.5.2018) - https://www.tieto.fi/uutiset/lohkoketju-mahdollistaa-taysin-digitaalisen-identiteetin-uusille-yrityksille

Standardien valinta, käyttöönotto ja kehittäminen

Suomeen on syntynyt ja ja syntyy jatkossakin erilaisia käytännön toteutuksia, jotka pyrkivät noudattamaan MyData-periaatteita. Nämä voivat olla yksittäisten yritysten tai organisaatioiden omia projekteja, laajempia toimialakohtaisia liiketoimintaverkostoja, julkishallinnon hankkeita, tutkimusprojekteja tai näiden yhdistelmiä. Eri toimijoiden toteutukset on rahoitettu ja organisoitu eri tavoin. Vaikka kaikki pyrkisivätkin noudattamaan samoja korkean tason periaatteita ihmiskeskeisestä henkilötiedon hallinnasta, niin toteutusten välistä yhteentoimivuutta ei synny ilman erityistä panostusta. Toisaalta taas yhteentoimivuuteen keskittyminen on työlästä ja saattaa eri MyData-toteutuksien tekijöiden näkökulmasta näyttäytyä ylimääräisenä tekemisenä.

Kevyt ja mahdollisimman paljon käytännön toteutuksia tukeva malli yhteentoimivuuden kehittämiseen on eri MyData-toteutusten yhteinen suosituksia antava toimielin. Toimielin antaisi teknisiä suosituksia, joita MyData-toteutuksia tekevät tahot asteittain sitoutuvat noudattamaan, ja suosituksia tarkennettaisiin saatujen käytännön kokemusten myötä. Toteuttajilla on kuitenkin osin samoja teknologiavalintoihin liittyviä haasteita ratkottavanaan ja kaikki hyötyisivät siitä, jos eri aihepiireistä olisi laadittu selkeitä perusteltuja suosituksia, joihin voisi nojautua.



Kuva 5.1: Kevyt ja mahdollisimman paljon käytännön toteutuksia tukeva malli yhteentoimivuuden kehittämiseen. Toisistaan riippumattomien MyData-toteutusten edustajat muodostavat toimielimen, joka antaa teknisiä suosituksia, joiden noudattamiseen eri toteutusten tekijät asteittain sitoutuvat.

5.2.2 Suomesta MyDatan kokeilumarkkina

Mikä kannustaa nykyisin dataa keräämiä organisaatioita avaamaan henkilötietoa ihmisille itselleen MyDataksi ja mitä oikeuksia on datan alkuperäisellä tuottaja-organisaatiolla? Miten MyData-rajapinnat toteutetaan turvallisesti? Mitkä ovat ensimmäiset menestyvät liiketoimintamallit MyDatassa? Mikä on julkishallinnon rooli? Miten nykyiset datajätit kuten Google ja Facebook reagoivat uuteen kehitykseen? Miten tietosuoja-asetuksen vaatima datan siirrettävyys toteutetaan? Millaisia palveluja ja palveluntarjoajia henkilötiedon hallinnointiin syntyy ja mikä on tällaisten toimijoiden liiketoiminnan ydin? Miten ratkaistaan datan semanttinen yhteentoimivuus? Miten koneoppiminen ja analytiikka toteutetaan MyData-maailmassa? Miten henkilötietoa saa tutkimuskäyttöön? Miten ihmisten arkiset dataan liittyvät toimintatavat muuttuvat? Miten datan hallinta voidaan tehdä ymmärrettäväksi ja käytettäväksi? Miten vältetään se, etteivät ihmiset vain salli kaikkea mahdollista datan käyttöä, kuten nykyisin, käyttöehtoja lukematta? Miten digitaalinen identiteetti toteutetaan niin, että se tukee hajautettua MyData-mallia?

MyData on monitahoinen kokonaisuus yhteiskunnallisia, teknisiä, juridisia ja liiketaloudellisia kysymyksiä. Kenttä on haastava, mutta samalla se tarjoaa valtavasti mahdollisuuksia uusille innovaatioille. Yritykset ja organisaatiot ympäri maailmaa kehittävät ja esittävät omia ratkaisujaan ja näkemyksiään yllä lueteltuihin ja muihin vastaaviin kysymyksiin kiihtyvällä tahdilla. Vaikka kehitys on nopeaa, niin etenkin infrastruktuuritason, hallinnon ja sääntelyn innovaatiot kypsyvät luonnostaan hitaammin, joten samassa ajassa teknologian ja liiketoiminnan kehityksessä ehditään tehdä useita kokeilukierroksia. Nyt ja lähivuosina emme vielä tiedä, mitkä ratkaisut tulevat jäädäkseen, mikä toimii ja mikä ei.

Vaikka digitaaliset markkinat ovat kansainväliset, niin innovaatioiden kehittämisessä saman alan toimijoiden fyysisestä läheisyydestä ja keskittymisestä on kuitenkin mittavaa etua ja se on monesti jopa välttämätöntä. Tällä hetkellä MyDataan liittyvän teknologian ja liiketoiminnan kehitys on hajautunut ympäri maailmaa. Eurooppa on selkeä veturi ja hyvä markkina-alue tietosuojaa korostavan ja yhtenäistyvän sääntely-ympäristön takia, mutta innovaatiokeskittymäksi Eurooppa on liian laaja. Yhdessä oppimisen ja yhteistoimintamallien syntymisen kannalta ei ole mitään iloa siitä, että yhdellä start-upilla on Reykjavikissa terveysdatapilotti ja toisella Pariisissa vakuutusalan kokeilu ja kolmas kehittää energiadatan alustaa Amsterdamissa.

Viime vuosien aikana Suomi on profiloitunut maana, jossa ymmärretään ja määrätietoisesti viedään eteenpäin ihmiskeskeistä henkilötiedon mallia kokonaisvaltaisesti. Kansainvälisessä kehityksessä Suomen rooli voisi olla tarjota houkutteleva alusta uusien MyData-palvelujen kokeiluille ja tuotekehitykselle – kuten Suomi oli vuosituhannen alussa kokeilumarkkina monille mobiilialan innovaatioille. Aiemmin mainittu TrustNet-hanke on esimerkki siitä, miten kansainvälinen uutta hajautetun identiteetin teknologiaa kehittävä Sovrin-säätiö (**sovrin.org**) on hankkeen puitteissa tuotu yhteistyöhön suomalaisten yritysten ja tutkimuslaitosten kanssa. Vastaavia esimerkkejä tarvitaan lisää.

Samalla kun kansainvälisiä toimijoita houkutellaan Suomeen, tulee huolehtia siitä, että oma visiomme avoimiin standardeihin pohjautuvasta yhteentoimivasta infrastruktuurista säilyy kirkkaana. Muutoin riskinä on päätyä lisensoimaan kansainvälisten toimijoiden kautta sellaisia teknologioita, jotka hämärtävät yhteentoimivuutta ja muodostavat suljettuja henkilötiedon hallinnan saarekkeita.

5.3 MyDataan liittyvää toimintaa Suomessa

Tähän osioon on koottu nostoja Suomen julkisen hallinnon ja välillisen julkisen hallinnon käynnissä olevista toimista, jotka tukevat MyData-kehitystä Suomessa.

Eettistä tietopolitiikkaa tekoälyn aikakaudella

Suomessa on valmisteltu loppusyksystä 2018 eduskunnalle annettavaa selontekoa työotsikolla ”Eettistä tietopolitiikkaa tekoälyn aikakaudella”. Selontekoon sisällytettävät toimet koskevat esimerkiksi tietoturvallisuutta ja tietosuojaa sekä tiedon keräämistä, yhdistämistä, avaamista ja säilyttämistä. MyData-periaatteet ovat erittäin hyvin linjassa eettisen tietopolitiikan tavoitteiden kanssa. Tekoäly ja MyData kytkeytyvät toisiinsa sitä kautta, että erilaisten koneoppimisen sovellusten kehittäminen edellyttää pääsyä laadukkaisiin data-aineistoihin. MyData-infrastruktuurin avulla tekoälyä kehittävät yritykset ja tutkimuslaitokset voivat saada pääsyn tarkkaan ja rikkaaseen ihmisten dataan ihmisten omalla suostumuksella. Tämä ei takaa samanlaisia massadatan apajia, joita esimerkiksi suurilla sosiaalisen median palveluilla on, mutta vastaavasti MyDatana luvitettu tieto on tarkempaa ja voisi tukea esimerkiksi henkilökohtaisten tekoälysovellusten kehittämistä.

Palveluväylä

Valtiovarainministeriön johdolla rakennettava palveluväylä on keskeinen kansallinen tietoarkkitehtuurin kehittämishanke. Sen on tarkoitus tarjota yhtenäiset keinot tunnistautumiseen ja tiedon siirtämiseen julkisten tietovarantojen ja tiedon käyttäjien välillä, samalla tehostaen myös henkilötiedon käyttöä. Julkishallinnolle on säädetty velvollisuus liittää merkittävimmät ihmisiä koskevat tietovarantonsa palveluväylään. Suomi.fi-verkkopalvelussa on kehitteillä kansalaisen palvelunäkymä, josta kansalaisen on helppo nähdä omat tietonsa lukuisista eri rekistereistä.

Palveluväylä sisältää siis useita niistä komponenteista, joita toimiva MyDatan hyödyntämisen järjestelmä edellyttäisi. Väestörekisterikeskus ryhtyi vuonna 2017 valmistelemaan sitä, että valikoidut tiedot palveluväylästä olisivat yksilöille tarjolla siirrettäväksi muihin palveluihin avoimien rajapintojen ja käyttäjän valinnan pohjalta. Suomen julkinen sektori on siis hyvissä asemissa tullakseen yhdeksi mallikkaaksi MyData-toimijaksi. Sen kannattaa erilaisten kokeilujen myötä oppia lisää siitä, minkä kaltaisilla järjestelyillä merkittävät julkiset tietovarannot voidaan saada hyödynnettäviksi, mikä tukee henkilötiedon ekosysteemin syntymistä.

Tietoja kysytään kansalaiselta ja yritykseltä vain kerran

Suomen julkishallinnon digitalisoinnin periaatteissa on linjattu: *”Asiakkaalta ei kysytä sellaista tietoa, joka julkisella hallinnolla on jo tiedossaan. Palveluiden tuottama tieto on yhteentoimivaa muiden palveluiden kanssa, jolloin palvelut voivat vaihtaa tietoja keskenään ilman tarvetta kysyä tietoa uudelleen ihmisiltä tai yrityksiltä. Mikäli asiakkaalta tarvitaan tietoja, joita meillä ei vielä ole, nämä tiedot selvitetään asiakkaan kannalta mahdollisimman sujuvasti ja vaivattomasti.”* Linjaus ohjaa julkisen sektorin toimijoita yhdenmukaistamaan tiedon hallinnon käytäntöjään. Tiedon parempi järjestäminen ja kokonaisvaltainen johtaminen tukee MyDatan kehittymistä ja tehostaa samalla koko julkisen hallinnon toimintaa.

Massadataan ja tekoälyyn liittyvä tutkimus ja kehitys

Viime aikoina massadatan (big data), tekoälyn ja erilaisten data-alustojen kehitys ovat olleet suosittuja tutkimus- ja tuotekehitysteemoja ja saaneet runsaasti rahoitusta ja huomiota niin kansallisesti kuin Euroopan tasollakin. Suomessa näihin teemoihin liittyvää rahoitusta myönnetään niin Business Finlandin, Suomen Akatemian kuin valtioneuvoston strategisten linjausten ja ministeriöiden toimesta. Koska MyDatalla, tekoälyllä ja massadatalla on yhteys esimerkiksi anonymisointirakenteiden kautta, voidaan osa tutkimukseen ja kehitykseen kanavoidusta rahoituksesta ohjata MyData-infrastruktuurin kehittämiseen. Tekoälyn ja massadatan tutkimuksen kannalta MyData voidaan nähdä ratkaisuna yksityisyys- ja suostumuskysymyksiin, jotka ovat useassa yhteydessä nousseet massadatan ja tekoälyn hyödyntämisen keskeisiksi haasteiksi. MyData onkin nostettu esille yhtenä massadataa täydentävä osa-alueena valtioneuvoston strategisessa tutkimuksessa (Antikainen et al. 2016).

Koski ja Kanta: Toimialojen ratkaisut

Suomen julkishallinto on kehittämässä toimialakohtaisia järjestelmiä, joiden on tarkoitus helpottaa tiedon välitystä alan toimijoiden kesken. Kansallinen Terveysarkisto KanTa on valtakunnallinen järjestelmä, johon voi tallentaa mm. potilastietoja ja reseptejä siirtymään helposti terveyspalvelujen tarjoajalta toiselle. Omakanta, sähköinen terveystietojen ja reseptien hallinnan palvelu, tarjoaa mahdollisuuden omien tietojen tarkasteluun ja niiden siirron luvitukseen. Kehitteillä on myös Omatietovaranto, johon asiakkaat voivat tallentaa itse tuottamiaan terveys- ja hyvinvointitietoja. Uusi laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (asiakastietolaki) on paraikaa valmisteilla. Tällä hetkellä käyttäjillä ei kuitenkaan ole mahdollisuutta ladata tietoja omaan käyttöönsä tai itse valita, mitkä palvelut pääsevät niitä käyttämään. Terveydenhuollon MyDataan liittyvät myös käynnissä olevat potilastietojärjestelmähankkeet kuten Apotti ja Una.

Vastaavasti Koski-palvelu on opetushallituksen opintotietojen hallintaa selkeyttävä hanke. Sen tavoite on saada kansalaisten opintoja koskevat tiedot yhteen järjestelmään nykyisten, päällekkäisten rekisterien sijasta. Koskeen tallennettuja tietoja käyttävät alan ammattilaiset koulutuksen suunnitteluun, mutta myös opiskelijat voivat itse käyttää tietoja esimerkiksi opintojensa suunnitteluun ja työnhakuun. Järjestelmään onkin suunnitteilla keinot, joilla omia tietoja voi joustavasti siirtää eteenpäin muiden käyttöön.

Henkilötiedon käyttöön liittyvät ratkaisut voivat monissa tapauksissa syntyä ensin konkreettisten, yksittäisiä aloja koskevien tarpeiden ympärille. Samalla toimialakohtaiset järjestelmätkin tulisi rakentaa avoimilla standardeilla ja muut mahdolliset sovellukset mielessä, niin että järjestelmien laajempi yhteentoimivuus voidaan saavuttaa. Erilaiset keskitetyt rekisterit tehostavat toimintaa, mutta myös lisäävät tietovuotojen ja väärinkäytösten riskiä. Luottamuksen lisäämiseksi ne pitäisi suunnitella niin, että ihmiset itse voivat nähdä ja hallita omien tietojensa käyttöä sekä hyötyä itseään koskevasta tiedosta

Sitran Ihmislähtöinen datatalous IHAN®-hanke

Sitra rakentaa ekosysteemiä reiluun datatalouteen yhdessä kansalaisten ja eri toimijoiden kanssa. Hankkeessa laaditaan EU-tasoinen tiekartta reilulle datataloudelle. Tiedonvaihdannalle luodaan yhteiset pelisäännöt ja konsepti, kehitetään tekninen alusta sekä määritellään yhteiset standardit, periaatteet ja hallintamalli. Tekninen alusta perustuu avoimeen lähdekoodiin ja on sisällytettävissä erilaisiin teknisiin toteutuksiin. *”IHAN®-numero”* yksilöi henkilöön liittyvän tiedon internetissä.

Digital Health Revolution -hanke

Kun Digital Health Revolution (DHR) -hankkeen valmistelu alkoi vuonna 2013, henkilötiedoilla oli vähäinen asema terveyspolitiikkaa koskevissa keskusteluissa. Viime vuosina henkilötietojen käsittelyyn, hallintaan ja käytettävyyteen on kiinnitetty huomattavasti enemmän huomiota kansallisissa ja EU-tason keskusteluissa. DHR-hanke (2014-2018) on ollut edelläkävijä ihmiskeskeisen tiedonhallinnan tutkimuksessa ja uudentyyppisten ennaltaehkäisevien ja ennakoivien terveyspalvelujen kehityksessä.

DHR oli Tekesin rahoittama strateginen tutkimusavaus, jossa oli mukana monitieteinen joukko seitsemästä korkeakoulusta ja tutkimuslaitoksesta. Hanke tarjosi MyData-arkkitehtuurin kautta työkaluja kehittäjille, tutkimusta ihmiskeskeisistä liiketoimintamalleista ja niiden mahdollisuuksista terveydenhuollossa, ymmärrystä asiakas- ja käyttäjäkokemuksista sekä tietoa henkilötiedon hyödyntämisen juridisista ja eettisistä kysymyksistä. Lisäksi DHR-pilotissa kokeiltiin käytännössä, miten yksilökeskeinen ja dataintensiivinen terveyspalvelu voi luoda näkymää henkilön terveydentilaan.

Hanke edesauttoi MyDatan integroitumista valtakunnantason toimenpiteisiin ja oli osaltaan tukemassa kehitystä, jonka ansiosta Suomi tunnistetaan kansainvälisissä verkostoissa MyDatan ja yksilökeskeisen datan hallinnan edelläkävijänä. On selvää, että kehittämistoimia on jatkettava edelleen ja tavoiteltava kestävää yhteistoiminnan mallia henkilötiedon hallintaan ja jakamiseen Suomessa ja EU:ssa. Kehittäminen vaatii organisaatiorajat ylittävää ja vuoropuhelua ja luottamuksen rakentamista.

DHR:n tuloksia voidaan hyödyntää monissa muissa hankkeissa ja verkostoissa. Esimerkiksi keväällä 2018 Sitra on avannut uuden IHAN®-avainalueen, jolla pyritään vastaamaan henkilökohtaisen tiedon siirrettävyyden haasteeseen ja Business Finland on lanseerannut Personalized Health -ohjelman.

Kuva 5.2: Digital Health Revolution -hankkeen loppuraportti on ladattavissa osoitteesta **digitalhealthrevolution.fi**

Lähteet

Antikainen, Janne, Jarmo Eskelinen, Marc de Vries, Heli Koski, Tommi Niemi, Mika Pajarinen, and Pyykkönen Sinikukka. 2016. *"Massadatasta Liiketoimintaa Ja Tehokkaita Julkisia Palveluja."* http://tietokayttoon.fi/julkaisu?pubid=10701.

EU. 2016. *"EU:n Tietosuoja-Asetus."* 2016/679. https://eur-lex.europa.eu/legal-content/FI/TXT/HTML/?uri=CELEX:32016R0679.

EU. 2017. *"Staff Working Document on the Free Flow of Data and Emerging Issues of the European Data Economy."* https://ec.europa.eu/digital-single-market/en/news/staff-working-document-free-flow-data-and-emerging-issues-european-data-economy.

European Commission. 2017. *"Guidelines on the Right to Data Portability – Article 29 Data Protection Working Party."* https://ec.europa.eu/newsroom/document.cfm?doc_id=44099.

FTC. 2014. *"FTC Recommends Congress Require the Data Broker Industry to Be More Transparent and Give Consumers Greater Control Over Their Personal Information."* http://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more.

Goode, Lauren. 2017. *"Carnegie Mellon Researchers Want to Fix App Permissions Once and for All."* The Verge. The Verge. https://www.theverge.com/2017/2/10/14562514/cmu-privacy-assistant-app-mobile-app-permission.

Kantara. 2017. *"Consent Receipt Specification – WG - Consent & Information Sharing - Kantara Initiative."* https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification.

Knuutila, Aleksi, Vesa Kokkonen, Heikki Sundquist, Ossi Kuittinen, and Salla Thure. 2017. *"MyData Muutosvoimana: Julkishallinnon Henkilötiedon Ihmiskeskeisen Hyödyntämisen Mallit Ja Vaikutukset."* Valtioneuvoston kanslia. http://urn.fi/URN:ISBN:978-952-287-446-7.

Newman, Nathan. 2013. *"Taking on Google's Monopoly Means Regulating Its Control of User Data."* http://www.huffingtonpost.com/nathan-newman/taking-on-googles-monopol_b_3980799.html.

Pitkänen, Jyrki. 2018. *"Itsehallittavan Identiteetin Sääntely EUn Yleisessä Tietosuoja-Asetuksessa."* Lapin yliopisto, Oikeustieteellinen tiedekunta.

Pitkänen, Olli. 2014. *"Sinun Tietosi Eivät Ole Sinun: Rekisteröidyn Oikeus Hyödyntää Omia Henkilötietojaan."* Oikeus, no. 2/2014: 202–14.

Poikola, Antti, Kai Kuikkaniemi, and Ossi Kuittinen. 2014. *"My Data – Johdatus Ihmiskeskeiseen Henkilötiedon Hyödyntämiseen."* Ministry of Transport and Communications. http://urn.fi/URN:ISBN:978-952-243-418-0.

Searls, Doc. 2012. *The Intention Economy: When Customers Take Charge.* Harvard Business Press.

Sirkkunen, E., and P. Haara. 2017. *"Yksityisyys Ja Notkea Valvonta: Yksityisyys Ja Anonymiteetti Verkkoviestinnässä-Projektin Loppuraportti."* tampub.uta.fi. http://tampub.uta.fi/handle/10024/100510.

TEM. 2017. *"Suomen Tekoälyaika – Suomi Tekoälyn Soveltamisen Kärkimaaksi: Tavoite Ja Toimenpidesuositukset."* 41. Työ- ja elinkeinoministeriö. http://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/80849/TEMrap_41_2017_Suomen_tekoalyaika.pdf.

Valtioneuvosto. 2015. *"Ratkaisujen Suomi – Pääministeri Juha Sipilän Hallituksen Strateginen Ohjelma 29.5.2015."* http://valtioneuvosto.fi/documents/10184/1427398/Ratkaisujen+Suomi_FI_YHDISTETTY_netti.pdf.

Viitanen, Jukka, Reijo Paajanen, Valto Loikkanen, and Aki Koivistoinen. 2017. *"Digitaalisen Alustatalouden Tiekartasto."* Tekes. https://www.tekes.fi/globalassets/global/ohjelmat-ja-palvelut/kampanjat/alustatalous/alustatalouden_tiekartasto_web_x.pdf.

World Economic Forum. 2013. *"Unlocking the Value of Personal Data."* http://www.weforum.org/reports/unlocking-value-personal-data-collection-usage.

Ympäristöministeriö. 2014. *"Sähköisen Asunto-Osakerekisterin Toimintamalli."* http://www.ym.fi/download/noname/%7B76F44244-DE60-4B65-95F2-634D6A857096%7D/99026.

Avoimesti lisensoitu opas

Alkuperäisen selvitystyön ja sen englanninkielisen tiivistelmän (Poikola, Kuikkaniemi, & Honko, 2015; Poikola et al., 2014), sekä tämän päivitetyn suomenkielisen version (2017) on toteuttanut Open Knowledge Finland ry:n MyData-työryhmä. Alkuperäisen selvitystyön rahoitti liikenne- ja viestintäministeriö. Päivitystyön rahoitti TEKESin strateginen avaus Digital Health Revolution, jonka puitteissa työhön on osallistunut tutkijoita Aalto-yliopistosta, Tampereen teknillisestä yliopistosta ja Oulun yliopistosta.

Ulkoasu: **Kirmo Kivelä**

Toinen uudistettu painos.

ISBN 978-952-243-553-8
MyData – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen
Erillisjulkaisu (painotuote)

ISBN 978-952-243-554-5
MyData – johdatus ihmiskeskeiseen henkilötiedon hyödyntämiseen
Erillisjulkaisu (verkkojulkaisu)

Painopaikka Markprint
Lahti 2018


A
B C
€