TURUN YLIOPISTO

TIIVISTELMÄ

	Kandidaatintutkielma
X	Pro gradu -tutkielma
	Lisensiaatintutkielma
	Väitöskirja

Oppiaine	Tietojärjestelmätiede	Päivämäärä	15.6.2020
Tekijä	Kristian Dahlström	Sivumäärä	131
Otsikko	Yksityisyyden paradoksin yksilön aikeisiin ja käytökseen vaikuttavat tekijät		
Ohjaaja	Minna Rantanen		

Tiivistelmä

Digitalisaation myötä yksilöihin perustuva data on tuonut lukuisia uusia mahdollisuuksia organisaatioille. Datasta on muodostunut organisaatioille kriittinen menestystekijä, jonka avulla voidaan tehostaa liiketoimintaa ja saada kilpailuetua. Internetin laajenemisen myötä tiedonsiirron nopeus ja kustannukset ovat kokeneet rajuja muutoksia sekä tietoa on saatavilla poikkeuksellisen paljon ja helposti, niin yksilöille kuin organisaatioille. Kehityksellä on kuitenkin ollut myös vähemmän positiivisia vaikutuksia. Yksityisyyden suoja ja siihen liittyvät ongelmat ovat ajankohtaisempia kuin koskaan. Yksilöiden huolet ja pelot yksityisyyteen liittyen ovat olleet merkittävässä kasvussa, mutta tietoja luovutetaan siitä huolimatta valtavia määriä organisaatioiden käyttöön; yksilöiden yksityisyyteen liittyvissä aikeissa ja käyttäytymisessä esiintyy ristiriitaisuutta. Ilmiöstä käytetään nimitystä yksityisyyden paradoksi.

Yksityisyyden suojaan liittyvästä kehityksestä johtuen ja yksityisyyden paradoksin ollessa monimutkainen ja ajankohtainen ongelma, tässä tutkielmassa tarkastellaan yksityisyyden käsitettä ja sen kehitystä sekä paradoksin taustalla vaikuttavia tekijöitä. Tutkimus toteutettiin teoreettisesta näkökulmasta käsiteanalyyttisena tutkimuksena.

Yksityisyys on kehittynyt fyysisestä koskemattomuudesta yksilön halukkuudeksi ylläpitää henkilökohtaisten tietojen kontrollia ja edelleen moniulotteiseksi käsitteeksi, jonka yksi olennaisimmista tasoista on tietojen yksityisyys. Yksityisyyden kehitys on seurannut läheisesti informaatioteknologian kehitystä ja tietojen yksityisyyteen liittyvät havainnot ovat johtaneet yksityisyyden paradoksin havaitsemiseen.

Tutkielman lopputuloksena ja kontribuutiona kehitettiin uusi teoreettinen viitekehys yksityisyyden paradoksin yksilöiden aikeisiin ja käytökseen vaikuttavista tekijöistä. Aikaisempi tutkimus on tarkastellut paljon muun muassa privacy calculus -teorian ja suunnitellun käyttäytymisen teorian tarjoamia näkökulmia, mutta tieteellisessä tutkimuksessa on myös keskitytty kohtuullisesti ihmisiin liittyviin yksilöllisiin tekijöihin, persoonallisuuteen liittyviin piirteisiin sekä ympäristöön ja päätöksentekotilanteisiin liittyviin seikkoihin. Lopputuloksena viitekehyksestä voidaan huomata, että yksilöiden aikeita ja käytöstä selittää suuri joukko paitsi yhteisiä, mutta myös eroavia tekijöitä. Yksityisyyden paradoksin ratkaiseminen vaikuttaa tämän tutkielman johtopäätösten pohjalta poikkeuksellisen haastavalta ilmiöltä ratkaista.

Avainsanat	Yksityisyys, yksityisyyden paradoksi, yksityisyyden suoja, henkilökohtaiset tiedot, aikeet, käyttäytyminen

TURUN YLIOPISTO
Kauppakorkeakoulu

YKSITYISYYDEN PARADOKSIN YKSILÖN AIKEISIIN JA KÄYTÖKSEEN VAIKUTTAVAT TEKIJÄT

Tietojärjestelmätieteen
pro gradu -tutkielma

Laatija:
Kristian Dahlström

Ohjaaja:
Minna Rantanen

15.6.2020
Turku

SISÄLLYS

Kuvioluettelo

Taulukkoluettelo

1 JOHDANTO

1.1 Aiheen motivointi ja tausta

Dataa on luonnehdittu nykyaikaisessa digitalisoituneessa ja globaalissa maailmassa liiketoiminnan mahdollistajaksi. Jokainen organisaatio hyödyntää dataa toiminnassaan jollakin tavalla. Datan tarkoituksena on tallentaa reaalimaailmassa esiintyviä tapahtumia ja tilanteita esimerkiksi numeerisina arvoina, tekstinä tai kuvioina. Data on usein menneisyyteen perustuvaa ja dataa prosessoimalla sekä analysoimalla yritys voi luoda informaatiota tai tietämystä. Edelleen tietämyksellä ja informaatiolla voidaan tehostaa organisaation prosesseja. Data ei ole pelkästään muuttanut liiketoimintaympäristöä, organisaatioiden välistä kilpailukenttää tai yrityksien tehokkuutta radikaalisti, vaan se on synnyttänyt täysin uudenlaista liiketoimintaa ja osaltaan myös luonut uudenlaisia velvollisuuksia organisaatioille. (Liew 2007; Zins 2007, 479–480.)

Internetin kehityksen ja laajenemisen myötä tiedonsiirron kustannukset ovat alentuneet ja nopeudet kasvaneet. Internet on kehittynyt yhä enenevissä määrin kohti niin sanottua Web 2.0 -toimintamallia, jossa korostuu yksilöiden ja verkon käyttäjien luoma sisältö, tiedonjako ja kommunikointi. Käyttäjien osallistuminen sisällön tuottamiseen tai tietojen jakamiseen on keskeistä muun muassa yhteisöllisillä internetsivuilla ja verkkokaupoissa. Sisällöntuotanto ja informaation tarjoaminen eivät enää keskity pelkille yrityksille tai suurille yhteisöille. Tietoa on saatavilla suuria määriä organisaatioiden lisäksi myös verkon käyttäjille, ajasta ja paikasta riippumatta. (Dinev ym. 2009, 1.) Datan muodostamien monipuolisten verkostojen ja kokonaisuuksien yhteydessä on alettu puhumaan muun muassa datataloudesta ja datatalouden ekosysteemeistä, joissa data on toiminnan keskipisteessä. Siinä missä datatalous viittaa laajemmin ihmisten ja teknologian muodostamaan suureen kokonaisuuteen, datatalouden ekosysteemeillä tarkoitetaan eri osapuolten ja sidosryhmien muodostamaa kompleksia verkostoa, jolle data muodostaa liiketoiminnan ytimen. Verkostoissa ovat omat sääntönsä ja arvoketjunsa, jotka edesauttavat ekosysteemin toimintaa. (Koskinen ym. 2019, 329–330; Rantanen 2019, 27, 29.)

Organisaatioiden hyödyntäessä yhä enenevissä määrin ihmisiin perustuvaa dataa, joka voi joskus olla jopa hyvinkin yksityiskohtaista ja arkaluontoista, julkisen keskustelun ja laajan tutkimuksen keskiössä ovat olleet huolet ihmisten yksityisyydestä, tietosuojasta ja tietoturvasta. Dataa kerätään muun muassa erilaisten yrityksien ja yhteisöjen toimesta muun muassa tutkimuskäyttöön, palvelujen ja tuotteiden personointia sekä erilaisia

tietokantoja varten. Personoinnilla tarkoitetaan organisaation tarjonnan räätälöimistä paremmin yksittäisten ihmisten toiveita ja tarpeita vastaaviksi. (Chellappa & Sin 2005, 181–182, 186.) Data toimii siis eräänlaisena vaihdon välineenä; ihmiset luovuttavat organisaatiolle dataa ja he saavat vaihdossa jonkinlaisia hyötyjä. Joidenkin tutkijoiden mukaan yksityisyys voidaan nähdä eräänlaisena hyödykkeenä tai maksuvälineenä. (Wilson & Valacich 2012, 2–3.) Yksilöt tyypillisesti suorittavat, tiedostetusti tai tiedostamatta, vertailua heikentyneen yksityisyyden ja tietojenluovutuksella saatujen hyötyjen välillä (Kokolakis 2015, 128).

Organisaatiot voivat hyödyntää parempaa yksityisyyden suojaa myyntivalttina tai jopa kilpailuedun mahdollistajana, sillä osa kuluttajista voi olla valmiita maksamaan preemion paremmasta yksityisyydestä (engl. privacy premium). Ihmisten tuottamalla datalla onkin arvoa, mutta itse datan arvonmääritys on haasteellista. Koska yksilöt eivät voi kontrolloida mitä tiedonkerääjät tekevät datalla, yksilöt voivat sen sijaan kontrolloida ketkä ulkopuoliset saavat henkilökohtaisia tietoja käytettäväksi. (Tsai ym. 2011, 266–267.) Henkilökohtaisten tietojen luovutusta liittyy muun muassa verkkokaupoissa asiointiin, verkkopankin käyttöön, julkisten toimijoiden sähköisten palveluiden hyödyntämiseen ja sosiaaliseen mediaan (Li ym. 2010, 62). Sosiaalisella medialla tarkoitetaan verkossa olevia ympäristöjä, joissa käyttäjät luovat itsestään profiilin luovuttamalla henkilökohtaisia tietojaan ja profiiliensa avulla käyttäjät voivat verkostoitua alustalla muiden käyttäjien kanssa (Young & Quan-Haase 2013, 481). Sosiaalinen media on hyvä esimerkki siitä, miten teknologian kehittymistä usein varjostaa suuri määrä uudenlaisia riskejä ja ongelmia. Sosiaalinen media on laajasti käytetty työkalu ja alusta erityisesti vapaa-ajalla ihmissuhteiden luomiseen ja ylläpitämiseen, mutta sosiaalinen media on tuonut yksityisyyden suojan heikkenemisen arkipäiväiseksi ongelmaksi. (Hallam & Zanella 2017, 217.)

Tiedonkeruu voi tapahtua ihmisen tietämättä tai tiedostamatta muun muassa evästeiden avulla tai avoimesti, jolloin ihmiset itse luovuttavat tietojaan tietoisesti esimerkiksi verkkokyselyn tekstikenttään (Aguirre ym. 2015, 34–36). Ihmisten välillä on merkittäviä eroja sen suhteen mitä tietoja he haluavat tai eivät halua luovuttaa ulkoisille tahoille, eli toisin sanoen siinä, miten he aikovat käyttäytyä. Tämän lisäksi ihmiset käyttäytyvät yksityisyyteen liittyvissä toimenpiteissä ja tilanteissa eri tavoin. Sekä tutkimuksissa että käytännön tilanteissa on osoittautunut, että näiden aikeiden ja käytöksen välillä on usein merkittäviä eroja myös yksittäistä ihmistä tarkastellessa. Tätä kuilua yksilön aikeiden ja

käytöksen välillä nimitetäänkin yleisemmin yksityisyyden paradoksiksi (engl. privacy paradox). Aikeet voidaan määritellä lyhyesti yksilön halukkuudeksi suorittaa jokin tietty ennalta määritelty käytös. Käytös taas puolestaan viittaa tilanteisiin, joissa yksilö suorittaa tiettyä toimintaa tai tekee ratkaisuja erilaisissa päätöksentekotilanteissa. (Norberg ym. 2007, 100–101.) Yksityisyyteen liittyvä käytös voidaan taas jakaa edelleen rationaaliseen ja irrationaaliseen käyttäytymiseen (ks. esim. Wilson & Valacich 2012). Muun muassa Joinson ym. (2006) ja Kehr ym. (2015, 608) korostavat päätöksenteon psykologista näkökulmaa ja tilanneriippuvaisuutta.

Ymmärrys yksityisyyden paradoksista on nykyään laajempaa kuin aikaisemmin kasvavan tieteellisen tutkimuksen ansiosta. Yksityisyyden paradoksin ollessa monimutkainen ja ajankohtainen ilmiö digitalisoituneessa maailmassa, aihe vaatii kuitenkin yhä enemmän tutkimusta. Yksityisyyden paradoksi on terminä ristiriitainen, sillä ilmiöön liittyy laaja-alaista ymmärrystä ja useita potentiaalisia loogisia selityksiä, mutta myös paljon erimielisyyksiä, epävarmuutta ja epäselviä seikkoja. Yksityisyyden paradoksia on kuvailtu muun muassa eräänlaisena valtavana palapelinä; tiedonpalaset ovat olemassa, mutta niitä on ollut mahdotonta yhdistää toisiinsa kokonaisen kuvan muodostamiseksi. (Kokolakis 2015, 122, 130–132.)

Barthin ja de Jongin (2017) artikkeli osoittaa, että vaikka yksityisyyden paradoksi on saanut osakseen runsaasti huomiota tutkimuksissa niin esimerkiksi käytännön keinoja yksityisyyden paradoksin ratkaisemiseksi, eli aikeiden ja käyttäytymisen välisen kuilun sulkemiseksi tai selittämiseksi, ei ole vielä löytynyt. On siis selvää, että ilmiön monimutkaisuudesta, ristiriitaisuuksista ja epäselvyyksistä johtuen aihe vaatii osakseen syvällisempää ja tarkempaa tutkimusta.

1.2 Tutkimuskysymykset ja rajaus

Organisaatioiden datankeruusta ja yksityisyyteen liittyvistä päätöksistä on tullut kiinteä osa yksilöiden elämää modernissa tietoyhteiskunnassa. Esimerkiksi verkkokauppoja, sosiaalista mediaa ja muita verkkosivustoja tai -alustoja käytetään jopa päivittäin. Yksityisyyden käsite on kokenut suuria muutoksia ajan saatossa erityisesti teknologisen kehityksen myötä ja yksityisyys on aihealueena ajankohtainen muun muassa datankeruun kasvun, tieteellisen tutkimuksen, lainsäädännöllisten muutosten ja julkisen keskustelun vuoksi. Koska yksityisyys ei ole käsitteenä täysin selkeä ja yksityisyyden käsitteen ymmärtäminen on keskeinen osa myös yksityisyyden paradoksiin liittyvää tutkimusta, on

keskeistä tarkastella ja analysoida yksityisyyden suojan määritelmää ja sen kehityskulkua.

Yksityisyyden paradoksi on noussut keskeisemmäksi ilmiöksi varsinkin internetiin ja yksityisyyteen liittyvän kehityksen vuoksi. Vaikka yksityisyyden paradoksiin liittyvä ristiriita yksityisyyttä koskevien aikeiden ja käytöksen välillä ilmeneekin yksilöissä, on paradoksilla vaikutuksia myös ulkopuolisiin. Organisaatioiden toiminnan ollessa yhä enemmän riippuvaista yksilöiltä kerättävästä datasta, voi yksilön ristiriitaisella, arvaamattomalla tai odottamattomalla käytöksellä olla vaikutuksia organisaatioiden menestymiseen. Ilman riittävää tai oikeanlaista dataa liiketoiminnan harjoittaminen voi vaikeutua tai estyä kokonaan. Myös viranomaisten toiminta edellyttää yhä useammin yksilöiltä kerättäviä tietoja. Koska paradoksi perustuu yksilöiden aikeiden ja käytöksen eroavaisuuksiin, herää kysymys muun muassa siitä, voisivatko aikeita ja käytöstä selittävät tekijät toimia apuna paradoksin ymmärtämisessä ja selittämisessä. Yksityisyyden paradoksin syvällisemmän ymmärryksen lisäämiseksi **tämän tutkielman lähtökohtaisena päätutkimusongelmana ja tarkoituksena on tarkastella sitä, miksi yksilön aikeet ja käyttäytyminen yksityisyyden suhteen eroavat usein toisistaan**. Päätutkimusongelmaan vastaamista ja aihealueen tarkastelua varten tutkielmassa vastataan myös kahteen seuraavaan alatutkimuskysymykseen:

- Mitä yksityisyydellä tarkoitetaan ja miten yksityisyyden käsitteen merkitys on muuttunut?
- Minkälaiset tekijät vaikuttavat yksilöiden aikeisiin ja käyttäytymiseen henkilökohtaisten tietojen luovutuksessa?

Tutkielmassa tullaan keskittymään ensisijaisesti tiedonluovuttajan eli yksilön näkökulmaan ja keskiössä on erityisesti verkossa toimiville organisaatioille tapahtuva henkilökohtaisten tietojen tiedonluovutus ja yksityisyyttä suojaavien toimenpiteiden suorittaminen digitaalisissa ympäristöissä. Yksityisyyden suojaan ja datan keräämiseen liittyvät teknologiset ja tekniset ratkaisut sekä lainsäädännölliset seikat jäävät rajauksen vuoksi vähäisemmälle huomiolle. Esimerkiksi lainsäädännössä esiintyy huomattavasti eroja eri valtioiden välillä, eikä tämän tutkielman tarkoituksena ole tarkastella yksityisyyttä ja siihen liittyviä ongelmia lainsäädännöllisestä näkökulmasta. Tutkielmassa kuitenkin käsitellään lyhyesti aiheen ja tutkimusongelman näkökulmasta merkittäviä lainsäädännöllisiä ydinkohtia ja yksilön henkilökohtaisten tietojen keräämisen ymmärtämisen kannalta olennaisimpia teknologisia näkökulmia.

Tämän tutkielman tavoitteena on luoda katsaus yksityisyydestä ja yksityisyyden paradoksista olemassa olevaan tieteelliseen kirjallisuuteen ja tutkimukseen. Tutkimus on toteutettu teoreettisena ja tulkitsevana käsittelyanalyyttisena tutkimuksena. Käsiteanalyysillä tarkoitetaan tutkimuksen aiheen pohjalta tapahtuvaa keskeisten käsitteiden ja niiden välisten suhteiden analyysiä ja selittämistä (koppa.jyu.fi). Tulkitsevassa käsitetutkimuksessa pyritään tulkitsemaan ja kuvailemaan käsitteiden merkitysten muodostamaan kokonaisuutta ja paljastamaan ilmiöiden taustalla olevia merkityksiä (Lämsä & Takala 2004). Koska yksityisyyteen ja yksityisyyden paradoksiin liittyvät käsitteet ja niiden väliset suhteet eivät ole tieteellisessä tutkimuksessa saavuttaneet universaaleja tai yksittäisiä ja tarkkoja määritelmiä, käsiteanalyyttinen lähestymistapa on hyödyllinen ilmiön syvällisemmässä ymmärtämisessä, tulkitsemisessa ja selittämisessä. Tutkielmassa tarkastellaan tieteellisen kirjallisuuden ja artikkelien valossa yksityisyyden paradoksiin aikeisiin ja käytökseen vaikuttavia tekijöitä. Tämän tutkielman tieteellisenä kontribuutiona on aikaisempien tutkimusten pohjalta muodostettava yksityisyyden paradoksin aikeita ja käytöstä selittävä sekä kuvaava teoreettinen viitekehys. Aikaisemmissa tutkimuksissa kehitetyt ja luodut viitekehykset paradoksin taustalla vaikuttavista tekijöistä ovat olleet hajanaisia tai usein keskittyneitä ainoastaan joko aikeisiin tai käytökseen. Aikaisempien mallien ja teorioiden väliset yhtäläisyydet, eroavaisuudet ja ristiriitaisuudet on myös otettava huomioon viitekehystä muodostettaessa. Yksityisyyden paradoksiin vaikuttavien tekijöiden tarkasteleminen ja ymmärtäminen on edellytys päätutkimusongelmaan vastaamiseen.

Lähteinä tutkielmassa on käytetty tieteellisiä artikkeleita ja muita kirjallisia teoksia. Tutkielmassa hyödynnetään myös muutamia verkkolähteitä, mutta ainoastaan joidenkin käsitteiden määrittelyn ja tarkastelun yhteydessä. Tässä tutkielmassa kehitettävään viitekehykseen hyödynnettävät lähteet ovat vuosien 2006 ja 2020 välillä tai aikana julkaistuja teoksia tai artikkeleita, jotka keskittyivät pääasiallisesti tai keskeisesti selittämään yksityisyyden paradoksia, siihen liittyviä aikeita, käytöstä tai päätöksentekoprosesseja. Koska yksityisyyden paradoksi tunnistettiin tieteellisenä ongelmana ja ilmiönä vasta vuonna 2006, eivät ennen tätä ajankohtaa julkaistut tutkimukset liity yksityisyyden paradoksin ratkaisemiseen tai selittämiseen.

Koska yksityisyyden paradoksi on monimutkainen ja laaja ilmiö, tässä tutkielmassa kehitettävästä viitekehyksestä jätettiin pois aikeisiin ja käytökseen välillisesti vaikuttavat tekijät, vaikuttavien tekijöiden väliset suhteet ja vaikuttavien tekijöiden taustalla vaikuttavat tekijät, sillä tutkielman tarkoituksena on esittää juuri yksityisyyden paradoksin aikeisiin ja käytökseen suoraan vaikuttavat tekijät.

1.3 Tutkielman rakenne

Tämä tutkielma jakaantuu viiteen päälukuun. Ensimmäisen pääluvun eli johdannon jälkeen toisessa pääluvussa tarkastellaan ja määritellään tutkielman kannalta keskeisimpiä käsitteitä, ilmiöitä ja teorioita. Toisessa pääluvussa aihealueina ovat pääasiassa yksityisyys ja sen kehittyminen, yksityisyyden paradoksi ja yksilöistä kerättävään dataan liittyvät seikat. Kolmannessa pääluvussa tarkastellaan tieteellisessä kirjallisuudessa ja artikkeleissa esiteltyjä malleja, tutkimuksia, teorioita ja viitekehyksiä yksityisyyden paradoksista ja siihen vaikuttavista tekijöistä. Neljännes pääluvussa esitetään tutkielman johtopäätökset, vastaukset tutkimuskysymyksiin ja havainnollistetaan tutkielman lopputulemana kolmannen pääluvun pohjalta rakennettu teoreettinen viitekehys. Tämän lisäksi neljännessä pääluvussa esitetään tähän tutkimukseen liittyviä rajoitteita, annetaan suosituksia tulevaisuuden tutkimusta varten ja pohdintoja aiheeseen liittyen. Tutkielman viidennessä eli viimeisessä pääluvussa esitetään yhteenveto tutkielmasta ja sen tuloksista. Tutkielman loppuun on kerätty tutkimuksessa hyödynnetty lähdemateriaali ja liitteet.

2 TEOREETTINEN TAUSTA

2.1 Yksityisyys käsitteenä

Tieteellisissä tutkimuksissa yksityisyys on laaja-alainen käsite ja yksityisyyden määritelmä on muuttunut merkittävästi ajan saatossa. Yksityisyyden eri määritelmät kiinnittävät huomiota eri osa-alueisiin eikä yksityisyydelle ole yhtä selkeää tai vakiintunutta määritelmää. Juuret yksityisyyden käsitteessä ovat Yhdysvalloissa vuonna 1890 Warrenin ja Brandeisin kirjoittamassa artikkelissa ”The Right to Privacy”. (Bratman 2002, 623–625.)

Warrenin ja Brandeisin (1890) mukaan yhteiskunnan laajan poliittisen, taloudellisen ja sosiaalisen kehityksen myötä pelkästään yksilön fyysisen koskemattomuuden ja omaisuuden turvaaminen ei enää riitä, vaan yksilön oikeuksien on oltava laajemmat. Ihmisten aineettomien ja henkisten ominaisuuksien sekä laajojen kansalaisoikeuksien turvaaminen tulisi ottaa huomioon lakien säätämisessä. Eräänlaiseksi yksityisyyden käsitteen kivijalaksi on muodostunut Warrenin ja Brandeisin (1890) toteamus siitä, että yksilöllä on oltava oikeus olla rauhassa ja yksin. Myös omaisuuden käsitteen kehityksen myötä yksilön aineettomien ominaisuuksien ja kykyjen nähtiin olevan keskeinen osa yksilön omaisuutta ja yksityisyyttä myös lainsäädännön näkökulmasta. Muun muassa yksilön tunteiden, älykkyyden, tietämyksen, yksityisyyselämän ja ihmissuhteiden turvaamisen merkitys tunnistettiin osana ihmisten oikeutta yksityisyyteen. (Warren & Brandeis 1890, 193–195.)

Gavison (1980) määrittelee artikkelissaan täydellisen yksityisyyden tilanteeksi, jossa ihminen saa olla fyysisesti täysin rauhassa, häneen ei kiinnitetä minkäänlaista huomiota eikä kenelläkään ole tietoa hänestä. Artikkelin mukaan tämänkaltainen täydellinen yksityisyys on käytännössä kuitenkin mahdotonta saavuttaa. Täydellinen yksityisyys ei ole lähtökohtaisesti edes toivottu tilanne, sillä yhteiskunnan toiminta ja yksilön elämä edellyttävät ihmisten välistä vuorovaikutusta. Gavisonin (1980) mukaan yksityisyyden käsitteen olemassaolo on keskeistä kolmen näkökulman pohjalta. Ensinnäkin, yksityisyyden käsitteen avulla voidaan tunnistaa ja tulkita yksilön yksityisyyden suojan menetystä tai vähenemistä. Toiseksi, yksityisyydellä voidaan nähdä olevan arvoa ja yksityisyyden menettäminen voi tästä syystä aiheuttaa haittoja yksilöille. Kolmanneksi, yksityisyyden suojan turvaamiseksi yksityisyyden tulee olla sovellettavissa oikeudellisissa ja lainsäädännöllisissä tilanteissa. Gavisonin (1980) mukaan yksityisyys koostuu kolmesta seuraavasta osa-alueesta:

1. Eristäytyneisyys eli ulkopuolisten mahdollisuus olla yksilön fyysisessä läheisyydessä tarkkailemassa yksilöä (engl. solitude).
2. Anonyymius eli kuinka paljon yksilöön kiinnitetään huomiota tai kuinka paljon yksilöstä yritetään saada tietoa (engl. anonymity).
3. Salaperäisyys eli mitä ja kuinka paljon ulkopuoliset tietävät tietystä yksilöstä (engl. secrecy).

Yksityisyyttä voidaan siis rikkoa yksilön näkökulmasta näillä osa-alueilla, mutta yksityisyyden menetys yhdellä osa-alueella ei välttämättä koske muita osa-alueita, sillä Gavisonin (1980) mukaan osa-alueet ovat toisistaan riippumattomia ja erillisiä. Tämä ei kuitenkaan poissulje tilanteita, joissa useampi osa-alue tai kaikki kolme osa-aluetta voivat olla samalla aikaa läsnä. Esimerkiksi terveydenhuollossa on tyypillistä, että hoitohenkilöstö on potilaan fyysisessä läheisyydessä, potilas on huomion keskipisteenä ja potilaasta on kerätty ja kerätään henkilökohtaisia tietoja. (Gavison 1980, 421–434, 440.)

Westin (2003) puolestaan määrittelee yksityisyyden yksilön haluksi ja vaatimukseksi päättää siitä, mitä tietoja ulkopuoliset hänestä tietävät. Itse tietojen lisäksi yksityisyyteen kuuluvat myös tiedonhankinta ja tietojen käyttäminen. Westin (2003) määrittelee yksityisyyden olevan tarkasteltavissa kolmella eri tasolla: poliittisella, sosiokulttuurisella ja yksilön tasolla. Poliittisella tasolla keskeistä ovat tarkkailun ja yksityisyyden oikean tasapainon löytäminen liiketoiminnan ja demokratian vastuullisen toteutuksen turvaamiseksi. Poliittisella tasolla viranomaisten suorittamaa tarkkailua ja tiedon keräämistä perustellaan laittomien toimien ennaltaehkäisemisellä. Poliittinen taso toimii myös pohjana seuraavalle yksityisyyden tasolle. Sosiokulttuurisella ja organisatorisella tasolla keskiössä ovat yksilön sosiaalinen asema ja status yhteiskunnassa. Korkeassa asemassa olevilla tai varakkailla yksilöillä on lähtökohtaisesti paremmat mahdollisuudet vetäytyä syrjään, mutta toisaalta korkeissa asemissa olevien ihmisten yksityisyyttä loukataan ja häiritään myös tyypillisesti enemmän. Sosiokulttuurinen taso huomioi myös toiminnan hyväksyttävyyden; mitä hyväksyttävämpää yksilön toiminta on, sitä tyypillisempää on luokitella toiminta yksityisyyden suojan piiriin. Sosiokulttuurisen tason pohjalta muutokset yhteiskunnan normeissa vaikuttavat yksilöiden yksityisyyden suojaan. Tällä kolmannella eli yksilön tasolla yksityisyys liittyy ihmisen päivittäiseen kommunikointiin ja elämään. Siinä missä Gavison (1980) määritteli yksilön yksityisyyden muodostuvan kolmesta osa-alueesta, Westin (2003) jakaa yksilön yksityisyyden neljään osa-alueeseen. Nämä neljä osa-aluetta ovat eristäytyneisyys (engl. solitude), anonyymiys (engl. anonymity), intiimiys (engl. intimacy) ja varautuneisuus (engl. reserve). (Westin 2003, 431–434.)

Westinin (2003) ja Gavisonin (1980) osa-alueet ovat lähellä toisiaan, mutta Gavisonin (1980) määritelmän salaperäisyys on korvattu Westinin (2003) määritelmässä intiimiydellä ja varautuneisuudella. Westinin (2003) määritelmän pohjalta toisessa ääripäässä yksilö haluaa olla yksin täydessä rauhassa ja eristäytyä kaikelta kommunikoinnilta, kun taas toisessa ääripäässä yksilö haluaa kommunikoida tuntemansa ihmisen kanssa henkilökohtaisista asioistaan. Yksilön tasolla Westin (2003) myös korostaa yksilön sosiaalisten ja muiden tarpeiden jatkuvaa vaihtelua, joten näiden neljän osa-alueen välinen tasapaino on jatkuvassa muutoksessa ja yksityisyydessä keskeistä onkin yksilön mahdollisuus vaikuttaa oman yksityisyyden suojan tasoonsa ja osa-alueiden väliseen tasapainoon. (Westin 2003, 431–434.)

Yksityisyys nähdään usein ennen kaikkea moraalisena ja lakisääteisenä oikeutena, mutta Clarke (1999) esittää yksityisyydessä pääasiassa olevan kyse yksilöiden halukkuudesta ylläpitää ja suojella henkilökohtaista tilaa ulkopuolisten huomiolta ja häirinnältä. Tämän henkilökohtaisen tilan nähdään koostuvan paitsi fyysisestä rauhasta, mutta myös oman käytöksen, henkilökohtaisten tietojen ja kommunikoinnin yksityisyydestä. Internetin yleistymisen ja digitalisaation myötä datan keräämisen ja käytön yleistyminen ovat osaltaan vaikuttaneet yksityisyyden käsitteen muutokseen ja uusien näkökulmien ilmenemiseen. Clarke (1999) kuvailee lisäksi artikkelissaan tietojen yksityisyyden (engl. information privacy) käsitteen tarkoittavan yksilöön liittyvän datan rajoitettua saatavuutta ulkopuolisille henkilöille tai organisaatioille ja yksilön mahdollisuuksia vaikuttaa hänestä kerätyn datan hyödyntämiseen. Tietojen yksityisyys ja internetissä yksilöistä kerätty data mahdollistaa organisaatioille tehokkaan profiloinnin ja yksilöiden ajatuksiin sekä käytökseen vaikuttamisen. Tietojen yksityisyyden merkityksen korostuessa fyysinen vakoilu onkin muuttunut enemmän digitaaliseksi tarkkailuksi ja ilmiötä on nimitetty osuvasti dataan liittyväksi vakoiluksi (engl. dataveillance). Yksityisyyden osalta keskipiste on siirtynyt fyysisen rauhan turvaamisesta tietojen yksityisyyden suojeluun. (Clarke 1999, 60–61, 66.)

Tietojärjestelmätieteen kirjallisuudessa tutkimuksen keskiössä on ollut tietojen yksityisyyden käsite ja fyysinen yksityisyys on usein jätetty pois tarkastelusta tai vähäiselle huomiolle. Bélanger ja Crossler (2011) määrittelevät tietojen yksityisyyden tarkoittavan yksittäisen ihmisen mahdollisuuksia vaikuttaa hänestä kerättyjen tietojen toissijaiseen käyttöön. Toissijaisella käytöllä tarkoitetaan tilannetta, jossa yksilöistä kerättyjä tietoja käytetään eri käyttötarkoituksiin kuin mitä varten tiedot ensisijaisesti kerättiin. Koska nykyään kommunikointi on pitkälti digitaalista ja se tallentuu digitaalisena datana, voidaan

tietojen yksityisyyden ajatella koostuvan henkilökohtaisen kommunikoinnin ja datan yksityisyydestä. (Bélanger & Crossler 2011, 1017–1018.)

Smith ym. (2011) tiedostavat artikkelissaan yksityisyyden käsitteen monimuotoisuuden. Heidän mukaansa yksityisyyttä voidaan tarkastella useasta näkökulmasta, muun muassa yksilön oikeutena, omien tietojen kontrollimahdollisuutena, hyödykkeenä tai saavutettavana olotilana. Tietojen yksityisyyden käsitteen kehitys on liittynyt läheisesti informaatioteknologian eli IT:n kehitykseen. Huolet ja riskit tietojen yksityisyyden suojasta ovat merkittävässä kasvussa IT:n kehityksen myötä paitsi yksilöiden, myös viranomaisten ja organisaatioiden liikkeenjohdon keskuudessa; esimerkiksi jopa 72 prosenttia kuluttajista ovat huolissaan oman toimintansa jäljittämisestä. Erityisesti tietokoneiden ja internetin yleistyminen ovat edesauttaneet negatiivisten seurausten parempaa hahmottamista ja tiedostamista. (Smith ym. 2011, 992–995.) Yksityisyyden käsitteen kehityksen ajanjaksot ja ajanjaksojen keskeiset piirteet esitellään taulukossa 1.

Taulukko 1. Tietojen yksityisyyden käsitteen kehittyminen

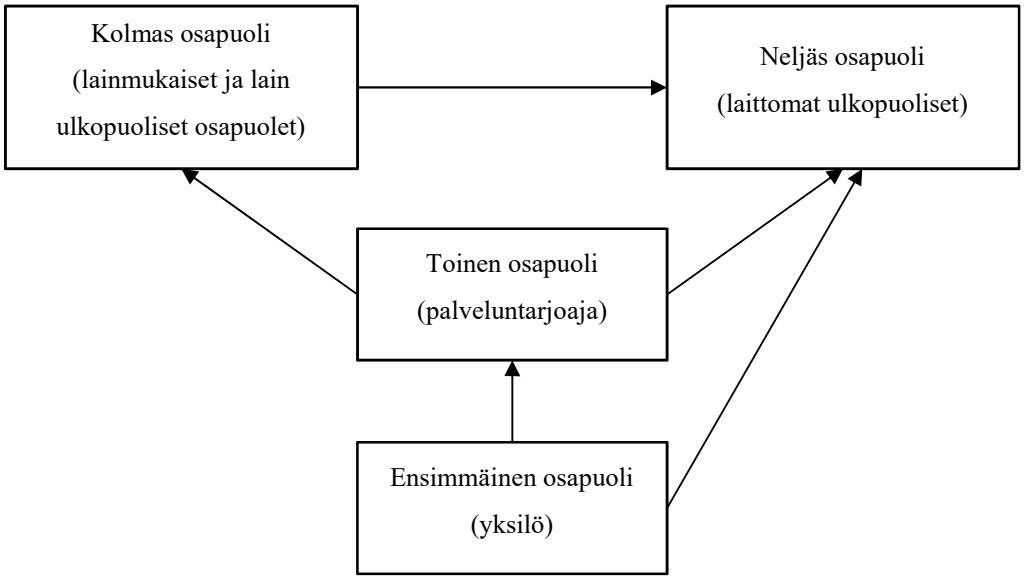
Tietojen yksityisyyden käsitteen kehityksen yhteys informaatioteknologian kehitykseen (Westin 2003; Smith ym. 2011)	
Ajanjakso	Ajanjakson piirteitä
Yksityisyyden käsitteen lähtötilanne 1945–1960	IT:n kehitys on maltillista. Luottamus julkisiin toimijoihin ja yrityksiin on korkealla tasolla sekä tietojen kerääminen yleisesti hyväksyttyä. Yksityisyyttä ei tunnisteta sosiaalisena tai poliittisena ongelmana ja yksityisyyden suojan rikkomukset ovat yleisiä.
Ensimmäinen yksityisyyden kehityskausi 1961–1979	Yksityisyys tunnistetaan selkeänä poliittisena, lainsäädännöllisenä ja sosiaalisena haasteena. IT:n kehityksen haittapuolien ja riskien hahmottaminen, uusien vakoilu- ja tarkkailuteknologioiden yleistyminen. Yhdysvalloissa reilujen tietokäytäntöjen (engl. Fair Information Practices, FIP) muodostaminen ja muiden yksityisyyteen liittyvien säännösten ja lainsäädännön kehittyminen.
Toinen yksityisyyden kehityskausi 1980–1989	Tietokoneiden, tietokantojen ja tietoverkkojen yleistyminen. Euroopassa kansallisten tietosuojalakien säätäminen julkisille ja yksityisille sektoreille yksilön oikeuksien turvaamiseksi.
Kolmas yksityisyyden kehityskausi 1990–	Internetin yleistyminen, tiedonlouhinta, Web 2.0 ja salausteknologioiden kehittyminen. Yksityisyyshuolten ja -riskien kasvaminen, identiteettivarkauksien yleistyminen. Yksityisyydestä korkean tason globaali, sosiaalinen ja poliittinen ongelma. Matkapuhelimien ja muiden langattomien sekä dataa keräävien laitteiden yleistyminen. Yksityisyyden painopiste yksilöiden henkilökohtaisten tietojen yksityisyyden suojeluun.

Kontekstista ja yksilöstä riippuen yksityisyyden optimaalinen, saavutettu ja toivottu taso voivat vaihdella merkittävästi. Tähän nojaten Trepte ym. (2014) määrittelevätkin yksityi-

syyden prosessiksi, jonka tavoitteena on pyrkiä optimoimaan ja tasapainottamaan yksityisyyden eri tasoja tilanteesta riippuen. Tasoja on neljä: tietojen, sosiaalinen, psykologinen ja fyysinen yksityisyys. Tietojen yksityisyys tarkoittaa yksilön itsestään liittyvän tiedon määrän, vastaanottajien ja sisällön kontrollointia. Sosiaalinen yksityisyys viittaa henkilön mahdollisuuksiin kontrolloida sosiaalista kanssakäymistä sekä sosiaalisia kohtaamisia ja suhteita. Yksilön kykyä kontrolloida omien kognitiivisten viestien viestimistä ja muiden kognitiivisten viestien vastaanottoa nimitetään psykologiseksi yksityisyydeksi. Psykologinen yksityisyys on toisin sanoen korkealla tasolla, kun yksilö pystyy vapaasti sekä valitsemaan mitä tietoa ilmaisee itsestään että halutessaan välttämään ja valikoimaan ulkopuolisten ihmisten kommunikointia. Viimeinen osa-alue, fyysinen yksityisyys, tarkoittaa henkilön fyysistä koskemattomuutta ja oman fyysisen tilan häiritsemättömyyttä. (Trepte ym. 2014, 3–4.)

Kokolakis (2015) puolestaan jakaa yksityisyyden kolmeen osa-alueeseen. Alueellisella yksityisyydellä (engl. territorial privacy) tarkoitetaan yksilöä ympäröivän alueen fyysistä häiritsemättömyyttä. Henkilön yksityisyys (engl. privacy of a person) puolestaan viittaa yksilön fyysiseen koskemattomuuteen. Tietojen yksityisyys (engl. informational privacy) tarkoittaa sitä, miten yksilöt voivat kontrolloida mitä ja kuinka paljon henkilökohtaisia tietoja ulkopuoliset henkilöt voivat kerätä, varastoida, prosessoida ja levittää yksilöön liittyen. Verkossa luonnollisesti korostuu lähinnä tietojen yksityisyys. (Kokolakis 2015, 123.) Myös Hallam ja Zanella (2017, 218) hyödyntävät yksilön intresseihin ja kontrolliin perustuvaa määritelmää yksityisyydestä: yksityisyys tarkoittaa heidän mukaansa yksilön kiinnostusta ja halua kontrolloida tai vaikuttaa heitä koskevan datan käsittelyyn.

Conger ym. (2013) nostavat puolestaan esiin artikkelissaan henkilökohtaisten tietojen yksityisyyden käsitteen (engl. Personal Information Privacy, PIP). Heidän mukaansa henkilökohtaisten tietojen yksityisyys tarkoittaa yksilön toiveita pitää tiettyjä tietoja pois ulkopuolisten saatavilta. Artikkelissa esitetään myös mallia yksityisten tietojen luovuttamiseen ja leviämiseen, joka ottaa huomioon yksityisyyden suojan säilymisen monimutkaisuuden sekä luvallisen ja luvattoman tietojen käyttämisen. (Conger ym. 2013, 401–404.) Malli esitetään kuviossa 1.



Kuvio 1. Malli yksityisyyteen liittyvistä osapuolista (Conger ym. 2013)

Congerin ym. (2013) mallissa tiedot omistava ja niitä luovuttava yksilö on ensimmäinen osapuoli, tietoja keräävä ja palveluja tarjoava organisaatio on toinen osapuoli. Organisaatio voi edelleen luovuttaa tietoja kolmansille osapuolille. Kolmannet osapuolet voivat olla joko lainmukaisia ja sopimuksessa määriteltyjä yksilön tietoihin käsiksi pääseviä osapuolia tai niin sanotulla epäselvällä harmaalla alueella toimivia osapuolia. Lain ulkopuolisella alueella toimivat kolmannet osapuolet eivät varsinaisesti ole laittomasti tietoja käyttäviä osapuolia, mutta usein yksilö ei ole tietoinen näistä osapuolista. Esimerkkinä artikkelissa annetaan viranomaisten suorittama tietojen kerääminen valtion turvallisuuden takaamiseksi. Neljännet osapuolet ovat laittomia, sopimuksenulkopuolisia tai muuten luvattomia yksilön dataa käyttäviä osapuolia. Neljännet osapuolet voivat käytännössä saada käsiinsä yksilön tietoja miltä tahansa osapuolelta, myös suoraan yksilöltä esimerkiksi hakkeroinnin eli tietomurtojen kautta. Malli kuvastaa siis tarkasti ja todenmukaisesti yksilön heikentyneitä kontrollimahdollisuuksia henkilökohtaisiin tietoihin liittyen ja sitä, miten yksityisyyden suojan ylläpitäminen ei ole enää pelkästään yksilöstä itsestään kiinni. (Conger ym. 2013, 404–407.)

Tarkasteltaessa yksityisyyden määritelmää ja sen kehitystä, voidaan havaita käsitteen tarkentuvan ja muuttuvan kokonaisvaltaisemmaksi. Ennen yksityisyyden käsitettä tavoitteena on ollut lähinnä turvata yksilöiden fyysinen omaisuus ja koskemattomuus. Yksityisyyden käsite luotiin arvojen ja lainsäädännön kehittyessä ottamaan huomioon myös hen-

kisiä ja aineettomia ominaisuuksia. Käsite on ajan saatossa kehittynyt ottamaan huomioon myös yksityisyyden yhteiskunnallisia näkökulmia muun muassa Westinin (2003) määritelmässä ja edelleen esimerkiksi Clarke (1999), Bélanger ja Crossler (2011), Smith ym. (2011), Conger (2013) ja Kokolakis (2015) ovat kiinnittäneet huomioon yksilöitä koskevien tietojen yksityisyyteen. Yksilön henkilökohtaisten tietojen yksityisyyttä on kuvailtu tietointensiivisen yhteiskunnan yhdeksi suurimmaksi ja tärkeimmäksi ongelmaksi (Liu ym. 2014, 1063).

2.1.1 Yksityisyys ihmisoikeutena

Monet yksilöt mieltävät yksityisyyden heille kuuluvana oikeutena. Jo Warrenin ja Brandeisin (1890) yksityisyyden käsitettä perustavanlaatuisesti määrittelevässä artikkelissa yksityisyyttä korostettiin yksilön oikeutena. Yksityisyyttä ei ole tunnistettu pelkästään tieteellisessä tutkimuksessa tai yhteiskuntien lainsäädännössä ihmisten oikeutena, vaan myös yleisesti ja universaalisti kaikille kuuluvana ihmisoikeutena.

Ihmisten oikeus yksityisyyteen huomioitiin laaja-alaisesti Yhdistyneiden kansakuntien ihmisoikeuksien yleismaailmallisessa julistuksessa vuonna 1948. Vaikka julistus ei varsinaisesti ole oikeudellisesti velvoittava, ovat ihmisoikeuksien julistuksessa mainitut seikat ja perusteet yleisesti hyväksyttyjä ympäri maailman. Esimerkiksi yksilön oikeus fyysiseen yksityisyyteen ja koskemattomuuteen huomioidaan 3. artiklassa, jossa todetaan yksilöillä olevan oikeus elämään, vapauteen ja henkilökohtaiseen turvallisuuteen. Julistuksen 12. artiklassa todetaan, ettei kenenkään yksityiselämään, kirjeenvaihtoon, kotiin tai perheeseen tule puuttua mielivaltaisesti ja jokaisella on oikeus lainsäädännön suojaan yksityiselämän, maineen ja kunnianloukkausta vastaan. Omaisuuden yksityisyys puolestaan huomioitiin 17. artiklassa, jonka mukaan jokaisella ihmisellä on oikeus omistaa omaisuutta yksin tai muiden kanssa eikä tätä omaisuutta saa mielivaltaisesti riistää. 18. artiklan mukaan ajatuksen, omatunnon ja uskonnon vapautta tulee olla oikeus harjoittaa yksityisesti ja julkisesti. Ja viimeiseksi, 19. artiklassa todetaan muun muassa, että yksilöillä tulee olla oikeus vastaanottaa, levittää ja hankkia tietoja. (United Nations 2020.)

Koska yksityisyys on yleisesti hyväksytty myös ihmisoikeutena, nähdään yksityisyyden suojan rikkomukset ja laaja datankeruu keskeisenä ongelmana nykyaikaisessa tietoyhteiskunnassa (Wiedmann ym. 2001, 180). Tämän takia datan keräämiseen ja käyttöön liittyy myös eettisiä näkökulmia. Onko esimerkiksi perusteltua käyttää yksityisyyttä vaihdannan välineenä ja voidaanko henkilökohtaisille tiedoille asettaa tai määritellä arvo?

Erityisesti yksilöstä kerättyjen tietojen luvaton väärinkäyttö, myyminen ja identiteettivarkaudet ovat kuitenkin selkeästi eettisestä näkökulmasta ongelmallisia tilanteita. Toisaalta datan keräämistä ja hyödyntämistä on perusteltu sillä, että yksilöt itse tekevät päätöksen tietojensa jakamisesta organisaatioille. (Liu ym. 2016, 140–141.) Toisaalta, kuten tämän tutkielman luvussa 2.6 huomataan, yksilöistä kerätään usein myös huomaamattomasti tietoja. Vaikka tämän tutkielman keskipisteessä eivät ole yksityisyyden eettiset näkökulmat, ovat ne keskeinen osa yksityisyyteen liittyvää keskustelua ja yksi syy siihen, miksi yksityisyyden suojaan liittyvät ongelmat ja ilmiöt ovat saaneet osakseen kasvavaa huomiota.

2.1.2 Tietosuoja ja tietoturva

Useasti yksityisyydestä ja yksityisyyden suojasta puhuttaessa käytetään myös tietosuojan ja tietoturvan käsitteitä. Vaikka kaikki edellä mainitut käsitteet liittyvät läheisesti toisiinsa, ei näitä tulisi sekoittaa keskenään tai käyttää samassa tarkoituksessa, varsinkaan tieteellisessä tutkimuksessa.

Tietosuojalla viitataan ensisijaisesti yksityisyyden suojan toteuttamiseen organisaatioissa ja yhteisöissä. Tietosuojan tarkoituksena on turvata yksilön oikeuksien toteutuminen organisaatioissa tapahtuvassa henkilökohtaisten tietojen käsittelyssä. Toisin sanoen tietoja käsitellään yksityisyyden suojan säilymiseksi. Tietoturva puolestaan on tapa toteuttaa tietosuojaa ja tietoturvan tarkoituksena on suojata yksilöistä kerättyjä tietoja ja tietoihin liittyviä tietojärjestelmiä, esimerkiksi tietojen tallentamiseen ja siirtämiseen liittyvien ratkaisujen ja teknologioiden avulla. (Stanton ym. 2007, 3; Tietosuoja.fi/tietosuoja.)

2.2 Yksityisyyden paradoksi

Asiakasdatan ja sen analysoinnin merkityksen korostuessa liiketoiminnassa, tulee organisaatioiden kiinnittää yhä enenevissä määrin huomiota yksilön yksityisyyden suojaan toiminnassaan. Koska yksilöistä kerättävä ja hyödynnettävä data on yhä yksityiskohtaisempaa, arkaluontoisempaa ja monimuotoisempaa, on tietovuotojen ja tietojen väärinkäytön estämisen eteen nähtävä entistä enemmän vaivaa. Yksilöiden tietojen yksityisyys on yrityksen johdon yksi vakavimmista ja merkittävimmistä ongelmista. (Awad & Krishnan 2006, 13–14.) Asiakkaisiin ja käyttäjiin liittyvän datan saatavuus on yleensä verkossa toimiville yrityksille välttämätöntä, ja niin sanotun yksityisyyden paradoksin on osoitettu

vaikuttavan merkittävästi yksilöiden halukkuuteen osallistua transaktioihin ja jakaa tietoja verkossa organisaatioille. (Malhotra ym. 2004, 336, 351.)

Internetin yleistymisen myötä yksityisyyteen ja henkilökohtaisten tietojen luovutukseen liittyvät tilanteet ja päätökset ovat tulleet kiinteämmäksi osaksi ihmisten elämää. Vuonna 2001 julkaistussa Brownin (2001) tutkimuksessa tarkasteltiin verkossa ostamisen suosiota ja käyttäjien huolia internetin turvallisuudesta ja yksityisyydestä. Tutkimuksessa havaittiin uudenlaisia piirteitä yksilöiden toiminnassa; yksilöt olivat huolissaan yksityisyyden suojan rikkomuksista ja liiallisesta tietojen keräämisestä, mutta henkilökohtaisia tietoja oltiin valmiita luovuttamaan esimerkiksi verkossa toimiville kauppiaille, kunhan jotain saataisiin vastineeksi luovutetuille tiedoille. Brownin (2001) tutkimus keskittyi kuitenkin enemmän kanta-asiakaskorttien käyttöön fyysisissä myymälöissä kuin henkilökohtaisten tietojen luovuttamiseen tai paradoksaaliseen käyttäytymiseen verkkoympäristöissä. Yksilöt käyttivät kanta-asiakaskorttejaan, vaikka he olivat huolissaan kauppiaiden mahdollisesti suorittamasta ostohistorian seuraamisesta. Tutkimus ei yhdistänyt paradoksiin viittaavien piirteiden esiintymistä varsinaisesti verkkoon, henkilökohtaisiin tietoihin tai yksilön aikomusten ja käyttäytymisen eroihin. (Brown 2001, 17–18.) Myös Spiekermannin ym. (2001, 45) mukaan käyttäjät luovuttavat henkilökohtaisia tietojaan verkkokaupoissa helposti preferensseistään poiketen ja tietojen luovutukseen liittyvä käyttäytyminen erosi käyttäjien asenteista ja preferensseistä suojella yksityisyyttä. Acquistin (2004, 27) mukaan käyttäjien yksityisyyteen liittyvä käytös on epäjohdonmukaista, sillä käyttäjät eivät usein suojele yksityisyyttään suunnitelmiensa mukaisesti ja yksityisyyden suojaan liittyvät riskit aliarvioidaan.

Yksityisyyden paradoksi on ilmiönä ja käsitteenä huomattavasti uudempi kuin yksityisyys. Vaikka paradoksiin viittaavia havaintoja ja piirteitä havaittiin edellä mainituissa tutkimuksissa jo 2000-luvun alkupuolella, varsinainen yksityisyyden paradoksin käsite tuli määritetyksi ja tiedostetuksi tieteellisissä yhteisöissä vasta vuonna 2006, kun ihmisten toiminnassa alettiin huomaamaan ristiriitaisia piirteitä vapaaehtoisessa tiedonjaossa, yksityisyyshuolissa ja henkilökohtaisten tietojen suojelussa muun muassa sosiaalisen median ja verkossa tapahtuvan liiketoiminnan yleistymisen ja laajenemisen myötä. (Dienlin & Trepte 2015, 285.) Barnes (2006) tunnisti vallitsevan yksityisyyden paradoksin neljän ristiriitaisen tekijän pohjalta yksilöiden sosiaalisen median käyttötottumuksista. Ensiksikin ihmiset luovuttavat suuria määriä dataa verkossa toimiville organisaatiolle. Toiseksi käyttäjien keskuudessa on yleistynyt yksityisyyden illuusio eli tilanne, jossa yksilöillä on muodostunut virheellinen käsitys yksityisyyden suojasta, jonka oletetaan olevan parempi

kuin mitä se on todellisuudessa. Kolmanneksi yksilön asenteissa, aikomuksissa ja käytöksessä tietojen luovuttamisen suhteen esiintyy eroavaisuuksia. Neljänneksi ja viimeiseksi verkkoa käyttävillä yksilöillä on vähäinen ymmärrys yritysten harjoittamasta datan keräämisestä, prosessoinnista ja käytöstä. Digitalisaatioon liittyvän tiedonsiirron ja päätelaitteiden hinnanlaskun on epäilty osaltaan edistäneen yksityisyyden paradoksin yleistymistä. (Barnes 2006; Dienlin & Trepte 2015, 285.)

Baek (2014) puolestaan korostaa yksityisyyden paradoksissa olevan kyse ihmisten huolista organisaatioiden datankeruuta ja henkilökohtaisten tietojen väärinkäyttöä kohtaan, mutta yksityisyyden suojaa ylläpitävät tai sitä edistävät toimenpiteet jätetään huomiotta. Muun muassa yksityisyysasetusten muuttaminen sosiaalisessa mediassa, tasaisin väliajoin tapahtuva evästeiden poistaminen ja oman harkinnan käyttö sekä varovaisuus henkilökohtaisten tietojen paljastamisessa ovat esimerkkejä yksityisyyttä suojaavista toimenpiteistä. (Baek 2014, 33–34.)

Yksityisyyden paradoksi on noussut keskeiseksi ilmiöksi erityisesti sosiaalisessa mediassa, verkkokaupoissa ja muussa verkossa tapahtuvassa vuorovaikutuksessa ja liiketoiminnassa. Yksilöillä on usein positiivisia asenteita yksityisyyden suojan edistämistä ja ylläpitämistä kohtaan sekä yleinen käsitys tiedonjakoon liittyvistä riskeistä ja tietoa yksityisyyden suojaa parantavista toimenpiteistä. Yksilöillä on yksityisyyteen liittyviä aikeita (engl. privacy intentions) ja halukkuutta suojella yksityisyyttään sekä rajoittaa omien tietojensa jakamista ulkopuolisille ihmisille tai organisaatioille, mutta varsinaisen yksityisyyteen liittyvän käyttäytymisen (engl. privacy behavior) on havaittu eroavan merkittävästi yksilöiden aikeista. Aikeet eivät siten onnistuneesti ennusta tai vastaa käyttäytymistä tiedonjakoon liittyvissä tilanteissa. Paradoksiin liittyvässä käyttäytymisessä on havaittu sekä rationaalisia että irrationaalisia piirteitä. Yksityisyyteen liittyvällä käytöksellä tarkoitetaan yksilön konkreettisia toimia ja päätöksiä omien henkilökohtaisten tietojensa luovuttamiseen tai suojaamiseen liittyen. (Barth & de Jong 2017, 1039–1040.) Tämän aikeiden ja käytöksen välisestä kuilusta johtuen, ilmiötä nimitetään yksityisyyden paradoksiksi tai vaihtoehtoisesti tietojen yksityisyyden paradoksiksi. Yksityisyyden paradoksi onkin keskittynyt juuri tietojen yksityisyyden käsitteen ympärille. (Hallam & Zanella 2017, 217–218.) Aivazpourin ja Raon (2020, 16) mukaan yksityisyyden paradoksiin liittyvät aikeet ja käyttäytyminen voivat liittyä kolmenlaisiin tapauksiin: varsinaiseen tietojen jakamiseen, tietojen jakoa edellyttäviin aktiviteetteihin ja yksityisyyden suojaa edistäviin toimenpiteisiin.

Yksityisyyden paradoksista on kehitetty kaksi toisistaan eroavaa teoriaa: käyttäytymiseen (engl. behavior-oriented) ja mielipiteisiin (engl. opinion-oriented) painottuvat tulkinnat. Käyttäytymiseen orientoituneen teorian mukaan yksilön käyttäytyminen on harkittua ja tietoista. Koska internetissä olevat palvelut ovat usein täysin ilmaisia ja esimerkiksi personoitujen palvelujen tarjoaminen olisi mahdotonta ilman minkäänlaisia tietoja palvelun käyttäjästä, ovat käyttäjät valmiita luovuttamaan henkilökohtaisia tietojaan odotettujen hyötyjen, lisääntyneen käyttömukavuuden tai muiden vastaavien etujen toivossa. Käyttäytymiseen ei liity yhtään epätietoisuutta, mutta huolet yksityisyyden suojasta saattavat rajoittaa yksilöiden tietoista toimintaa. Käyttäytymiseen orientoitunut teoria ehdottaa toimivaksi ratkaisuksi tietojenluovutukseen itsesääntelyä ja vapaita sopimuksia organisaatioiden ja käyttäjien välille. Valtion tai muiden julkisten toimijoiden ei tulisi puuttua yksilöiden käyttäytymiseen lainsäädännöllä tai säännöksillä. Mielipiteisiin orientoituneen teorian mukaan paradoksin ajatellaan aiheutuvan ihmisten huonosta ja rajallisesta tietämyksestä muun muassa siitä, miten organisaatiot voivat prosessoida ja hyödyntää keräämiään tietoja. Huolet ovat tiedostettuja ja aiheellisia, mutta rajallinen tietämys teknisistä asioista ja datankeruusta johtavat yksilöissä huolimattomaan ja riskialttiiseen käyttäytymiseen. Päinvastoin kuin käyttäytymiseen orientoituneessa teoriassa, mahdollisena ratkaisuna ongelmiin nähdään ennaltaehkäisevä lainsäädäntö, joka suojelisi yksilöiden yksityisyyden suojaa enemmän ja rajoittaisi organisaatioiden mahdollista tietojen väärinkäyttöä. (Baek 2014, 34.)

Mahdollisiksi ratkaisuiksi yksityisyyden paradoksiin Barnes (2006) pohdiskeli artikkelissaan koulujen ja yliopistojen mahdollisuutta opettaa ja sivistää ihmisiä tietoisuuden lisäämiseksi, vanhempien velvollisuutta kasvattaa lapsistaan vastuullisia internetin käyttäjiä, valtioiden ja viranomaisten lainsäädännöllisiä ratkaisuja sekä organisaatioiden toimintaperiaatteiden vastuullista muotoilua. Esimerkiksi Pötzschin (2009, 228) mukaan yksityisyyteen liittyvä tietoisuus (engl “privacy awareness”) tarkoittaa yksilön tietoisuutta, huomiota ja käsityksiä seuraavista seikoista:

- Onko ulkopuolisilla henkilöillä tietoja yksilöstä?
- Mitä tietoja ulkopuolisilla on yksilöstä?
- Miten tietoja prosessoidaan ja käytetään?
- Kuinka suuren määrän ulkopuolisten ihmisisten tietoja yksilö voi saada käsiinsä?

Lyhyesti sanottuna yksityisyyden paradoksissa on siis kyse siitä, että yksilöt luovuttavat henkilökohtaisia tietojaan tietoisesti tai tietämättään, usein potentiaalisten hyötyjen toivossa, vastoin omia aikomuksiaan. Paradoksi ei käsitä pelkästään yksilöiden huolia ja

epäilyksiä kasvaneesta datankeruusta, vaan myös huolimattoman ja ristiriitaisen yksityisyyttä heikentävän käytöksen sekä yksityisyyttä suojaavien toimenpiteiden tekemättä jättämisen ja laiminlyönnin.

2.2.1 Yksityisyyteen liittyvät aikeet

Yksityisyyteen liittyvillä aikeilla viitataan erityisesti yksilön muodostamiin suunnitelmiin ja arvioihin omasta käyttäytymisessä tulevaisuuden päätöksentekotilanteissa, joihin liittyy joko oman yksityisyyden suojaamista tai henkilökohtaisten tietojen luovutusta. Aikeet voidaan eritellä lyhyelle ja pitkälle aikavälille. Aikomuksilla tarkoitetaan hyvin usein myös yksilön halukkuutta ja kiinnostusta tietojen luovutusta ja yksityisyyden suojaamista kohtaan. Aikomukset voivat olla joko tiedostamattomia tai selkeästi tiedostettuja. Koska yksityisyyteen liittyvät päätöksentekotilanteet ovat nykyään poikkeuksellisen arkipäiväisiä ja yleisiä sekä päätöksiä voidaan tehdä jopa impulsiivisesti ja hetken mielijohteesta, voivat aikeet olla myös tiedostamattomalla tasolla. (Aivazpour & Rao 2020, 15–20.) Yleisesti ottaen mitä vahvemmat yksilön yksityisyyteen liittyvät käyttäytymisaikeet ovat, sitä todennäköisemmin aikeet ennustavat tulevaisuuden käyttäytymistä. (Norberg ym. 2007, 102–107; Hallam & Zanella 2017, 219–220.)

Suurin osa kirjallisuudesta ja tutkimuksesta ei kuitenkaan tarkastele aikeita erikseen pitkällä tai lyhyellä aikatähtäimellä. Tämän takia tässä tutkielmassa yksityisyyden paradoksiin liittyvistä aikeista puhuttaessa tarkoitetaan sekä pitkän että lyhyen aikavälin yksilön aikomuksia, halukkuutta tai kiinnostusta luovuttaa tai suojella omia henkilökohtaisia tietojaan.

2.2.2 Yksityisyyteen liittyvä rationaalinen käytös

Koska yksityisyyden paradoksiin liittyvää käytöstä voidaan tarkastella sekä yksilön rationaalisen että irrationaalisen käytöksen näkökulmasta, tarkastellaan seuraavaksi tutkimusten keskeisiä havaintoja kummastakin näkökulmasta. Yksi keskeisimmistä ja parhaiten tunnetuista osa-alueista yksityisyyden paradoksiin liittyvästä päätöksenteosta on yksilöiden suorittama rationaalinen arvio tietojen luovuttamisen avulla saavutettavista hyödyistä ja aiheutuvista haitoista sekä riskeistä (ks. esim. Keith ym. 2013; Alashoor ym. 2018; Wang ym. 2020). Yksityisyyden tutkimuksessa ilmiö tunnetaan laajemmin privacy calculus -teoriana. Privacy calculus -teoriaa käsitellään tarkemmin tutkielman luvussa 2.10. Rationaalisuuden mukaisesti yksilöt pyrkivät usein maksimoimaan päätöksenteosta

saavutettavat hyödyt ja minimoimaan haitat sekä tyydyttämään tarpeitaan vaihtamalla omia resurssejaan muihin resursseihin; eli yksityisyyden paradoksin kohdalla henkilökohtaisia tietoja vaihdetaan ikään kuin hyödykkeitä tai palveluja vastaan. On kuitenkin kyseenalaistettu, että yksityisyyden paradoksiin liittyvä rationaalinen käytös ja päätöksenteko eivät ole ainoita selityksiä yksilön käyttäytymiseen. (Barth & de Jong 2017, 1044–1052.)

2.2.3 Yksityisyyteen liittyvä irrationaalinen käytös

Vaikka yksilöiden käyttäytymisessä on havaittu useita rationaalisuuden piirteitä, yksityisyyden paradoksin ymmärryksen lisäämiseksi ja selittämiseksi myös irrationaalisen käyttäytymisen merkitystä päätöksenteossa ja toiminnassa on tutkittu. Esimerkiksi Barth ja de Jong (2017) esittävät yksilöiden tiedonjakoon liittyvien päätösten tapahtuvan valtaosin irrationaalisin perustein. Päätökset ovat riippuvaisia teknologian käytöstä ja päätöksentekotilanteesta. Esimerkiksi älypuhelimien ja mobiiliapplikaatioiden myötä tiedonjakoon liittyvät päätöksentekotilanteet ovat yhä yleisempiä ja päätöksenteko tehdään usein nopeasti, arkipäiväisissä tilanteissa ja kodin tai työn ulkopuolella liikkeellä ollessa. Sopimusehtojen ja käyttölupien lukemisen laiminlyönti sekä oletusasetuksiin tyytyminen ovat tavanomaisia toimintamalleja yksilöille verkossa. Intuitio voidaan nähdä keskeisenä osana irrationaalista käytöstä ja riskiarviointi tiedonjaosta saatetaan jättää tekemättä. Tiedon jakamisesta on tullut eräänlainen rutiini ja keskeinen osa sosiaalista ja päivittäistä elämää. Vaihtoehtoisesti yksilöt saattavat tunnistaa useita riskejä ja omia huoliaan yksityisyyden suojasta, mutta käyttäjille epäsuotuisat käyttöehdot ja käyttöliittymä ovat yhä yleisempiä. Myös ennakkoluuloiset tai vääristyneet riskiarviot päätöksenteon tukena ovat osa irrationaalista käyttäytymistä. (Barth & de Jong 2017, 1039–1040, 1050–1051.)

Selityksinä yksityisyyden paradoksin olemassaololle on ehdotettu myös yksilöiltä puuttuvia kokemuksia yksityisyyden suojan häirinnästä ja yksityisyyden suojaamiseen tarvittavan tietämyksen rajallisuutta. Yksilöiden asenteet usein pohjautuvat muiden ihmisten kertomiin kokemuksiin tai yksilön omiin heuristisiin ajatuksiin. Yksityisyyden suojan parantamiseen ja ylläpitämiseen vaadittavat työkalut vaativat lähtökohtaisesti teknistä ymmärrystä verkon ja päätelaitteen käytöstä, kuten esimerkiksi tietoa evästeiden poistosta, yksityisyysasetusten muuttamisesta, kommunikoinnin salaamisesta ja oman toiminnan anonymisoinnista. Yksilöllä voi olla siis rajallista tietoa sekä yksityisyyden suojan heikkenemisestä aiheutuvista negatiivisista seurauksista että internetiin ja yksityi-

syyteen liittyvistä asioista ja päätyy tämän takia tekemään irrationaalisia valintoja. (Gerber ym. 2018, 229–231.) Esimerkiksi Cognitive deficiency -teorian mukaan yksilöiden puutteellisen tietämyksen takia henkilökohtaisten tietojen suojelemisesta verkossa yksityisyyteen liittyvät aikeet eivät ennusta käyttäytymistä. Cognitive deficiency -teoria saattaa selittää osittain yksityisyyden paradoksin olemassaoloa, mutta teoria ei selitä paradoksia esimerkiksi IT-ammattilaisten tai muiden yksityisyyttä laajasti ymmärtävien henkilöiden keskuudessa. (Hallam & Zanella 2017, 219.)

Myös heuristiikan on havaittu olevan osana yksityisyyden paradoksiin liittyvää päätöksentekoa. Heuristisessa päätöksenteossa yksilö tekee päätöksen, joka johtaa tarpeeksi lähelle toivottavaa lopputulosta. Usein tietoa tai muita resursseja päätöksen tekemiseksi voi olla liian rajallisesti saatavilla. Ihmiselle on myös tyypillistä tehdä päätöksiä lyhyen aikavälin tähtäimellä, eli nopeammin saavutettava pienempi hyöty valitaan ennemmin kuin pitkällä aikavälillä realisoituva suurempi hyöty. (Barth & de Jong 2017, 1046–1048.)

Yksilöiden päätöksentekoon liittyy ajoittain myös kognitiivista vinoumaa, eli taipumusta painottaa asioita ja tehdä havaintoja joillakin tietyillä tavoilla. Yksilö ei välttämättä ota huomioon päätöksenteossa kaikkea olemassa olevaa informaatiota, hyötyjä, haittoja tai kustannuksia. Yksilö ei välttämättä edes ole tietoinen siitä, että hänen dataansa kerätään. Yksilön päätökset perustuvat siis tämänkaltaisissa tilanteissa epätäydelliselle informaatiolle, jonka takia hyödyt tai riskit voidaan yli- tai aliarvioida. Yksilö päätyy toimimaan irrationaalisesti jättäessään osan saatavilla olevasta informaatiosta huomiotta. Vaikka yksilöllä olisi saatavilla kaikki mahdollinen informaatio, olisi täysin rationaalisen päätöksen tekeminen haastavaa, koska ihmisen kognitiivinen prosessointikyky on myös rajallinen. Kirjallisuudessa ja tieteellisessä tutkimuksessa ilmiöstä käytetään usein nimitystä rajoittunut rationaalisuus. Tämän takia alkuperäiset asenteet tai aikomukset voivat olla ristiriidassa käytöksen kanssa. (Gerber ym. 2018, 226–227, 229–230.)

Yleisiä ja yksityisyyden kannalta keskeisiä kognitiivisia vinoumia ovat muun muassa seuraavat (Gerber ym. 2018, 229–230):

- Saatavuuden vinouma: yksilöillä on taipumus yliarvioida tapahtumia, jotka he muistavat hyvin. Esimerkiksi mediassa esillä olevat vastaavanlaiset asiat voivat altistaa tämänkaltaiselle vinoumalle.
- Optimismin vinouma: yksilöt aliarvioivat oman riskinsä altistua yksityisyyden suojan ongelmille.
- Vahvistusharha: yksilöt etsivät ja tulkitsevat tietoa sekä tilanteita, mitkä vahvistavat heidän omia oletuksiaan ja uskomuksiaan.

- Tunteisiin pohjautuva vinouma: yksilöt tulkitsevat asioita tunteidensa pohjalta, jolloin mieluisten ja pidettyjen asioiden riski koetaan todellista pienempänä, kun taas epämieluisten asioiden riski yliarvioidaan.
- Välittömän mielihyvän vinouma: ajankohtaista ja nykyistä hyötyä tai riskiä painotetaan enemmän kuin tulevaisuuden ja pitkän aikatähtäimen hyötyjä tai riskejä. Välittömän mielihyvän vinoumaa nimitetään myös liikadiskonttaukseksi.
- Valenssiefekti: suotuisten tapahtumien todennäköisyys yliarvioidaan.
- Kehystysvaikutus: informaation esitystavalla tai kysymysten asettelulla voidaan vaikuttaa tarkoituksellisesti yksilöön.
- Rationaalinen ignoranssi: jotkin tekijät, kuten esimerkiksi tiedonjaosta aiheutuvat kustannukset, jätetään huomioimatta. Yksilöt kokevat, että tiedonkeräämisen ymmärtämisestä tai kokonaisvaltaisemmasta ymmärtämisestä aiheutuvat kustannukset ja vaiva ylittävät tiedonjaosta saavutettavat hyödyt.

Yksilöillä on usein vääristynyt käsitys omista mahdollisuuksistaan kontrolloida omaa yksityisyyden suojaa ja datan käyttöä. Ihmisille on tyypillistä sekoittaa keskenään omien tietojen käytön ja julkaisemisen kontrolli. Jos yksilöllä itsellään on mahdollisuudet vaikuttaa omien tietojensa julkaisemiseen verkossa, yksilöt luovuttavat helpommin tietoja organisaatioiden käytettäväksi. Koska yksilön käsitys oman datan kontrollista on virheellinen ja se koskee vain tietojen julkaisemista, nimitetään yksilön virheellistä käsitystä yleisesti kontrollin illuusioksi tai yksityisyyden illuusioksi. Tyypillinen esimerkki kontrollin illuusiosta on sosiaalisen median käyttäjän mahdollisuus rajata oman julkaisunsa yleisöä. Tiedot päätyvät yhä sosiaalisen median organisaatiolle, mutta yksilöllä on mahdollisuus vaikuttaa julkaistujen tietojen näkyvyyteen omien kontaktiensa kohdalla. Kontrollikäsitys on virheellinen, koska kontrolli koskee ainoastaan tietojen näkyvyyden rajaamista. (Barnes 2006; Gerber ym. 2018, 229–231.)

Yksityisyyteen liittyvää käytöstä voidaan tarkastella hyvinkin yksityiskohtaisella tai yleisellä tasolla. Tässä tutkielmassa yksityisyyteen liittyvää käytöstä tarkastellaan näkökulmasta, jossa yhdistyvät pitkä ja lyhyt aikaväli sekä irrationaalinen ja rationaalinen käytös. Käyttäytyminen voi olla tämän tutkielman näkökulman mukaan paitsi yksityisyyttä heikentävää tai vaarantavaa, kuten esimerkiksi tietojen luovutusta, tai yksityisyyden suojaa edistävää, kuten esimerkiksi yksityisyysasetusten muutamista tai tietojen luovuttamatta jättämistä. Useissa paradoksia tarkastelevissa tutkimuksissa ei käsitellä erikseen pitkän ja lyhyen aikavälin käyttäytymistä, rationaalista ja irrationaalista käyttäytymistä tai yksityisyyttä suojaavaa ja heikentävää käyttäytymistä. Tämän takia mahdollisimman kattavan kuvan luomiseksi paradoksista pysytään käytöksen tarkastelussa tasolla, johon

lukeutuvat pitkä ja lyhyt aikaväli, rationaalinen ja irrationaalinen käytös sekä yksityisyyttä suojaava ja heikentävä käytös.

2.3 Yksityisyyshuolet

Yksityisyyteen ja yksityisyyden paradoksiin liittyvässä keskustelussa nousee usein esiin yksityisyyshuolten käsite. Yksityisyyshuolet tarkoittavat yksilöiden subjektiivista käsitystä ja suhtautumistapaa henkilökohtaisten tietojen keräämisen ja käytön heikentyneestä kontrollista (Liu ym. 2014, 1065). Yksityisyyshuolet ovat merkittävä ongelma erityisesti yksilöiden keskuudessa. Jopa 91 prosenttia amerikkalaisista aikuisista kokevat menettäneensä kontrollin datan keruusta ja käytöstä. Puolet amerikkalaisista internetin käyttäjistä ovat huolissaan siitä, miten paljon heistä itsestään löytyy tietoa verkosta. Myös eurooppalaisista 57 prosenttia ovat huolissaan yksityisyyden suojastaan. (Gerber ym. 2018, 227.)

Yksityisyyshuolet voidaan jakaa sosiaalisiin ja institutionaalisiin yksityisyyshuoliin. Sosiaalisilla yksityisyyshuolilla tarkoitetaan lähtökohtaisesti yksilön huolia, jotka kohdistuvat muihin yksilöihin, ihmissuhteisiin ja yksityiselämään. Yksilöt ovat siis huolissaan muiden yksilöiden suorittamasta yksityisyyden suojan häirinnästä, kuten esimerkiksi tietojen asiattomasta levittämisestä, tietojen kalastelusta tai nettikiusaamisesta. Sosiaaliset yksityisyyshuolet ovat yksilöille helposti hahmotettavia ja ymmärrettäviä. Institutionaaliset huolet ovat puolestaan yksilöille huomattavasti epäselkeämpiä ja vaikeammin ymmärrettäviä. Institutionaaliset huolet kohdistuvat viranomaisten, yritysten tai muiden yhteisöjen suorittamaan tarkkailuun, luvattomaan tietojen keräämiseen ja muuhun tietojen väärinkäyttöön. (Raynes-Goldie 2010; Young & Quan-Haase 2013, 479–481.) Institutionaaliset yksityisyyshuolet liittyvät juuri organisaatioiden datan keräämiseen ja hyödyntämiseen. Yleisesti yksilöt ovat enemmän tietoisia sosiaalisista huolista ja siten myös paremmin varautuneita sosiaalisia yksityisyyshuolia kohtaan. Koska institutionaalisten huolten hahmottaminen on haastavampaa ja vähemmän tiedostettua, ollaan juuri institutionaalisilta yksityisyysvaaroilta heikommin varauduttuja ja suojattuja. Tyypillisesti yksilöt luottavat enemmän esimerkiksi viranomaisiin, rahalaitoksiin ja pankkeihin, kun taas verkossa toimiviin yrityksiin lähtökohtaisesti luotetaan huomattavasti vähemmän. (Lutz & Strathoff 2011, 84–85, 93–95.)

Yksilöiden yksityisyyshuolet perustuvat pääasiassa seitsemään seikkaan (Liu ym. 2014, 1064–1065):

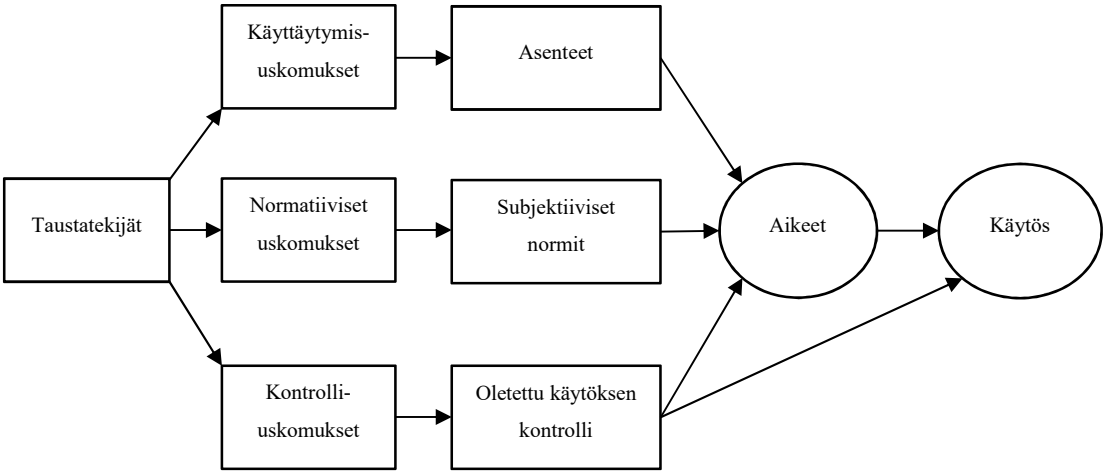
- Henkilökohtaisia tietoja kerätään suuria määriä.
- Kerätyt tiedot voivat olla virheellisiä tai epätarkkoja.

- Kerättyjä tietoja voidaan käyttää salattuihin tai epäsopiviin tarkoitukseen, eli niin sanottu tietojen toissijainen käyttö.
- Organisaatiot voivat epäonnistua kerättyjen tietojen suojelussa ja ulkopuolisilla voi siten olla mahdollisuus päästä käsiksi yksilön tietoihin.
- Kysymys siitä, onko organisaatiolla käytössään lainmukainen sopimus tai seloste. Tällaisen sopimuksen puute tai olemassaolo vaikuttavat huoliin.
- Organisaation ominaisuudet ja maine. Esimerkiksi suurilla organisaatioilla oletetaan olevan tarpeeksi resursseja ja kykyjä palvelujen tarjoamiseen, eikä yksilön tietojen eteenpäin myymiseen oleteta olevan tällöin tarvetta.
- Huolet tietojen julkaisemisesta ja käyttöehtojen muutoksista. Koska esimerkiksi mobiiliapplikaatioiden käyttöehdot päivittyvät usein, sopimusehtojen muutokset voivat jäädä huomaamatta tai tiedostamatta.

Yksityisyyshuolet ja edellä mainittujen seikkojen painottuminen vaihtelevat tyypillisesti tietojen tarkkuuden ja arkaluontoisuuden mukaan. Esimerkiksi yksilöiden taloudelliset tiedot tai tunnistamiseen ja identifiointiin käytettävät tiedot, kuten henkilötunnus, aiheuttavat enemmän huolia yksityisyydestä kuin yleisemmän tason demografiset tiedot, kuten ikäluokka tai sukupuoli. Yksityisyyshuolet voivat vaihdella yksilöittäin, esimerkiksi yksilöiden persoonaan liittyvien ominaisuuksien tai kulttuurillisten erojen johdosta. (Liu ym. 2014, 1064–1065.)

2.4 Suunnitellun käyttäytymisen teoria

Yksityisyyden paradoksiin liittyvässä tutkimuksessa on usein noussut esiin Ajzenin vuonna 1985 kehittelemä suunnitellun käyttäytymisen teoria (engl. Theory of Planned Behaviour). Suunnitellun käyttäytymisen teoria on yksi tunnetuimmista ja eniten hyödynnetyistä teorioista ihmisen käyttäytymisen tutkimuksessa. Teorian ytimessä on ajatus siitä, että yksilön asenteet, subjektiiviset normit ja oletettu oman käytöksen kontrolli vaikuttavat yksilön käyttäytymisen aikomuksiin ja sitä kautta varsinaiseen käyttäytymiseen. Teorian pääasiallisena tavoitteena on paremmin ennustaa ja ymmärtää ihmisen aikeita ja osittain myös käyttäytymistä. (Deborah ym. 1999, 225–226; Ajzen 2002, 665.) Suunnitellun käyttäytymisen teoria esitellään kuviossa 2.



Kuvio 2. Suunnitellun käyttäytymisen teoria (Al Maskari 2018)

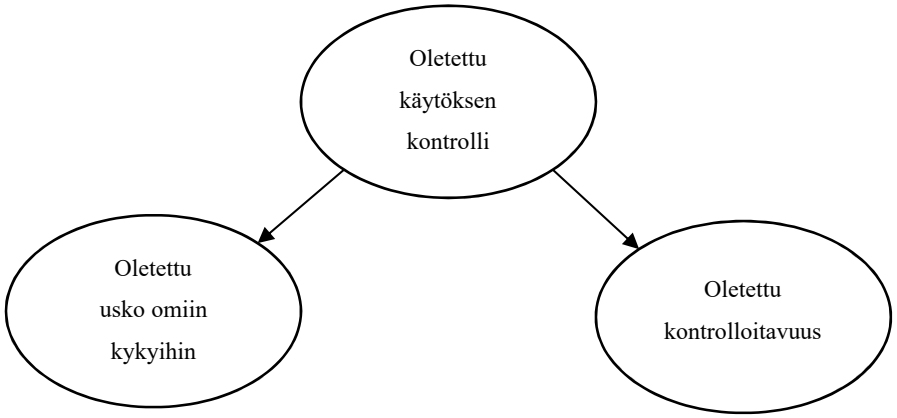
Suunnitellun käyttäytymisen teoria on kehittynyt Fishbeinin ja Ajzenin vuonna 1975 kehittämästä perustellun toiminnan teoriasta (engl. Theory of Reasoned Action). Teoriat ovat muuten samanlaisia, mutta suunnitellun käyttäytymisen teoria lisäsi perustellun toiminnan teoriaan liittyvään malliin kontrolliuskomukset ja oletetun käytöksen kontrollin. Suunnitellun käyttäytymisen teoria toimii siis jatkeena perustellun toiminnan teorialle. (Deborah ym. 1999, 225–226.) Kontrolliin perustuvien tekijöiden lisääminen osaksi mallia koettiin tarpeelliseksi, koska vaikka yksilön aikeet olisivat kuinka selkeät ja vahvat, joidenkin asioiden kontrolloiminen voi olla yksilön vaikutusmahdollisuuksien ulottumattomissa. Toisin sanoen käytöksen toteuttamiseen voi liittyä myös ulkopuolisten tahojen toimintaa, jolloin on olennaista huomioida yksilön kokema kontrolli käyttäytymiseen liittyvästä tilanteesta käyttäytymisen ennustamisen tarkentamiseksi. (Ajzen 2002, 666–667.)

Suunnitellun käyttäytymisen teoria lähtee liikkeelle yksilöön liittyvistä taustatekijöistä. Taustatekijät voidaan jakaa kolmeen ryhmään: persoonaan liittyvät tekijät, sosiaaliset taustatekijät ja tietoihin liittyvät tekijät. Yksilön persoonaan liittyviä tekijöitä ovat esimerkiksi persoonallisuus ja luonteenpiirteet, arvot, tunteet, älykkyys ja yleiset asenteet. Sosiaalisia taustatekijöitä ovat puolestaan muun muassa ikä, sukupuoli, etnisyys, koulutus ja uskonto. Tietoon liittyvät taustatekijät pohjautuvat yksilön aikaisempiin kokemuksiin, omaan tietämykseen ja medialle altistumiselle. Taustatekijöiden pohjalta yksilöille muodostuu kolmenlaisia uskomuksia. (Al Maskari 2018, 46–48.)

Käyttäytymisuskomuksilla tarkoitetaan uskomuksia käyttäytymisestä aiheutuvista seurauksista ja yksilön käyttäytymisuskomuksista seuraa posiitivis- tai negatiivissävyt-

teinen asenne toimintaa kohtaan. Normatiivisilla uskomuksilla tarkoitetaan yksilön uskomuksia ympäröivien ihmisten käsityksistä siitä, tulisiko jotain tiettyä toimintaa tai käytöstä suorittaa. Normatiiviset uskomukset aiheuttavat yksilöille käsityksiä subjektiivisista normeista. Subjektiiviset normit tarkoittavat yksilön näkemyksiä muiden ympäröivien ihmisten odotuksista ja näkemyksistä jotakin tiettyä aktiviteettia tai toimintaa kohtaan. (Ajzen 2002, 665.) Tyypillinen esimerkki subjektiivista normeista on yksilön kokema sosiaalinen ryhmäpaine tai yksilön muilta ihmisiltä saadut vaikutelmat käyttäytyä muiden arvostamalla ja hyväksymällä tavalla (Dincelli & Goel 2017, 4015). Kontrolliuskomuksilla puolestaan tarkoitetaan yksilön käsitystä käytöstä edistävistä ja estävistä seikoista, jotka luovat yksilön mielessä oletuksen käytökseen liittyvästä kontrollista (Ajzen 2002, 665). Oletettu käytöksen kontrolli tarkoittaa sitä, miten helpoksi tai vaikeaksi yksilöt kokevat jonkin toiminnan tai käytöksen suorittamisen. Asenteilla tarkoitetaan yksilön muodostamaa arviota kyseisen käytös- tai toimintatavan hyväksyttävyydestä. (Hughes-Roberts & Kani-Zabihi 2014, 221–223.) Yksilön omat asenteet käyttäytymistä kohtaan, oma käsitys käytöksen kontrollista ja itse muodostettu arvio subjektiivista normeista yhdessä luovat yksilölle käyttäytymisaikeita. Muodostetuilla käyttäytymisaikeilla on suora vaikutus yksilön käyttäytymiseen. Koska yksilöt voivat kokea usein käytöksen haastavaksi, on oletetun käytöksen kontrollin huomattu vaikuttavan yksilön arvioon käytöksen haastavuudesta ja omasta kontrollista käyttäytymistilanteessa. Tätä kautta oletetun käytöksen kontrollin on havaittu ennustavan osittain myös lopullista käytöstä. (Ajzen 2002, 665–666.)

Oletettua käytöksen kontrollia voidaan tarkastella tarkemmin hierarkkisen mallin avulla. On keskeistä ottaa huomioon yksilöstä itsestään lähtöisin oleva kyky, usko ja luottamus hallita omia kykyjä sekä ulkoisten tekijöiden häiritsevä tai avustava vaikutus käytökseen, eli toisin sanoen kuinka paljon yksilön kontrolloitavissa käytös ja lopputulema ovat. Nämä kaksi tekijää muodostavat yhdessä oletetun käytöksen kontrollin käsitteen. (Ajzen 2002, 678–680.) Hierarkkinen suhde esitetään kuviossa 3.



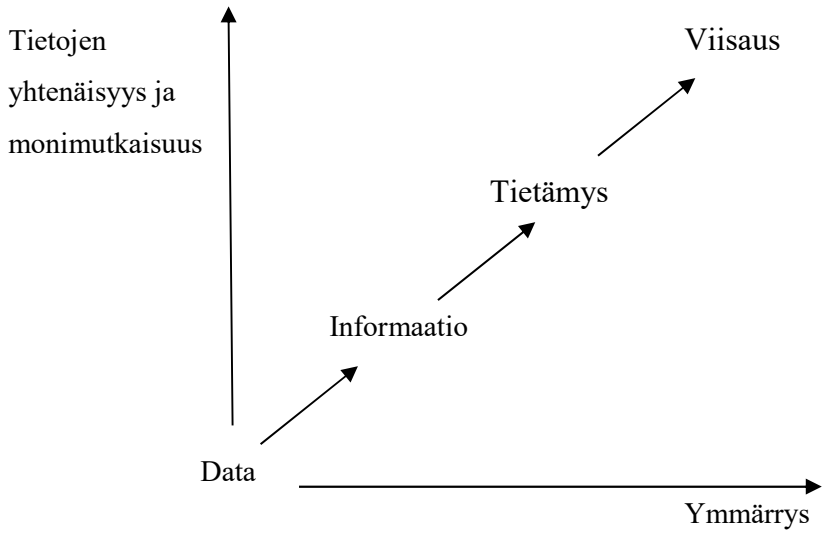
Kuvio 3. Oletetun käytöksen kontrollin hierarkkinen malli (Ajzen 2002)

2.5 Datan määritelmä

Ihmisistä kerättävää dataa on kuvailtu kriittiseksi menestystekijäksi, liiketoiminnan tehostajaksi ja uusia toimintatapoja mahdollistavaksi resurssiksi modernissa liiketoiminnassa. Datasta on tullut eräänlainen raaka-aine organisaatioiden toiminnassa. (Aguirre ym. 2015, 34.) Dataa on kuvailtu jopa 2000-luvun tärkeimmäksi raaka-aineeksi (Igo 2018, 625). Datan prosessointia, hyödynnettävyyttä ja jalostamisen jatkumoa on tyypillisesti kuvattu DIKW-viitekehyksellä (engl. Data, Information, Knowledge, and Wisdom framework) (Matney ym. 2011, 6–8).

Datalla tarkoitetaan raakaa ja analysoimatonta tietoa reaalimaailman tapahtumista ja ilmiöistä. Data on tyypillisesti esimerkiksi tekstiä, kuvioita tai numeerisia arvoja. Nykyään valtaosa datasta kerätään digitaalisessa muodossa. Tyypillinen järjestelmä digitaaliseen tiedon siirtämiseen ja tallentamiseen tunnetaan yleisemmin binäärijärjestelmänä. Binäärijärjestelmässä muuttujan eli bitin arvo on joko nolla tai yksi. Pelkistetysti sanottuna digitaalinen data koostuu vaihtelevan kokoisista bittien sarjoista. Kerätty raaka ja analysoimaton data ei itsessään tue organisaatioiden toimintaa tai päätöksentekoa. Datasta voidaan kuitenkin jalostaa informaatiota. Informaatiolla tarkoitetaan jäsenneltyä ja ihmiselle ymmärrettävässä muodossa olevaa dataa, jota voidaan käyttää hyödyksi päätöksenteossa. Informaatiosta puolestaan voidaan luoda tietämystä, joka tarkoittaa informaation avulla saavutettua henkistä pääomaa ja jonka avulla voidaan lisätä ymmärrystä datasta, organisaation kokonaisarvoa ja hahmottaa syy-seuraussuhteita yksilöissä tai ympäristössä. Tietämystä kuvaillaan usein yleisesti hyväksyttynä ja todellisuutta vastaavana informaationa. Sekä informaatioon että tietämykseen liittyy dataa hyödyntävän henkilön omaa tulkintaa

ja ajattelua. Ylimpänä tasona DIKW-viitekehyksessä nähdään viisaus, joka tarkoittaa kykyä ratkaista inhimillisiä ongelmia tietämystä hyödyntämällä. Viisautta on mahdollista saavuttaa soveltamalla eettisiä ja moraalisia näkökulmia tietämykseen. (Liew 2007; Zins 2007, 479–480; Cooper 2016, 55.) Mitä enemmän dataa on jalostettu, sitä syvällisempää ymmärrystä saavutetaan ja sitä monimutkaisempia sekä yhtenäisempiä tiedot ovat. DIKW-viitekehyksen riippuvuussuhteet ja jatkumo ovat esitelty kuviossa 4.



Kuvio 4. DIKW-viitekehys (Cooper 2016)

Dataa analysoimalla ja jalostamalla voidaan muodostaa informaatiota ja tietämystä päätöksenteon avuksi sekä syy-seuraussuhteiden hahmottamiseksi organisaation toiminnan suunnittelua ja kehittämistä varten. Informaation avulla voidaan saada esimerkiksi tietoa kuluttajien preferensseistä ja tietämyksen avulla puolestaan pyritään ymmärtämään paremmin kuluttajien toimintaan liittyvien syiden ja seurausten suhteita. On olemassa kahdenlaista yksilöihin liittyvää tietämystä: tietämystä yksilöistä (esimerkiksi preferenssit, elämäntyyli ja demografiset tekijät) ja yksilöiden tietämystä (esimerkiksi näkemykset, kokemukset ja mielipiteet markkinoista sekä organisaatioiden tarjonnasta). Nykyään kestävyyden, eettisen ja sosiaalisen näkökulman huomioiminen organisaation toiminnassa nähdään yhä tärkeämpänä ja yhteiskuntavastuuta edistävänä asiana. Viisauden avulla organisaatiot voivat ottaa huomioon myös vastuullisuuteen liittyvät näkökulmat päätöksenteossaan, esimerkiksi arvioimalla henkilökohtaisten tietojen keräämisen, käsittelyn ja käytön moraalisia näkökulmia. (Lee ym. 2006, 290; Liew 2007; Matney ym. 2011, 6–9.)

Yleensä organisaation toiminnassa itse data ei ole olennaisin seikka, vaan se miten dataa analysoidaan, jalostetaan ja hyödynnetään. Datan määrän jatkuvasti lisääntyessä onkin tunnistettava organisaation toiminnan kannalta olennainen data. Usein osa kerätystä datasta on virheellistä tai epärelevanttia ja hyödytöntä organisaation toiminnan kannalta, eikä tämänkaltaisen datan jalostamisesta ole apua päätöksenteossa. Lukuisissa tapauksissa datan on oltava myös mahdollisimman ajankohtaista. (Braganza 2004, 347–350.)

Yhä yleisemmin dataan liittyvässä keskustelussa puhutaan big datasta. Big datalla tarkoitetaan tyypillisesti suuria, monimutkaisia ja analysoimattomia datamassoja. Data-analytiikan avulla big datasta voidaan saada käyttäjistä tai asiakkaista monipuolista ja syvällistä ymmärrystä. Big data vaatii yritykseltä tarvittavan arkkitehtuurin datan keräämiseen, tallentamiseen ja analysointiin. Usein juuri big data ja sen avulla jalostettu tietämys ovat organisaatioille keskeisiä resursseja. (Erevelles ym. 2016, 897–898.)

Big dataa käsitellään tavanomaisesti niin sanotun kolmen V:n avulla (Erevelles ym. 2016, 898):

- Datan määrä (Volyme).
- Datan määrän kasvun nopeus (Velocity).
- Datan monimuotoisuus (Variety).
- Määritelmää voidaan täydentää myös kahdella muulla V:llä, datan todenmukaisuudella (Veracity) ja datan arvolla (value).

2.6 Datan keräämisen toteutustavat

Internetin laajenemisen ansiosta saatavilla olevan informaation ja datan määrä on kasvanut räjähdysmäisesti. Tämä edesauttaa muun muassa räätälöityjen palveluiden ja tuotteiden parempaa saatavuutta, alhaisempia hintatasoja ja valinnanvaran kasvamista. Verkko on mahdollistanut paitsi tehokkaan ja nopean datankeruun, mutta myös tuonut täysin uusia keinoja kerätä ja hyödyntää yksilöistä kerättyjä tietoja. (Lee ym. 2006, 290.)

Yksityisyyden näkökulmasta on hyvinkin olennaista tarkastella, miten dataa kerätään yksilöistä. Datan hyödyntämiselle ja käytölle onkin lähtökohtana datan huolellinen kerääminen ja sen tallentaminen. Jo yksilöihin liittyviä tietoja kerätessä ja tallentaessa tulee minimoida virheet ja yksityisyyden suojaa on kunnioitettava säännösten ja lakien pohjalta. Yksilöille on myös hyötyä datankeruutapojen ymmärtämisestä ja hahmottamisesta yksityisyyden suojaan liittyvässä toiminnassa. (Crié & Micheaux 2006, 282–284.)

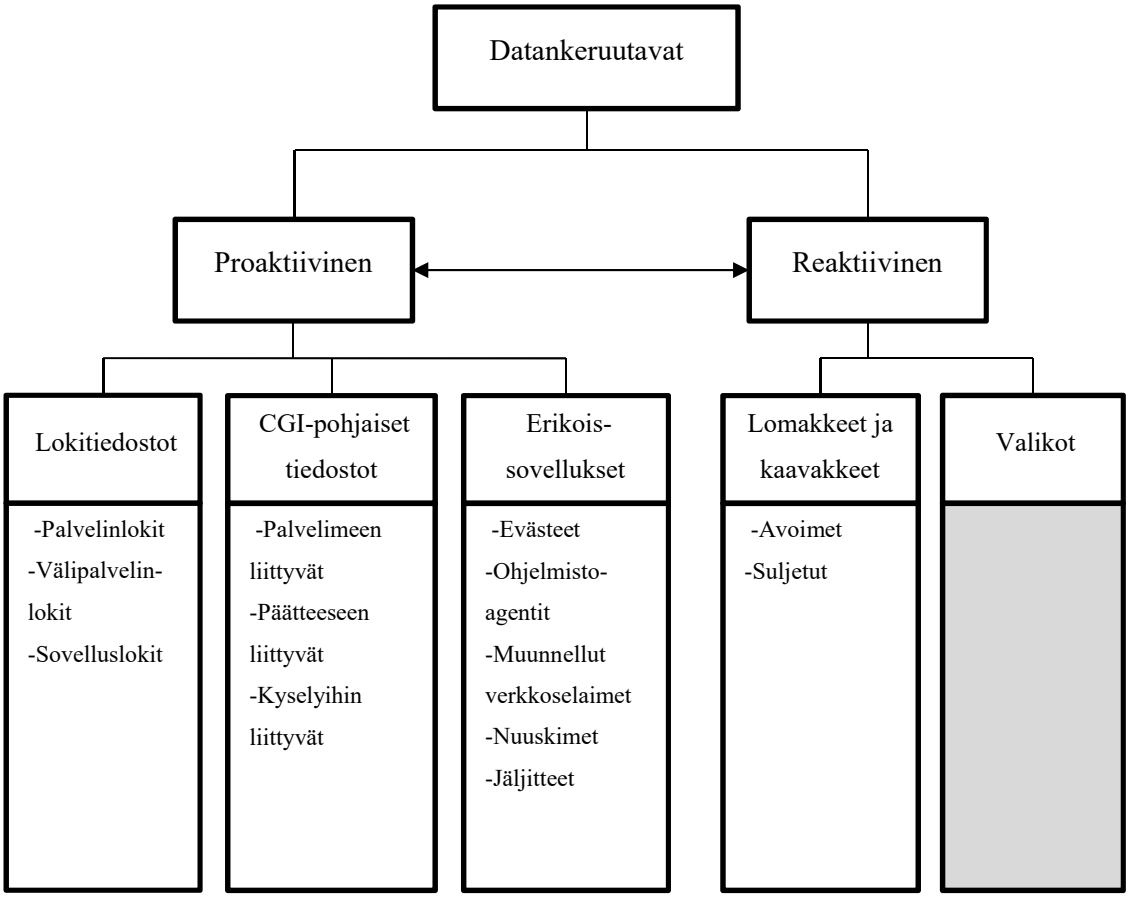
Leen ym. (2006, 290–291) mukaan verkossa suoritettava datankeruu käyttäjiltä voidaan suorittaa seuraavilla tavoilla:

- Verkkosivuilla suoritettavat kyselyt ja tutkimukset. Verkkopalvelun käyttäjä vastaa itse kysymyksiin tai täyttää tietojaan verkossa oleviin lomakkeisiin, vastauslaatikoihin tai tutkimuksiin. Organisaation näkökulmasta säästetään aikaa ja vaivaa tietojen keräämisessä sekä tiedon oikeellisuuteen ja syöttämiseen liittyvien virheiden riski vähenee, kun yksilöt antavat omatoimisesti ja oma-aloitteisesti tietojaan organisaation käyttöön.
- Transaktiot. Yksilöt antavat itse usein transaktioiden yhteydessä vähintään transaktion kannalta välttämättömät tiedot. Riippuen liiketoimen laadusta ja yksityiskohdista, välttämättömiä tietoja voivat olla esimerkiksi nimi, puhelinnumero, osoite, luottokortin tiedot tai sähköpostiosoite. Transaktioiden yhteydessä on mahdollista kerätä myös tietoja huomaamattomasti, esimerkiksi käyttäjän aikaisemmin vierailtujen nettisivujen lista tai verkkosivulla tapahtuneet klikkaukset voidaan saada selville hyödyntämällä seurantateknologioita tai evästeitä.
- Palvelimien lokitiedot. Lokitiedoista voidaan luoda profiileja muun muassa IP-osoitteen hakuhistoriasta tai yksilön toiminnasta, joka ei päätynyt suorittamaan transaktiota. Lokitiedot ovat hyödyllisiä esimerkiksi verkkosivun houkuttelevuuden ja menestyksen arvioinnissa.
- Verkkoyhteisöt. Käyttäjät antavat itse täysin oma-aloitteisesti ja oman mielenkiintonsa pohjalta tietoja itsestään ja kokemuksistaan osallistuakseen sosiaaliseen kanssakäymiseen. Keskustelufoorumeilta, sosiaalisesta mediasta tai muista verkkoyhteisöistä saatavat tiedot voivat olla yksi tehokkaimmista, helpoimmista ja rikkaimmista tiedonlähteistä. Esimerkiksi arviot ja ajatukset tuotteen tai palvelun laadusta ja käyttökokemuksesta ovat yleisiä. Ilman käyttäjiensä oma-aloitteisuutta ja aktiivisuutta verkkoyhteisöt eivät tuota dataa. Usein yhteisöissä edellytetään henkilökohtaisten tietojen syöttämistä vähintäänkin omaan käyttäjäprofiiliin.
- Evästeet. Evästeiden tarkoituksena on tallentaa tekstitiedostoja yksilöiden puhelimiin, tietokoneisiin ja muihin päätelaitteisiin, jotka keräävät tietoa yksilön toiminnasta verkossa automaattisesti ja huomaamattomasti. Evästeiden avulla organisaatiot voivat saada selville esimerkiksi verkkosivuilla vietetyn ajan ja klikkausten määrän.

Käyttäjän tottumuksia ja jokaista toimenpidettä voidaan seurata aktiivisesti ja kaikki data käyttäjän toiminnasta voidaan tallentaa yksityiskohtaisesti. Esimerkiksi tiedot käyttäjän suorittamasta tiedonhausta ja verkkosivuilla käytetystä ajasta voidaan yhdistää edelleen aikadatan avulla tapahtumajärjestyksen ja tarkan aikajanan selvittämiseksi. Kun tämän-

kaltainen data yhdistetään yksilön demografisiin tekijöihin ja muihin yksilöllisiin tietoihin, voidaan muodostaa tarkka ja kokonaisvaltainen kuva jokaisesta palvelua käyttävästä yksilöstä. Teknologisen kehityksen ansiosta datan tallentaminen ja kerääminen ovat mahdollista. Internetin kehityksen ansiosta verkosta on tullut yksi keskeisimmistä paikoista transaktioiden tekemiseen ja tiedonvaihtoon sekä datankeruun automatisoinnin myötä yksilöiden profilointi aiheuttaa poikkeuksellisen vähäisen määrän lisäkustannuksia tai ylimääräistä vaivaa organisaatioissa. (Wiedmann ym. 2001, 170–172.)

Wiedmann ym. (2001) puolestaan tarkastelevat artikkelissaan organisaatioiden datankeruun proseduureja asiakasdatan keruussa. Artikkelissa verkon kautta suoritettava datan kerääminen jaetaan reaktiiviseen ja proaktiiviseen datankeruuseen. Reaktiivisella datankeruulla artikkelissa tarkoitetaan tilanteita, joissa yksilö on tietoinen toimintansa seuraamisesta ja seurannan perusteella tapahtuvasta tietojen keräämisestä. Reaktiivista tiedonkeruuta suositaan tilanteissa, joissa halutaan kerätä sosiodemografisia ja psykografisia tietoja sekä tietoja yksilön ominaisuuksista, joita ei voida pelkän havainnoinnin avulla saada. Sosiografisella datalla tarkoitetaan muun muassa syntymäaikaa, koulutusta, sukupuolta ja tulotasoa. Psykografista dataa ovat puolestaan esimerkiksi yksilön kiinnostuksenkohteet, harrastukset ja mielipiteet. Proaktiivisessa tiedonkeruussa yksilö ei puolestaan ole tietoinen tiedonkeruusta ja proaktiivisessa tiedonkeruussa tämä nähdäänkin osaltaan olennaisena tiedonkeruun kannalta; koska yksilöt eivät tiedä tiedonkeruusta, saattavat he toimia ja käyttäytyä eri tavalla verrattuna tilanteeseen, jossa he olisivat tietoisia seurannasta ja datankeruusta. Toisaalta tämänkaltainen datankeruu on yksityisyyden suojan ja eettisyyden kannalta kyseenalaisempaa. Proaktiivisessa datankeruussa korostuu muun muassa yksilöiden käyttötottumusten havainnoiminen. Proaktiivista datankeruuta on kritisoitu muun muassa siitä, miten laajasti tietoa kerätään ilman käyttäjän suostumusta. Esimerkiksi jopa 60 prosenttia internetin käyttäjistä ei tiedä miten evästeiden käytöstä voidaan kieltäytyä. Kuviossa 5 esitellään artikkelin esittelemien reaktiivisen ja proaktiivisen datankeruun toteutustavat. (Wiedmann ym. 2001, 170–176, 181.)



Kuvio 5. Datankeruun menetelmät verkossa (Wiedmann ym. 2001)

Verkon toiminta datan siirtämisen osalta perustuu käyttäjän päätteen ja palveluntarjoajan palvelimen väliseen toimintaan. Lokitiedostot tallentavat automaattisesti tietoja palvelimen ja päätteen välisestä datan siirrosta. Yleisin lokitiedostomuoto on nimeltään ECLF (engl. Extended Common Log Format). Yleisimpiä ECLF-tiedoston tarjoamia tietoja ovat esimerkiksi käyttäjän IP-osoite, datansiirron kellonaika, käyttäjän palvelimelle lähettämä pyyntö, käyttäjän tunniste tai tunnus, tieto tiedonvaihdon onnistumisesta tai epäonnistumisesta, siirrettyjen tavujen määrä sekä tiedot käyttäjän aikaisemmin vierailemasta URL-osoitteesta, käyttöjärjestelmästä ja selainohjelmasta. Yhdistelemällä lokitiedostojen tallentamia tietoja voidaan jo profiloida käyttäjää tarkemmin. (Wiedmann ym. 2001, 173–174.) Sovellus- eli applikaatiolokit tallentavat tietoja käyttäjän sovelluksessa tekemistä valinnoista, painalluksista ja muusta toiminnasta, palvelinlokit puolestaan palveluntarjoajan palvelimessa tapahtuneista aktiviteeteista ja välipalvelinlokit toimivat ja tallentavat tietoja käyttäjän applikaatiolokin ja organisaation palvelinlokin välillä olevalta palveli-

melta. Sovelluslokit tuottavat tarkinta ja autenttisinta tietoa, kun taas palvelinlokit tuottavat epätarkinta ja yleisimmän tason tietoa; välipalvelinlokit ovat taas sovelluslokien ja palvelulokien välimaastossa tiedon tarkkuuden ja laadun suhteen. (Hussain ym. 2010.)

CGI-pohjaiset (engl. Common Gateway Interface) tiedostot tallentavat tietoja käyttäjän toiminnan seurauksena aiheutuneista tapahtumista, esimerkiksi aikaan sidottuja tietoja käyttäjän verkkosivun käyttötavoista ja siten täydentävät lokitiedostojen tarjoamia tietoja. Käyttäjän päätelaite ajaa CGI-pohjaisen ohjelmakoodin organisaation palvelimella. CGI-tiedostot voivat pohjautua käyttäjään, palvelimeen tai käyttäjän ajaman ohjelmakoodin kyselyyn. (Wiedmann ym. 2001, 172, 175.)

Erikoissovelluksia ovat aikaisemmin käsitellyn tekstitiedostopohjaisten evästeiden lisäksi ohjelmistoagentit, muunnellut verkkoselaimet, nuuskimet ja jäljitteet. Ohjelmistoagentti tarkoittaa ohjelmaa, joka voi tehdä käyttäjän puolesta tai käyttäjän avuksi tiettyjä määrättyjä toimenpiteitä. Esimerkiksi tiedonhakurobotit, sähköpostiohjelman suodattimet tai verkkosivuston chat-keskusteluissa toimivat botit ovat ohjelmistoagentteja. Ohjelmistoagentti voi tallentaa tietoja käyttäjän vuorovaikutuksesta agentin kanssa. Muunnelluissa selaimissa lähdekoodia on puolestaan muunnettu datan keräämisen edistämiseksi. Nuuskin (engl. packet-sniffing technology) on ohjelmistopohjainen teknologia, joskus myös päätelaitteen mikrosiru, joka analysoi, tarkkailee ja voi tallentaa käyttäjän kaikkea verkkoliikennettä. Nuuskimet ovat tehokas tapa saada paljon dataa käyttäjän huomaamatta. Nuuskimia voi käyttää verkkoa hallinnoiviin ja ongelmia ratkaiseviin tarkoituksiin tai käyttäjien tietojen kalasteluun ja muihin negatiivisiin tarkoituksiin. Koska nuuskimet voivat seurata kaikkea verkkoliikennettä, esimerkiksi salasanojen ja muiden arkaluontoisten tai kriittisten tietojen tallentaminen on myös mahdollista. (Wiedmann ym. 2001, 175; Ansari ym. 2003, 17.) Jäljitteet (engl. web bugs) voivat olla esimerkiksi erilaisia kuvia tai linkkejä, jotka lähettävät tietoja palvelimelle käyttäjän toiminnasta aina kun jäljitteen kanssa ollaan vuorovaikutuksessa. Yleinen esimerkki jäljitteestä on yrityksen sähköpostitse lähettämissä uutiskirjeissä olevat klikattavat linkit ja kuvakkeet. (Dobias 2010, 244–248; tsk.fi.)

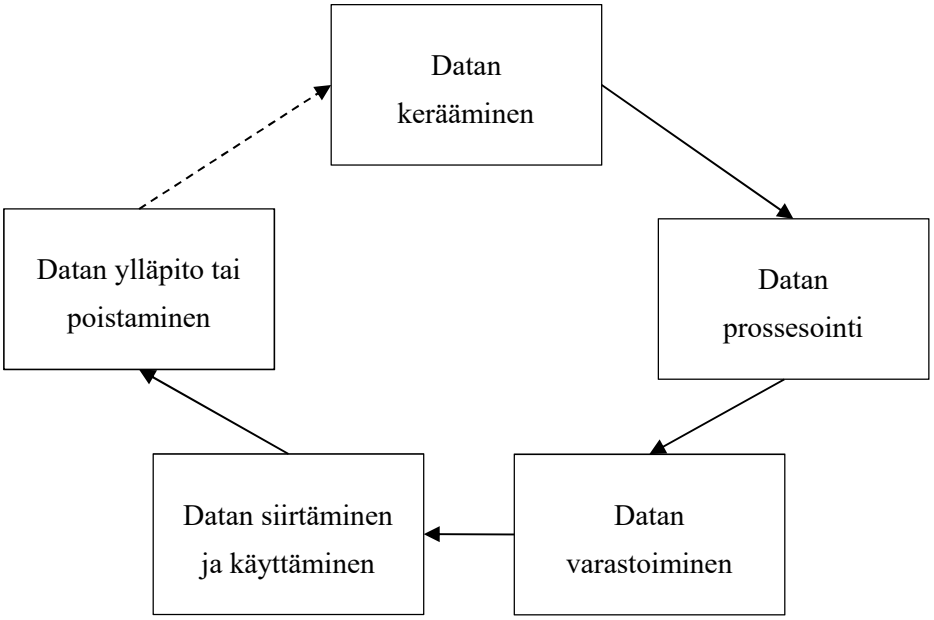
Reaktiivisessa datankeruussa tietoja voidaan saada lomakkeiden ja kaavakkeiden sekä erilaisten valikoiden avulla. Suljetuissa lomakkeissa rajoitetaan vastaamisvapautta esimerkiksi aiheen osalta tai vaihtoehtoisesti käyttäjää edellytetään syöttämään tarkasti määriteltyjä ja rajattuja tietoja. Avoimissa lomakkeissa sen sijaan käyttäjä on vapaa syöttämään tai kertomaan vapaammin omia tietojaan. Valikoissa puolestaan vastausvaihtoeh-

dot ovat tarkasti ja ennalta määriteltyjä. Reaktiivisen tiedonkeruun avulla yksilöistä saadaan pääsääntöisesti kolmeen eri ryhmään luokiteltavaa dataa: tunnistamiseen liittyvää dataa, kuvailevaa dataa ja kommunikaatiodataa. Tunnistamiseen liittyvä data voi olla esimerkiksi käyttäjän nimi, sähköposti, käyttäjätunnus tai puhelinnumero. Kuvailevan datan avulla organisaatiot puolestaan voivat tunnistaa yksilöiden uniikkeja ja yhteneväisiä preferenssejä. Yksilöiden ja organisaation välisestä yhteydenpidosta, neuvotteluista tai tilauksista puolestaan saadaan kommunikaatioon liittyvää dataa. (Wiedmann ym. 2001, 175–176.)

Datankeruutapoja tarkastelemalla voidaan huomata, että organisaatioiden mahdollisuudet saada tietoja yksilöistä ovat monipuolisia ja tehokkaita, usein myös teknisesti monimutkaisia ja tavanomaiselle käyttäjälle hankalasti ymmärrettäviä. Ymmärtämällä tietojen keräämiseen liittyviä metodeita ja teknologioita paremmin, voivat yksilöt tehdä harkitumpia ja perustellumpia päätöksiä.

2.7 Datan elinkaari

Koska tietojen luovuttamiseen liittyy lukuisia huolia ja riskejä, on olennaista huomioida myös yksilön luovuttaman datan elinkaari. Aina päätöksentekotilanteissa ei kuitenkaan tiedosteta dataan liittyvän elinkaaren pitkäkestoisuutta. Datan elinkaari alkaa tyypillisesti tietojen luovuttamisesta tai keräämisestä ja päättyy datan poistamiseen tai hävittämiseen. Lyhyesti sanottuna datan elinkaari tarkoittaa tietojen läpikäymiä vaiheita tietojärjestelmissä tietojen järjestelmään syöttämisestä aina tietojen poistamiseen asti. Elinkaaren jokainen vaihe edellyttää organisaatiolta tarpeellisia tietoturvaan ja tietosuojaan liittyviä toimenpiteitä yksilöiden yksityisyyden suojan varmistamiseksi, aina datan keräämisestä sen poistamiseen asti. Erityisesti nykyajan verkkopalveluissa on tyypillistä arkistoida tai tallentaa tietoja pysyvästi tai huomattavan pitkäksi aikaa ja usein samaa dataa voidaan hyödyntää useaan kertaan. On siis jopa mahdollista, että data saavuttaa elinkaarensa päätepisteen vasta hyvin kaukaisessa tulevaisuudessa. Datan elinkaaresta on esitetty kirjallisuudessa lukuisia malleja, mutta tässä tutkielmassa tarkastellaan lyhyesti tunnistettaviin tietoihin perustuva malli. (Michota & Katsikas 2015, 139–140; Arass ym. 2017.) Tunnistettavien tietojen käsitettä tarkastellaan tässä tutkielmassa luvussa 2.9.3. Tunnistettavien tietojen elinkaareen liittyvä malli on esitetty kuviossa 6.



Kuvio 6. Datan elinkaari (Michota & Katsikas 2015)

Mallin esittelemä datan elinkaari alkaa datan keräämisestä. Jo dataa kerätessä on keskeistä varmistaa datan tarkkuus ja virheettömyys. Datan keräämisen jälkeen data prosessoidaan ja samassa yhteydessä tallennetaan datankeruuseen liittyviä tietoja, kuten esimerkiksi tietoja siitä milloin ja miten data kerättiin. Seuraavaksi prosessoitu data varastoidaan käyttöä varten. Tämän jälkeen varastoitua dataa voidaan siirtää, julkaista, muokata tai käyttää. Kun dataa on hyödynnetty, voidaan tietoja päivittää, muokata tai poistaa. Mikäli tietoja ei poisteta, päivitetyistä tiedoista tulee ikään kuin uutta dataa, joka edelleen kerätään, prosessoidaan ja varastoidaan talteen. Sama sykli voi toistua siis lukuisia kertoja. (Michota & Katsikas 2015, 139–140; Arass ym. 2017.)

2.8 Datan käyttötarkoituksia

Organisaatioiden toiminta perustuu yhä enemmän datan keräämiseen ja sen hyödyntämiseen, koska verkossa voidaan kerätä käyttäjistä ja asiakkaista laaja skaala erilaisia tietoja. Koska yksityisyyden paradoksissa keskiössä on yksilöiden luovuttama data organisaatioille, seuraavaksi tarkastellaan lyhyesti organisaatioiden keskeisiä tapoja hyödyntää yksilöitä koskevaa dataa toiminnassaan. Organisaation esittämällä tietojen käyttötarkoituksella tai käyttäjän uskomuksilla tietojen käyttötarkoituksista voi olla vaikutuksia yksilön päätöksentekoprosesseihin, tehtyihin valintoihin tai muodostettuihin aikomuksiin.

2.8.1 Personointi

Verkkoliiketoiminnan ja kilpaillun kasvaessa asiakassuhteiden luominen ja ylläpito on tuonut lukuisia uusia haasteita. Kuluttajien tarpeet on pyrittävä tyydyttämään yhä tehokkaammin ja kilpailukykyisemmin. Personointi tarkoittaa relevantin tiedon, markkinoinnin, tuotteen tai palvelun kohdentamista yksilön tai ryhmän tarpeisiin kuluttajista ja asiakkaista kerätyn tiedon perusteella. Personointi on vahvasti riippuvaista käyttäjien tarjoamista henkilökohtaisista tiedoista. (Fan & Poole 2006, 179–180.) Personoinnissa on tarkoituksena parantaa asiakastyytyväisyyttä ja tehostaa myyntiä, eikä tyypillistä ole kilpailla pelkästään hinnalla, vaan ennemminkin tuotteen tai palvelun ominaisuuksilla (Liang ym. 2012, 275–278). Asiakastyytyväisyydellä tarkoitetaan asiakkaan muodostamaa arviota yrityksen suorituskyvystä vertaamalla ennakkoon muodostettuja odotuksia ja transaktiolla saavutettuja lopputuloksia (Caruana 2002, 815). Wun ym. (2003) mukaan personointi puolestaan on tehokas ja moderni tapa suunnitella ja hyödyntää tietojärjestelmiä vastaamaan kuluttajien ja asiakkaiden yksilöllisiä vaatimuksia. Tietojärjestelmätieteen mukaan personoinnissa on keskeistä asiakasdatan ja sen hyödyntäminen sekä personoinnin vaatiman teknologian ja yksilöiden tarpeiden huomiointi (Sunikka & Bragge 2012, 10049–10050).

Läheisesti personointiin liittyviä käsitteitä ovat segmentointi, profilointi ja kustomointi. Siinä missä segmentointi ja profilointi ovat personoinnissa hyödynnettäviä toimintatapoja, kustomointi viittaa asiakkaan aktiiviseen osallistumiseen personointiprosessissa ja ratkaisujen löytämisessä. Personointi on siis organisaation itse suorittamaa, kun taas kustomoinnissa personointiprosessi tapahtuu asiakkaan ja yrityksen välisessä vuorovaikutuksessa ja toiminnassa. (Fan & Poole 2006, 179–180; Ho & Bodoff 2014, 498.)

Personoinnin avulla voidaan vähentää uusasiakashankinnan tarvetta ja parantaa olemassa olevien asiakkaiden lojaaliutta ja sitoutumista asiakassuhteeseen. On jopa viisi kertaa kalliimpaa hankkia uusia asiakkaita kuin säilyttää vanhoja asiakkaita. Vanhat ja lojaalit asiakkaat luovat yritykseen myös tasaista kassavirtaa ja ovat usein täysin uusia asiakkaita kannattavampia ja halukkaampia kokeilemaan organisaation uusia tuotteita ja palveluja. (Desouza & Awazu 2005, 42.) Kilpailijoiden on digitalisoituneessa ja globaalissa liiketoimintaympäristössä helppo kopioida ja seurata muita alan yrityksiä, mutta yksilöistä kerättyä dataa ja siitä jalostettua informaatiota tai tietämystä taas on hyvin vaikeaa tai jopa mahdotonta kopioida (Lesser ym. 2000, 36–37). Yritykset voivat löytää uusia liiketoimintamahdollisuuksia tai parantaa tarjoamaansa asiakkaidensa preferenssien ja

tarpeiden pohjalta. Asiakastietoja ja analytiikkaa hyödyntämällä on mahdollista tunnistaa ja tyydyttää myös määrittelemättömiä ja piileviä tarpeita. Syvällisellä asiakkaan ymmärtämisellä ja personoiduilla ratkaisuilla voidaan luoda kilpailuetua. (Jayachandran ym. 2014, 219–221.)

Yksilöiden ja organisaation ulkopuolisten näkökulmasta personointi parantaa transaktioon liittyvien prosessien sujuvuutta ja käyttökokemusta, kun organisaatiot tunnistavat yksilön tarpeet ja luovat näihin personoituja ratkaisuja (Liang ym. 2012, 275–277). Personoinnilla pystytään myös vähentämään yksilöön kohdistuvaa markkinoinnin ja tietojen ylikuormitusta (Ansari & Mela 2003, 131) ja useat tuotteet tai palvelut voidaan tarjota yksilöille ilmaiseksi tai edullisemmalla hinnalla (Christiansen 2011, 509). Suurin haaste organisaatiolle ja suurin riskitekijä yksilölle on kuitenkin personoinnista aiheutuvat tietoturvariskit ja yksityisyyden suojan heikkeneminen (Li & Unger 2012, 621–624).

2.8.2 Innovointi sekä tutkimus- ja kehittämistoiminta

Osittain ja läheisesti personointiin liittyen, yksilöistä kerätyn datan hyödyntämisellä on yhä enenevissä määrin potentiaalia synnyttää uudenlaisia innovaatioita. Innovointi on prosessi, jonka lopputuloksena hyödynnetään uudenlaisia prosesseja, tuotteita, palveluita tai uudenlaista tietämystä muun muassa liiketoiminnan harjoittamisessa. Innovaatioiden avulla voidaan yksilöistä kerätystä datasta saada aikaan merkittäviäkin muutoksia, esimerkiksi uusien liiketoimintamallien ja -mahdollisuuksien syntymistä. (Zillner ym. 2016, 171.)

Tutkimus- ja kehittämistoiminta (t&k) on systemaattista toimintaa, jonka tavoitteena on löytää uusia sovellutuksia tai toimintatapoja. Tutkimus- ja kehittämistoimintaan lukeutuvat seuraavat kolme osa-aluetta (Tilastokeskus 2020):

- Perustutkimus, jonka tavoitteena on luoda uutta tietoa tai tehdä uusia havaintoja eikä tarkoituksena ole soveltaa tietoa vielä käytännössä.
- Soveltava tutkimus, joka tähtää uuden käytännön sovellutuksen löytämiseen.
- Kehittämistyö eli tuote- ja prosessikehitys, jonka avulla voidaan kehittää uusia prosesseja, tuotteita, palveluita ja järjestelmiä.

Siinä missä tutkimus- ja kehittämistoiminta on uuden tietämyksen ja toimintatapojen etsimistä, innovointi puolestaan on tutkimus- ja kehitystoiminnassa syntyneen tiedon ja lopputulosten hyödyntämistä käytännössä.

2.8.3 Poaching

Organisaatioiden hyödyntäessä yksilöihin liittyviä tietoja on yksilön näkökulmasta aina myös riski siihen, että organisaatio päätyy väärinkäyttämään yksilön luovuttamia tietoja. Clemonsin ja Hittin (2004) mukaan poaching viittaa tilanteeseen, jossa organisaatio käyttää keräämiään tietoja sopimuksessa mainitsemattomiin tai sopimuksen ulkopuolisiin tarkoituksiin. Tämä sopimuksenvastainen tietojen hyödyntäminen aiheuttaa haittaa sopimuksen toiselle osapuolelle, mutta kerryttää organisaatiolle puolestaan taloudellista hyötyä. Termille poaching ei ole olemassa suomenkielistä vastinetta, joten tässä tutkielmassa käytetään englanninkielistä termiä. Poaching-ilmiössä on lyhyesti sanottuna kolme keskeistä piirrettä (Clemons & Hitt 2004, 94):

- Kahden osapuolen välillä on solmittu sopimus tiedon jakamisesta tuotteen tai palvelun vastaanottamiseksi. Tiedonjako on välttämätöntä sopimuksen toteutumiselle.
- Tietoja vastaanottava ja keräävä osapuoli hyödyntää tietoja tarkoituksiin, joista ei olla sovittu sopimuksessa, motiivinaan saavuttaa taloudellisia hyötyjä ja edistää omaa etua.
- Tietoja keränneen osapuolen toiminta aiheuttaa haittaa tai taloudellista menetystä tietoja luovuttaneelle osapuolelle.

Poaching on käytännössä transaktioihin ja sopimuksiin liittyvä riskitekijä. Ilmiö lukeutuu pohjimmiltaan osaksi laajempaa opportunismin käsitettä, jolla tarkoitetaan tilannetta hyväksikäyttävää käytöstä moraalisia näkökulmia huomioon ottamatta. Poaching viittaa kuitenkin juuri tiedonvaihtoon perustuviin tilanteisiin ja se on seurausta palvelukeskeisen ja tiedon hyödyntämiseen perustuvan yhteiskunnan kehityksestä. Kehityksen jatkuessa edelleen on yhä olennaisempaa tiedostaa ilmiön tuomat riskit. Poaching on myös yleinen ilmiö ja riskitekijä yritysten välisillä B2B-markkinoilla yksilön ja yrityksen välisten B2C-markkinoiden lisäksi. Poaching liittyy läheisesti myös muihin opportunistisiin ongelmiin, kuten organisaation mahdollisuuksiin hyväksikäyttää toista osapuolta sopimuksen suuren neuvotteluvoiman nojalla tai asiakasosapuolen rajallisiin keinoihin tarkkailla organisaation alisuoriutumista sopimussuhteessa. Poachingia edesauttavat esimerkiksi tietojen käyttöön liittyvän sopimuksen ulkopuolisen käytön tarkkailun ja havaittavuuden vaikeus. (Clemons & Hitt 2004, 88–91, 94–97, 105.)

2.9 Tietojen tunnistettavuus

Yksityisyyden näkökulmasta on hyvinkin olennaista se, että internetin laajenemisen ja digitalisaation myötä yksilöiden kaikesta toiminnasta verkkoympäristöissä jää jonkinlainen digitaalinen jalanjälki, jota organisaatiot voivat hyödyntää toiminnassaan ja tietojen keräyksessä. Usein varsin epätarkkojen sekä mitättömiltä ja merkityksettömiltä vaikuttavien tietojenkin avulla on mahdollista muodostaa kohtuullisen tarkkoja profiileja yksilöistä. Vaihtoehtoisesti tämänkaltaisia tietoja voidaan hyödyntää olemassa olevien profiilien täydentämiseen ja rikastamiseen. (Li & Unger 2012, 621–622.)

Yksilöiden huolet yksityisyyden suojan näkökulmasta eivät rajoitu pelkästään tietoihin, joiden avulla heidät voidaan tarkasti tunnistaa, vaan myös epätarkemmat tiedot ovat osaltaan nostaneet yksilöiden huolia yksityisyydestä. Kerättyjen tietojen tarkkuutta arvioitaessa on muun muassa huomioitava se, että tarkempien ja yksityiskohtaisempien tietojen kerääminen, analysointi ja hyödyntäminen mahdollistavat tarkemman profiloinnin ja siten esimerkiksi käyttäjäystävällisemmän, räätälöidymmän ja paremmin tarpeita vastaavan tuotteen tai palvelun saamisen. (Cho & Fiorito 2009, 392.)

Yksilöistä kerättävät tiedot voidaan pääsääntöisesti jakaa kolmeen eri pääluokkaan, jotka ovat anonyymit tiedot, tunnistamattomat tiedot ja tunnistettavat tiedot (Chellappa & Sin, 2005, 187–188).

2.9.1 Anonyymit tiedot

Anonyymit tiedot ovat tietoja, jotka voidaan kerätä yksilöiltä täysin huomaamattomasti, ilman minkäänlaisia näkyviä tai tunkeilevia kyselyjä ja pyyntöjä esimerkiksi verkkosivukäyntien yhteydessä. Anonyymien tietojen avulla tai yhdistämällä anonyymejä tietoja muuhun dataan yksilöä ei voida suoraan tunnistaa eikä tunnistaminen ole mahdollista ilman poikkeuksellisen suurta vaivannäköä. Anonyymejä tietoja ovat esimerkiksi kaikissa internetissä suoritettavissa klikkauksissa ja pyynnöissä siirtyvät ja välittyvät tiedot, kuten muun muassa laitteen IP-osoite ja käyttöjärjestelmä, paikallinen kellonaika, käytettävä selain, selaimen kieli ja versionumero. (Chellappa & Sin 2005, 187–188.)

Anonyymeistä tiedoista erityisesti IP-osoitteen on kritisoitu luovan virheellistä yksityisyyden, turvallisuuden ja anonyymiyden tunnetta, sillä IP-osoitteen avulla pystytään usein yksilöimään käyttäjää tai jopa tunnistamaan ja paikantamaan laitteen käyttäjä. IP-osoitteella tarkoitetaan internetin protokollaosoitetta, eli jokaiselle laitteelle uniikkia ja yksilöityä numerosarjaa, jonka avulla laitteet voivat kommunikoida keskenään laitteiden

välisessä verkostossa. IP-osoitteen avulla saadaan selville vähintäänkin esimerkiksi laitteen karkea sijainti. (Schwartz & Solove 2011, 1837–1841.)

2.9.2 Tunnistamattomat tiedot

Tunnistamattomat tiedot (engl. Personally Unidentifiable Information, PUI) ovat tietoja, joiden perusteella ei ole yksinään mahdollista identifioida tai paikallistaa käyttäjää tarkasti, mutta niiden avulla voidaan luoda paikkansapitäviä ja toimivia nimettömiä profiileja yksilöistä. Osa tunnistamattomista tiedoista on yksilöiden itse verkkoon luovuttamia tai syöttämiä muun muassa erilaisten valikoiden tai valmiiden valintaruutujen välityksellä, kuten sukupuoli, koulutus, ikä, syntymäaika, harrastukset, postinumero ja tulotaso. Toinen osa tunnistamattomista tiedoista on erilaisten seurantateknologioiden, kuten verkkojäljitteiden ja evästeiden avulla saatuja ja kerättyjä tietoja. Evästeiden avulla palvelun tarjoaja voi tallentaa tietoja käyttäjän päätelaitteelle ja välittää tietoja takaisin palvelun-tarjoajalle esimerkiksi käyttäjän verkkosivun käyttötottumuksista. Tunnistamattomat tiedot ovat siis huomattavasti yksityiskohtaisempia tietoja kuin anonyymit tiedot, mutta eivät täysin yksilön identiteettiä paljastavia tietoja. (Chellappa & Sin 2005, 188; Cho & Fiorito 2009, 392.)

2.9.3 Tunnistettavat tiedot

Yksityiskohtaisimpia ja tarkimpia yksilöistä kerättäviä tietoja nimitetään tunnistettaviksi tiedoiksi (engl. Personally Identifiable Information, PII). Tunnistettavien tietojen avulla yksittäinen ihminen voidaan helposti tunnistaa, identifioida ja paikantaa. Nämä tiedot riittävät yksinään yksilön tunnistamiseen, mutta tunnistettavia tietoja voidaan myös yhdistää muihin yksilöistä kerättyihin tai julkisesti saatavilla oleviin tietoihin. Rajanveto tunnistettavien ja tunnistamattomien tietojen välillä voi olla usein haastavaa ja raja voikin vaihdella tapauskohtaisesti. (Narayanan & Shmatikov 2010, 24–26.)

Organisaatiot keräävät tunnistettavia tietoja vain yksilöiltä itseltään ja yksilön suostumuksen nojalla, esimerkiksi verkkosivulle tarkoitetun käyttäjätilin luonnin tai transaktioiden tekemisen yhteydessä. Esimerkiksi nimi, osoite, matkapuhelinnumero, henkilötunnus ja luottokortin tunnus ovat yksilön tunnistettavia tietoja. (Chellappa & Sin 2005, 188.) Tunnistettavien tietojen käsite on hyvin lähellä henkilötiedon käsitettä. Henkilötietojen määritelmä voi vaihdella esimerkiksi kansallisen lainsäädännön tai julkisten toimijoiden takia eri maiden tai alueiden välillä. Esimerkiksi Euroopan komissio määrittelee

henkilötiedoiksi kaikki sellaiset tiedot, jotka liittyvät joko tunnistettuun tai tunnistettavissa olevaan henkilöön sekä tiedot, jotka yhdistettyinä muihin tietoihin mahdollistavat tietyn yksittäisen henkilön tunnistamisen. Esimerkkejä komission mukaan henkilötiedoista ovat muun muassa etunimet ja sukunimi, sähköpostiosoite, kotiosoite, IP-osoite ja matkapuhelimen paikannustiedot. Tiedot, joita voidaan salauksesta, anonymisoinnista tai pseudonymisoinnista huolimatta käyttää henkilön tunnistamiseen ovat myös henkilötietoja. Jos henkilötieto anonymisoidaan peruuttamattomasti ja siten, ettei henkilö ole enää tunnistettavissa, tietoa ei enää lueta henkilötiedoksi. (European Commission 2020.) Pseudonymisoinnilla tarkoitetaan henkilötietojen käsittelyä sillä tavalla, että henkilötietoja ei voida enää lähtökohtaisesti yhdistää tiettyyn henkilöön ilman lisätietoja, esimerkiksi korvaamalla jokin henkilön tieto toisella tiedolla tietokannassa. Anonymisoinnilla tarkoitetaan puolestaan tietojen käsittelyä tavalla, että henkilöä ei voida enää tunnistaa kyseisistä tiedoista, esimerkiksi tietoa voidaan karkeistaa yleisemmälle tasolle. (Tietosuoja.fi/pseudonymisointi-anonymisointi.)

Schwartzin ja Soloven (2011) mukaan tunnistettavat tiedot ovat lainsäädännön näkökulmasta yksi tärkeimmistä ja keskeisimmistä käsitteistä yksityisyyteen liittyvissä säännöksissä. Heidän mukaansa tunnistettavien tietojen (PII) käsitettä tulisi uudistaa niin sanotuksi PII 2.0 -malliksi, sillä tunnistettavien tietojen käsitteen rajat muun muassa lainsäädännössä voivat olla epäselviä. PII 2.0 mallissa yksilön tiedot voivat liittyä yhteen kolmenlaisesta henkilöstä: tunnistettuun henkilöön (eli henkilö ja hänen identiteettinsä on tunnistettu), tunnistettavissa olevaan henkilöön (eli henkilöä ei ole identifioitu eikä tunnistaminen ole todennäköistä, mutta se on mahdollista) tai ei-tunnistettavissa olevaan henkilöön (eli tietoja ei ole lähtökohtaisesti mahdollista hyödyntää yksilön tunnistamiseen tai sen riski on olemattoman pieni). PII 2.0 mahdollistaisi lainsäädännön näkökulmasta enemmän liikkumavaraa yksityisyyteen liittyvissä ongelmissa ja se ottaisi huomioon eri riskitasoja yksityisyyteen liittyen kolmen henkilökategoriansa perusteella, verrattuna yleisesti käytettyyn tunnistettavien tietojen käsitteeseen. Hyödyksi PII 2.0 -mallissa kuvaillaan myös PII 2.0 -mallin luovan kannustimen organisaatioille pitämään yksilöistä kerätyn datan mahdollisimman tunnistamattomassa tai vähäriskisessä muodossa, koska perinteinen tunnistettavien tietojen käsite ei luo samalla tavalla eroa tunnistetun ja tunnistettavissa olevan yksilön välillä. (Schwartz & Solove 2011, 1816, 1877–1879, 1883.)

2.10 Privacy calculus: yksityisyys vaihdannan välineenä

Yksilöiden tuottamilla ja jakamilla tiedoilla on nykyään yhä selkeämmin taloudellista arvoa, sillä data on yhä keskeisempi resurssi organisaatioiden toiminnassa. Asiakasdata, asiakasymmärrys ja profilointialgoritmit ovat nykyään liikesalaisuuden piiriin kuuluvia voimavaroja. (Malgieri & Custers 2018, 289–290.) Erityisesti yksityisyyden paradoksin ja big datan myötä on noteerattu näkökulma yksityisyydestä eräänlaisena hyödykkeenä. Näkökulmasta riippumatta yksityisyys nähdään edelleen yksilön oikeutena ja sosiaalisesti tärkeänä arvona, vaikka yksityisyyttä tarkasteltaisiin hyödykkeenä. Hyödykenäkökulmassa keskitytään yksityisyyden vaihdannalliseen puoleen; yksityisyys toimii esimerkiksi maksuvälineenä, jolle voidaan asettaa rahallinen arvo tai sitä voidaan käyttää vastineena rahalliselle suoritukselle. (Smith ym. 2011, 993–994.) Stanton ym. (2007, 1–3) sanovat yksityisyyden olevan rajoitettu hyödyke, sillä ihmisillä on tarpeita ja halukkuutta luopua osittain yksityisyydestään.

Privacy calculus tarkoittaa sitä, että yksityisyyttä käsitellään ja ajatellaan eräänlaisena vaihdannan välineenä tai hyödykkeenä. Yksilöt voivat tämän ajattelutavan mukaan aikeita ja päätöksiä muodostaessaan harkita miten hyödyt suhtautuvat menetettyyn tai heikentyneeseen yksityisyyteen. Toisin sanoen kuluttajat analysoivat aiheutuvia hyötyjä ja haittoja. (Wilson & Valacich 2012, 2–3.) Privacy calculus -teoria on kehittynyt Laueferin ja Wolfen vuonna 1977 kehittämästä calculus of behavior -teoriasta (Dinev & Hart 2006, 62). Calculus of behavior -teorian mukaan yksilöt punnitsevat ja ajattelevat omasta käyttäytymisestään tulevaisuudessa aiheutuvia seurauksia (Laufer & Wolfe 1977, 35–37). Esimerkiksi taloudellisesta näkökulmasta katsottuna yksilöt vertaavat toiminnastaan aiheutuvia kustannuksia ja realisoituvia hyötyjä tai etuja (Li ym. 2010, 63). Privacy calculus -teoria on esimerkki yksilöiden rationaalisesta käytöksestä (Barth & de Jong 2017, 1041). Teorian mukaan odotettu hyöty vaikuttaa positiivisesti yksilön käyttäytymisaikeisiin ja odotettujen yksityisyyden suojan vähenemiseen liittyvien haittojen vaikuttavan negatiivisesti käyttäytymisen aikeisiin. Privacy calculus -teoriaa on hyödynnetty useimmiten erityisesti aikeiden tutkimuksessa. Privacy calculus -teorian mukaisesti yksilöt siis pyrkivät maksimoimaan positiivisia lopputulemia ja minimoimaan negatiivisia seurauksia. (Keith ym. 2013, 1165.) Yksilölle aiheutuvat kustannukset ovat usein abstrakteja, vaikeasti laskettavissa tai aineettomia. Privacy calculus -teorian mukaan yksilö päätyy luovuttamaan tiedot, mikäli oletetut saavutettavat hyödyt ylittävät oletetut aiheutuvat kus-

tannukset. Teorian mukaan siis yksilö voi edelleen periaatteessa olla huolissaan tai epävarma yksityisyyden suojastaan toiminnastaan huolimatta; privacy calculus -teoria siis osittain selittää ristiriitaisuuksia yksilön huolten, asenteiden, aikeiden ja käytöksen välillä. (Gerber ym. 2018, 229.)

Vaikka privacy calculus -teoria kehittyi tunnettuun muotoonsa vasta Culnanin ja Armstroning vuonna 1999 julkaistun artikkelin pohjalta (Kehr ym. 2015, 608), ajatustapa yksityisyyden arvosta ja yksityisyyden suojan heikkenemisestä aiheutuvista haitoista on ollut esillä yksityisyyttä käsittelevässä tutkimuksessa jo pitkään (ks. esim. Gavison 1980, 423, 441).

Privacy calculus -teorian taustalla on selkeä ajatus yksilön henkilökohtaisten tietojen arvosta. Yksityisyydellä voi olla yksilöille itselleen arvoa, mutta arvoa käsiteltäessä tutkimuksissa keskitytään yleensä yksityisyyden konkreettisempaan arvoon, esimerkiksi taloudellisesta näkökulmasta käsin. Koska organisaatiot ovat valmiita luovuttamaan tuotteita tai palveluja yksilön käyttöön ilman rahallista suoritusta tai edullisemmin yksilön tietojen keräämiseen johdosta, on perusteltua ajatella heikentynyttä yksityisyyttä ja luovutettuja tietoja eräänlaisena maksuna. Luovutetut tiedot eivät kuitenkaan ole suoraan verrattavissa rahaan, sillä usein tiedonjakoa ei voida korvata täysin rahallisella maksulla. Privacy calculus -teorian mukainen kustannusten ja hyötyjen analyysi on yksi yksilöiden monimutkaisiin päätöksentekoprosesseihin vaikuttavista tekijöistä. (Li ym. 2010, 62–64.)

Koska privacy calculus -teorian ytimessä on ajatus yksityisyyden vaihdannallisuudesta, olisi käytännön näkökulmasta tärkeää kehittää malli, joka ratkaisisi datan hinnoitteluun ja markkinoilla taloudellisen näkökulman käyttöönottoon liittyvät ongelmat. Toimivaksi tavaksi on esitetty yksilön valinnanvaraa transaktion maksamisessa; yksilö voi joko maksaa kulut rahalla tai luovuttamalla henkilökohtaisia tietojaan organisaatioiden käyttöön ja antamalla suostumuksensa profilointiin. Varsinaisessa datan taloudellisen arvion määrittämisessä voidaan hyödyntää kahta lähestymistapaa. Ensimmäisessä niin sanotussa ylhäältä alas -lähestymistavassa keskitytään datan tarjontaan, kun taas toisessa alhaalta ylös -lähestymistavassa keskitytään datan kysyntään. Tarjontaan keskittyvässä näkökulmassa on keskeistä löytää parametri, jonka perusteella organisaatiot voivat maksaa yksilön datasta. Kysynnän näkökulmasta taas pohdittaisiin sitä, kuinka paljon yksityisyyden suojan heikkeneminen tuottaa vahinkoa yksilölle. Datankin arvonmäärityksessä sovellettaisiin markkinoiden keskeistä kysynnän ja tarjonnan lakia, eli hinta määräytyisi markkinoilla kysynnän ja tarjonnan mukaan (Malgieri & Custers 2018, 289–297.)

Datan arvon määrittämisessä on kuitenkin lukuisia ongelmia. Ensinnäkin tarkemmat metodit datan hinnoittelun analysointiin ja toteuttamiseen voivat tuottaa haasteita. Henkilökohtaiset tiedot muuttuvat ajansaatossa ja voivat siten vanhentua tai tulla käyttökelvottomiksi. Samoja tietoja voidaan myös kopioida, hyödyntää muihin käyttötarkoituksiin tai myydä ulkopuolisille. Yksilön henkilökohtaisten tietojen arvon hinnoittelua voidaan lisäksi pitää moraalisesti kyseenalaisena. Esimerkiksi vähävaraisten ihmisten alhaisemman ostovoiman ja kulutusalttiuden takia heidän tietonsa voisivat olla vähäarvoisempia kuin varakkaiden ihmisten tuottama data. Tämä asettaisi yksilöt eriarvoiseen asemaan ja mahdollistaisi sopimusehtojen muokkaamisen yksilöstä riippuen. Yksityisyyden ollessa osa ihmisten oikeuksia, on aiheellista kyseenalaistaa henkilökohtaisten tietojen laajempi hyödykkeellistäminen ja hinnoittelu. Idea datan hinnoittelusta on saanut osakseen monenlaista muutakin kritiikkiä: henkilökohtaiset tiedot ovat aineettomia, osittain dynaamisia ja kontekstisidonnaisia, yksityisyyttä on hankalaa mitata rahassa, identiteettivarkauden tai muiden väärinkäytösten riski on vaikea huomioida hinnoittelussa ja tietojen todellisen kokonaisarvon laskeminen ei ole käytännössä realistista. Yksilöiden kognitiivisten rajoitteiden vuoksi on myös mahdollista, että datan hinnoittelu ja tieto datan taloudellisesta arvosta ei vaikuttaisi osaan ihmisistä ollenkaan. Yksilöille on tyypillistä yksinkertaisesti sivuuttaa tai jättää huomioimatta yksityisyyden suojaan liittyvää tietoa. Hyvänä esimerkkinä toimivat organisaatioiden selosteet yksityisyyden suojasta ja datan hyödyntämisestä. Yksilöt harvoin lukevat yksityisyyden suojaan koskevia selosteita kokonaan tai ollenkaan. (Malgieri & Custers 2018, 289–297.)

Yksilöiden on usein hankalaa ymmärtää tai ajatella henkilökohtaisten tietojensa taloudellista arvoa. Mikäli kuluttajat olisivat tietoisempia omien henkilökohtaisten tietojensa arvosta, he voisivat paremmin ja tehokkaammin suojata yksityisyyttään sekä ymmärtää omien henkilökohtaisten tietojensa olevan suuri voimavara organisaatioille. Yksilöiden tietoisuus ja ymmärrys datalähtöisessä liiketoimintaympäristössä ja yhteiskunnassa on askel yksilöiden etujen ajamiseksi, koska yksilöt voivat siten rajoittaa datan rajatonta ja vapaata keräämistä sekä kohdistaa huomiota ihmisten oikeuksiin ja yksityisyyden suojaan. Yksilöiden pitäisi saada paitsi tietoa henkilökohtaisten tietojensa taloudellisesta arvosta, mutta myös tietoja datan keräämisestä, oikeuksia kontrolloida organisaatioiden mahdollisuuksia kerätä ja käyttää dataa, mahdollisuuksia korjata virheellistä dataa ja oikeutta pyytää datan poistoa. Yksilön oikeuksia datan keräämiseen, käyttöön ja poistamiseen liittyen on pyritty huomioimaan muun muassa Euroopan unionin yleisessä tietosuoja-asetuksessa eli GDPR:ssä (engl. General Data Protection Regulation). (Malgieri

& Custers 2018, 289, 297–302.) GDPR:n ensisijaisena tavoitteena on ollut tarjota yksilöille mahdollisuutta saada parempi kontrolli omista henkilökohtaisista tiedoistaan. Keskeisimpiä hyötyjä ovat oikeus tulla unohdetuksi, eli oikeus pyytää tietojen poistamista, lisääntynyt läpinäkyvyys yksilöille datan prosessoinnista, datan siirtämisen helpottuminen eri palveluntarjoajien välillä, oikeus tietää organisaatioiden tietomurroista ja organisaatioiden velvollisuus huolehtia tietosuojasta oletusarvoisesti jo suunnitteluvaiheesta lähtien. (European Commission 2018.)

Yksityisyyden ja datan arvoon liittyvässä keskustelussa on tärkeää myös huomioida taloudellisen arvon lisäksi yksilöiden henkilökohtaisia arvostuksia ja arvokäsityksiä dataa ja yksityisyyttä kohtaan. Organisaatioiden kohdalla painottuu erityisesti henkilökohtaisten tietojen taloudellinen arvo. Yksilöt pitävät yksityisyyteen liittyviä seikkoja usein jo itsessään arvokkaina, kuten esimerkiksi datan kontrollointimahdollisuuksia (muun muassa tietojen muokkaamista ja poistamista), anonyymisyyttä ja tietoturvaa (Rantanen 2019, 32–36).

Lin ym. (2010) mukaan puhdas taloudellinen näkökulma verkossa tapahtuvien transaktioihin liittyvään tietojen jakamiseen on kiistanalainen. Tietojen jako on yleensä niin sanotusti sivuvaikutusta varsinaisesta vaihdannasta, joka on pääsääntöisesti konkreettisten tuotteiden tai palveluiden ja rahan vaihtokauppaa. Esimerkiksi verkosta ostetun tuotteen toimittaminen asiakkaalle edellyttää yhteystietojen luovuttamista. Toisin sanoen verkossa tapahtuvat transaktiot ovat ennen kaikkea liiketoimen mahdollistajia, eivätkä ne aina perustu pelkkään asiakasdatan keräämiseen. Organisaatiot tarjoavat taloudellisia etuja käyttäjilleen tai asiakkailleen liiketoimen suorittamisen rohkaisuksi, eivätkä pelkästään houkutellakseen käyttäjiä luopumaan yksityisyydestään. (Li ym. 2010, 62–63.) Kun data tai yksityisyys toimii liiketoimessa vaihdannan välineenä, voidaan tunnistaa kolmentyylisiä transaktioita (Malgieri & Custers 2018, 292):

- Verkkopalvelujen tarjoaminen alhaisemmalla hinnalla tai ilmaiseksi. Esimerkiksi ilmainen WLAN-verkkoyhteys selaushistoriaa ja paikannusdataa vastaan.
- Arvokkaan verkkosisällön tarjoaminen alhaisemmalla hinnalla tai ilmaiseksi. Esimerkiksi pääsy Spotifyn tekijänoikeuksien alaiseen musiikkikirjastoon Facebookin profiilidataa luovuttamalla.
- Verkon ulkopuolisten palveluiden tarjoaminen alhaisemmalla hinnalla tai ilmaiseksi. Esimerkiksi sairasvakuutuksen tarjoaminen halvemmalla yksilön terveyttä monitoroivien laitteiden tietoja vastaan.

Vaihtoehtoisesti tiedonjakoon perustuvia transaktioita voidaan luokitella toisellakin tavalla. Niin sanotussa yhdistelmätransaktiossa (engl. composite transaction) organisaatio tarjoaa kuluttajalle tuotteita tai palveluita ja informaatiota näistä transaktion kohteista sekä kuluttajat maksavat rahalla, henkilökohtaisilla tiedoillaan tai molemmilla. Informaatiotransaktiossa (engl. information transaction) puolestaan liikkuu pelkästään tietoa, yleensä kuluttajalta yritykselle. Dataa koskeviin transaktioihin ja tietojen hinnoitteluun liittyen on ehdotettu käytettäväksi niin sanottua aktiivisen valinnan mallia. Kuluttajat voisivat siis itse päättää hankkivatko he tuotteen tai palvelun maksamalla rahaa ilman suostumusta tietojen keräämiseen tai vaihtoehtoisesti transaktio suoritetaan pelkästään henkilökohtaisia tietoja jakamalla kuluttajan omasta suostumuksesta. (Malgieri & Custers 2018, 292.)

2.10.1 Tietojenluovutuksen hyödyt

Yksilön ehkä yleisimmistä motivaatiotekijöistä harkita henkilökohtaisten tietojensa luovuttamista organisaatiolle on tietojen luovuttamisesta realisoituvat hyödyt ja etuudet. Hyödyt voivat olla joko konkreettisia ja taloudellisia, tai abstrakteja ja aineettomia.

Taloudellisia perusteita tietojen jakamiselle ovat esimerkiksi tuotteesta tai palvelusta saatavat hinnanalennukset sekä erilaiset tulot ja tuotot. Käyttäjä voi saada alennusta esimerkiksi verkkokauppaostoksistaan luovuttamalla sähköpostiosoitteensa ja tilaamalla yrityksen uutiskirjeen. Osa internetin digitaalisista palveluista voivat myös olla käyttäjille täysin ilmaisia tietojen luovuttamisen jälkeen. Tuloista ja tuotoista voidaan mainita esimerkkinä Brave-verkkoselain, jonka avulla yksilöt voivat tienata rahaa digitaaliseen lompakkoon muun muassa jakamalla Bravelle tietojaan ja jaettujen tietojen perusteella käyttäjät saavat mainoksia. Brave jakaa osan saamistaan mainosten tuotoista käyttäjilleen. (Malgieri & Custers 2018, 292–293.)

Hyödyt eivät ole kaikissa tapauksissa taloudellisia. Henkilökohtaisia tietoja luovuttamalla voidaan esimerkiksi lisätä toiminnallisuutta, käyttömukavuutta ja sujuvuutta. (Pötzsch 2009, 230–231.) Esimerkiksi verkkokaupan käyttö voi olla kätevämpää kuin fyysisessä liikkeessä asioiminen tai tallentamalla verkkokauppaan omat yhteystiedot ja luottokorttinumero säästetään vaivaa tulevaisuuden ostokerroilla ja ostoprosessista tulee automatisoidumpi käyttäjän näkökulmasta. Personoidut tuotteet ja palvelut ovat yleinen kuluttajien tavoittelema hyöty. Lukuisat yksilöt myös kokevat kohdennetun tai personoidun mainonnan, sisällön ja informaation esimerkiksi uutiskirjeissä tai verkon sisältöehdotuksissa mielekkääksi ja arvokkaaksi. Usein tietojen luovuttaminen säästää yksilöltä

aikaa ja vaivaa, esimerkiksi verkkokaupasta tilaaminen voi säästää yksilöltä käynnin fyysisessä myymälässä. Tietojen luovuttaminen voi olla myös reunaehtona palvelun käytölle eli kannustimena ja hyötynä toimii oikeus palvelun käyttöön. Esimerkiksi useat sosiaalisen median sivustot voivat olla kokonaan suljettuja käyttäjältä ilman henkilökohtaisten tietojen avulla luotua profiilia. Sosiaalisessa mediassa tai muissa verkkoyhteisöissä yleisiä yksilöille realisoituvia hyötyjä ovat muun muassa sosiaalisen pääoman luominen, ihmissuhteiden solmiminen ja ylläpitäminen. Sosiaalisen median alustoja voidaan hyödyntää myös esimerkiksi yksilön oman maineen parantamiseen tai niin sanotun henkilöbrändin rakentamiseen. Erityisesti nuorten ihmisten keskuudessa on yleistä ajatella yksityisyyden suojan menettämisen olevan pakollista sosiaalisen yhteenkuuluvuuden varmistamiseksi. (Adorjan & Ricciardelli 2019, 10; Marwick & Hargittai 2019, 1697–1702.)

2.10.2 Tietojenluovutuksen kustannukset

Privacy calculus teorian mukaisesti hyödyillä on aina myös oma vastapuolensa, niin sanotut tiedonjaosta aiheutuvat kustannukset, jotka yleisemmin ajatellaan riskeinä, huolina tai haittoina. Voidaan puhua niin sanotuista psykologisista kustannuksista (Lee ym. 2006, 293). Taloudellisena haittana voi realisoitua esimerkiksi organisaation suorittama hintasyrjintä. Organisaatio voi muun muassa yksilön tulotason tai elämäntilanteen tuntemalla suorittaa vaihtelevaa hinnoittelua eri käyttäjien kohdalla. (Malgieri & Custers 2018, 296–299.) Tiedonjaon kustannukset ovat useammin kuitenkin aineettomia ja abstrakteja. Esimerkiksi tietoja luovuttamalla identiteettivarkauden todennäköisyys kasvaa, yksilö altistuu helpommin roskapostille, liialliselle mainonnalle ja vakoilulle. (Pötzsch 2009, 230.) Tietojen luovuttamisesta voi aiheutua yksilölle mielipahaa, esimerkiksi syrjinnän pelon tai skeptisyyden muodossa (Marwick & Hargittai 2019, 1697–1702). Yksityisyyteen liittyviä kustannuksia ovat myös arkaluontoisten tietojen helpompi löydettävyys ulkopuolisille, tietojen kopiointi ja heikko kontrolli tietojen leviämisestä suurelle joukolle tuntemattomille ihmisiä (Adorian & Ricciardelli 2019, 9–10). Myös esimerkiksi aikaisemmin tämän tutkielman luvussa 2.3 esitellyt yksityisyyshuolet luetaan useissa tutkimuksissa osaksi privacy calculus -teoriaa (ks. esim. Dinev & Hart 2006; Keith ym. 2013; Wang ym. 2020).

Vaihtoehtoisesti yksityisyyden suojan heikkenemisestä aiheutuvat haitat (kustannukset) voidaan karkeasti jakaa kahteen luokkaan: subjektiivisiin ja objektiivisiin haittoihin. Subjektiivisia haittoja ovat yksilöstä itsestään lähtöisin olevat tuntemukset, kuten muun

muassa ahdistuksen tai epämukavuuden tunteet. Objektiivisia haittoja ovat taas näkökulmasta riippumatta havaittavissa olevat negatiiviset seuraukset, kuten epäsymmetrinen informaatio, identiteettivarkaus ja tietojen avulla toteutettava syrjintä esimerkiksi heikompien sopimusehtojen tai kalliimman hinnoittelun muodossa. (Malgieri & Custers 2018, 294.) Epäsymmetrisellä informaatiolla tarkoitetaan tilannetta, jossa transaktion toisella osapuolella on halussaan enemmän tietoa vastapuolesta (Maylanova ym. 2012, 240–241).

3 YKSITYISYYDEN PARADOKSIIN VAIKUTTAVAT TEKIJÄT

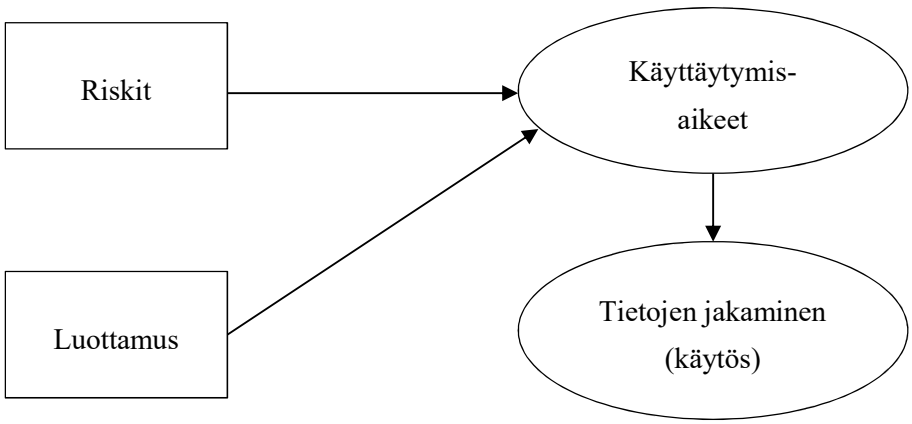
Seuraavaksi tutkielmassa tarkastellaan tieteellisten artikkelien, tutkimuksien ja kirjallisuuden esittelemiä malleja, viitekehyksiä, tutkimuksia ja teorioita yksityisyyden paradoksin selittämiseksi sekä yksityisyyteen liittyvien aikeiden ja käytöksen taustalla olevien vaikuttavien tekijöiden tarkastelemiseksi. Tässä pääluvussa keskitytään mallien ja teorioiden esittelyyn sekä niiden erojen ja yhtäläisyyksien vertailuun. Luvussa edetään pääsääntöisesti enemmän tunnetuimmista malleista ja tekijöistä yksityiskohtaisemmille sekä vähemmän tutkituille tasoille.

Artikkelit ja muu kirjallinen materiaali hankittiin verkon sähköisistä tietokannoista. Tietokantoina ja lähteiden etsimiseen käytettyjä sivuja varsinaista viitekehystä varten olivat ensisijaisesti Scopus, ScienceDirect, Emerald ja SpringerLink. Hyödynnetyt lähteet ovat vuosien 2006 ja 2020 välillä tai aikana julkaistuja artikkeleja tai teoksia, sillä yksityisyyden paradoksi tunnistettiin ilmiönä ja ongelmana vasta vuonna 2006. Etsittyjen artikkelien sopivuuden arvioinnissa tutkielman tekijä aloitti tutustumalla huolellisesti artikkelin tai teoksen otsikkoon, tiivistelmään, avainsanoihin ja johtopäätöksiin. Usein arviointi vaati myös syvällisempää artikkeliin tutustumista tai koko artikkelin lukemista. Varsinaiseen viitekehyksen kehittämiseen hyödynnettävien artikkelien valitsemiselle oli kriteerinä keskittyminen yksityisyyden paradoksiin tai yksityisyyteen liittyvään käyttäytymiseen tai aikeisiin. Koska yksityisyys on monimutkainen ilmiö ja paradoksi on syntynyt nimenomaan yksityisyyteen liittyen, pelkästään yleisesti käyttäytymiseen tai aikeisiin keskittyvät tutkimukset eivät välttämättä päde yksityisyyteen liittyvässä päätöksenteossa. Tämän takia artikkelien valinta tehtiin tiukasti tutkimuksiin ja teoksiin, joissa yksityisyys, tietojen jakaminen tai yksityisyyden paradoksi oli tarkastelussa keskeisessä näkökulmassa. Jokaisen viitekehykseen valittavan artikkelin tai teoksen kielenä oli englanti ja jokainen tätä tutkielmaa varten valittu valmis malli, teoria tai viitekehys oli joko testattu toimivuudeltaan tai havaittu empirian avulla.

3.1 Riski-luottamusmalli

Norbergin ym. vuonna 2007 julkaistu tutkimus yksityisyyden paradoksista toi lisää fokusta yksityisyyden paradoksiin ilmiönä Barnesin (2006) alkuperäisen paradoksin käsitteen lanseeraavan artikkelin jälkeen. Norbergin ym. (2007) artikkelissa kuvailtu tutkimus oli yksi ensimmäisistä yrityksistä etsiä ratkaisua ja selityksiä yksityisyyden paradoksin

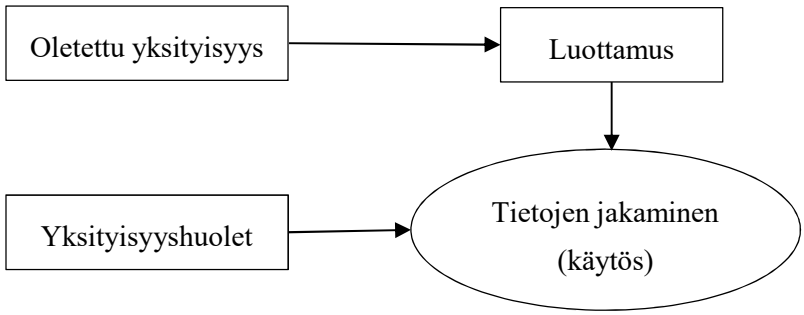
taustalla vaikuttavista tekijöistä. Heidän tutkimuksensa lopputuloksena esiteltiin yksityisyyden paradoksin yksi varhaisimmista ja tunnetuimmista malleista riskin ja luottamuksen vaikutuksista paradoksiin. Tämän mallin mukaan yksilön kokemat riskit ja luottamus organisaatiota kohtaan vaikuttavat tietojen jakoon liittyviin aikeisiin ja aikeet edelleen käytökseen. Myös luottamuksen vaikutusta käytökseen testattiin, mutta yhteyttä ei havaittu. Luottamuksella tarkoitetaan yksilön muodostamaa ja kokemaa arviota organisaation luotettavuudesta. Luottamus organisaatioon on yksi merkittävimmistä edellytyksistä yksilön tietojen luovutukseen. Tutkimuksen lopputulokset tukivat lisäksi hypoteesia aikeiden ja käytöksen välisestä kuilusta ja siten vahvistivat Barnesin (2006) tunnistaman yksityisyyden paradoksin. Riskin ja luottamuksen vaikutus käyttäytymisaikeisiin ja aikeiden vaikutus lopulliseen käytökseen ovat muodostuneet eräänlaisiksi kulmakiviksi yksityisyyden paradoksiin liittyvässä tutkimuksessa. Mitä enemmän riskejä yksilö koki tietojen luovutuksella olevan, sitä vähemmän tietoja aiottiin luovuttaa. Luottamus taas lisäsi käyttäytymisaikeita tietojen luovutusta kohtaan. Norbergin ym. (2007) esittelemät paradoksiin vaikuttavat tekijät on esitelty kuviossa 7. (Norberg ym. 2007, 100–108, 113, 115–120.)



Kuvio 7. Riski-luottamusmalli (Norberg ym. 2007)

Siinä missä Norbergin ym. (2007) mallissa luottamuksen ei havaittu vaikuttavan käytökseen, Joinsonin ym. (2006) tutkimuksessa puolestaan havaittiin yhteys luottamuksen ja käyttäytymisen välillä ja tarkasteluun otettiin myös yksityisyyshuolten vaikutus käytökseen: luottamus lisää yksilön tietojen jakamiseen liittyvää käyttäytymistä, kun taas yksityisyyshuolet vähentävät tietojen luovutusta. Joinson ym. (2006) havaitsivat myös, että

oletettu yksityisyyden suojan korkea taso kohensi yksilöiden kokemaa luottamusta. Kuvio 8 havainnollistaa Joinsonin ym. (2006) tutkimuksen lopputuloksena syntyneen mallin.



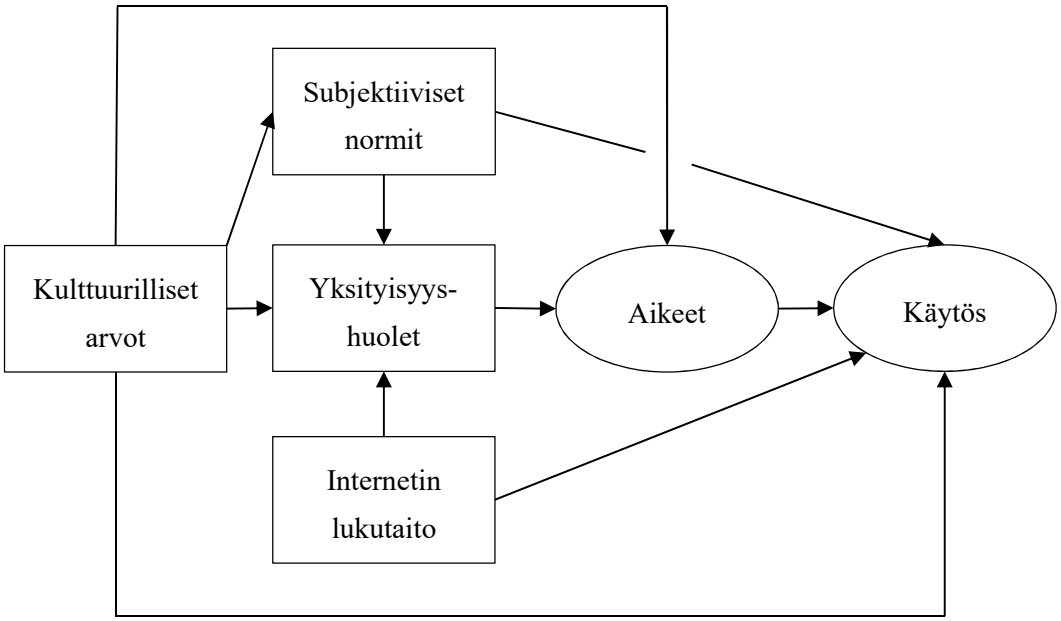
Kuvio 8. Luottamuksen ja yksityisyyshuolten vaikutus yksilön käytökseen (Joinson ym. 2006)

3.2 Suunnitellun käyttäytymisen teoriaan perustuvat mallit

Joinsonin ym. (2006) ja Norbergin ym. (2007) mallit olivat suhteellisen yksinkertaisia ja keskittyivät pääasiallisesti luottamuksen vaikutusten tarkasteluun yksityisyyden paradoksiin liittyviin aikeisiin ja käytökseen. Aikaisemmin tässä tutkielmassa luvussa 2.4 esitelty suunnitellun käyttäytymisen teoria on ollut ensisijaisesti käyttäytymisen ennustamiseen tarkoitettu lähestymistapa, mutta teoriaa on hyödynnetty runsaasti yksityisyyden paradoksia koskevassa tutkimuksessa.

Dincelli ja Goel (2017) hyödynsivät tutkimuksessaan pohjana suunnitellun käyttäytymisen teoriaa, mutta asenteet korvattiin yksityisyyshuolilla, oletetun käytöksen kontrollin sijasta tarkasteltiin internetiin liittyvää lukutaitoa ja tarkasteluun otettiin mukaan kulttuurilliset arvot. Esimerkkejä kulttuurillisista arvoista ovat individualismin tai kollektivismin väliset painotukset sekä vapauden ja kontrollin arvostus. Dincellin ja Goelin (2017) artikkelissa korostetaan sitä, kuinka yksityisyyteen liittyvä käyttäytyminen saa usein vaikutteita ympäristöstä ja ulkopuolisilta ihmisiltä. Sosiaalisiin odotuksiin vastaaminen ja itsestään mahdollisimman houkuttelevan vaikutelman rakentaminen verkossa ulkopuolisten silmistä ovat yleistä muun muassa sosiaalisessa mediassa. Yksilö voi kokea merkittävää ryhmäpainetta jakaa omia tietojaan verkossa esimerkiksi yhteenkuuluvuuden tunteen kasvattamiseksi. Kulttuurillisten arvojen ehdotetaan myös vaikuttavan siihen, miten ihmiset tasapainottavat ulkopuolisista ja itsestään lähtöisiä olevia tekijöitä sekä arvoja

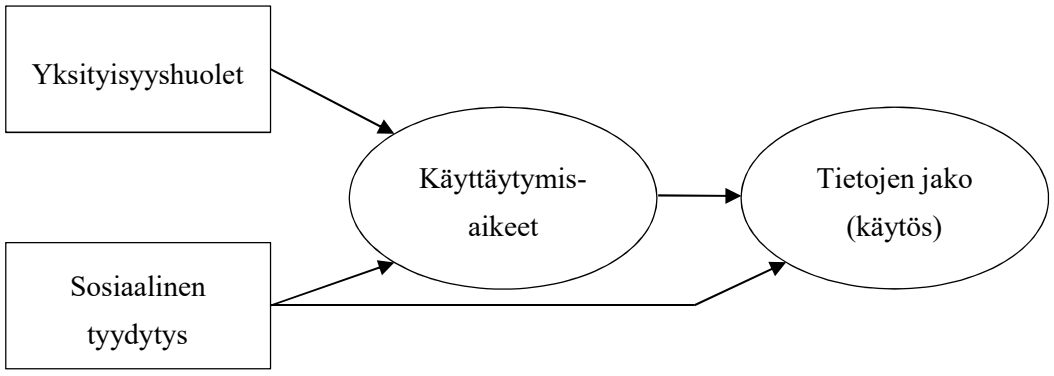
käytöksessään. Dincellin ja Goelin (2017) suunnitellun käyttäytymisen teoriaan perustuva malli esitetään kuviossa 9. (Dincelli & Goel 2017, 4012–4015.)



Kuvio 9. Dincellin ja Goelin (2017) sovellus suunnitellun käyttäytymisen teoriasta

Internetiin liittyvällä lukutaidolla (engl. Internet literacy) tarkoitetaan yksilön kykyjä käyttää internetin sovelluksia kommunikointiin työ- ja viihdetarkoituksissa sekä mahdollisuuksia välttää ja hallita haitallista sisältöä, esimerkiksi tietojen varastamista tai roskaposteja. Usein internetiin liittyvään lukutaitoon yhdistetään myös muita yksilön kykyjä, esimerkiksi kykyä ymmärtää organisaatioiden datankeruuta tai yksityisyyden suojan ylläpitämiseen vaadittavia taitoja. Mahdollisten yksityisyyden suojan rikkomusten tai muiden negatiivisten seurausten hahmottamisen voidaan ajatella myös olevan olennainen osa internetiin liittyvää lukutaitoa. Internetin lukutaidon havaittiin lisäävän yksityisyyttä suojaavaa käytöstä, mutta vaikutuksia aikeisiin ei havaittu. Internetiin liittyvään lukutaitoon liittyviä tutkimuksia esitellään lisää tämän tutkielman luvussa 3.5. Subjektiiviset normit eivät vaikuta suunnitellun käyttäytymisen teorian mukaisesti suoraan aikeisiin. Toisin kuin alkuperäisessä suunnitellun käyttäytymisen teoriassa, Dincellin ja Goelin (2017) havaintojen mukaan subjektiiviset normit vaikuttavat käyttäytymiseen. (Dincelli & Goel 2017, 4015–4018.)

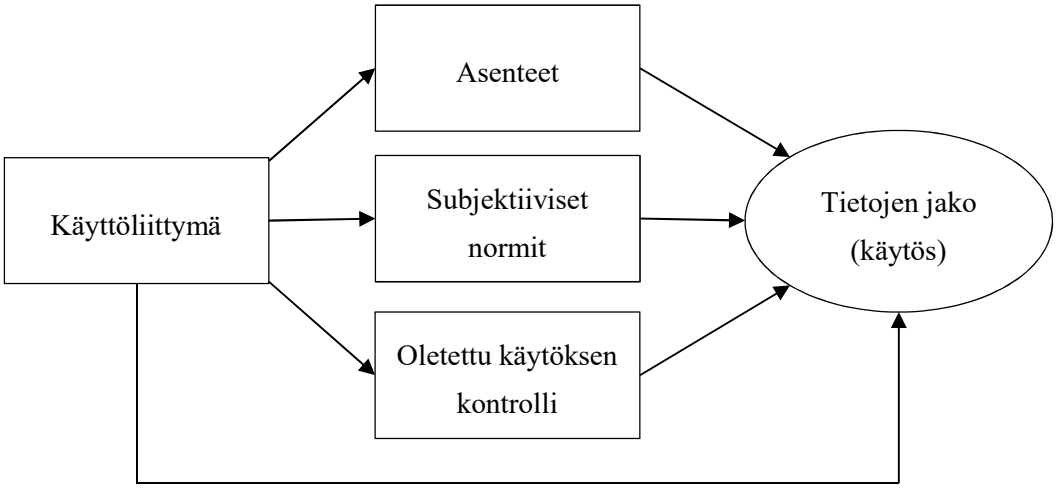
Toisin kuin Dincellin ja Goelin (2017) tutkimuksessa, Hallam ja Zanella (2017) tarkastelivat yksityisyyshuolten vaikutuksia myös käytökseen. Hallam ja Zanella (2017) tutkivat artikkelinsa mallissa yksityisyyshuolten ja sosiaalisen tyydytyksen vaikutuksia aikeisiin ja käytökseen. Sosiaalisella tyydytyksellä tarkoitetaan yksilön kokemaa hyötyä ja tyytyväisyyttä sosiaalisista suhteista ja kanssakäymisestä, joita voidaan mahdollistaa esimerkiksi jakamalla tietoja verkossa. Hallamin ja Zanellan (2017) tutkimuksessa sovellettiin suunniteltua käyttäytymistä CLT-teorian (engl. Construal level theory) avulla. CLT-teorian ajatuksena on se, että mitä konkreettisemmin jotakin asiaa ajatellaan tai tarkastellaan, sitä enemmän yksilö arvostaa tai painottaa asiaa lyhyemmällä aikavälillä ja vastapainoisesti mitä abstraktimmin asiaa lähestytään, sitä enemmän asia nähdään kaukaisemmaksi ja pidemmällä aikavälillä painotettavaksi. Toisin sanoen aikeet jaettiin lyhyen ja pitkän aikavälin aikeisiin. (Hallam & Zanella 2017, 217–224.) Kuviossa 10 havainnollistetaan Hallamin ja Zanellan (2017) tutkimuksen tulokset, kuitenkin lyhyen ja pitkän aikavälin aikeiden erottelun sijaan tuloksia käsitellään tätä tutkielmaa varten kehitettävää viitekehystä silmällä pitäen aikeina, joka huomioi sekä pitkän että lyhyen aikavälin aikomukset samassa käsitteessä.



Kuvio 10. Hallamin ja Zanellan (2017) CLT-teoriaa soveltava malli

Hallamin ja Zanellan (2017) mukaan sosiaalinen tyydytys ja yksityisyyshuolet molemmat vaikuttivat aikeisiin, kun taas aikeet ja sosiaalinen tyydytys vaikuttavat käyttäytymiseen. Yksityisyyshuolilla ei havaittu olevan merkittävää vaikutusta tietojen jakamiseen liittyvään käyttäytymiseen. (Hallam & Zanella 2017, 217–224.) Luvun 3.1 Joinsonin ym. (2006) mallin mukaan yksityisyyshuolet puolestaan vaikuttivat käyttäytymiseen.

Hughes-Roberts ja Kani-Zahibi (2014) tutkivat artikkelissaan yksityisyyden paradoksia käyttöliittymän näkökulmasta suunnitellun käyttäytymisen teorian avulla (kuvio 11). Käyttöliittymä (engl. User Interface, UI) on verkkoon liittyvä ympäristötekijä, jonka avulla navigoidaan ja käytetään verkossa olevaa internetsivua. Käyttöliittymän suunnittelulla voidaan ohjata käyttäjää tekemään helpommin tietynlaisia valintoja, esimerkiksi sosiaalisen median sivusto voidaan suunnitella kannustamaan avoimuuteen ja siten kannustavaksi omien henkilökohtaisten tietojen jakamiseen. (Hughes-Roberts & Kani-Zahibi 2014, 221.) Tämä on esimerkki aikaisemmin tutkimuksessa luvussa 2.2.3 mainitusta eräästä kognitiivisesta vinoumasta, kehystysvaikutuksesta.

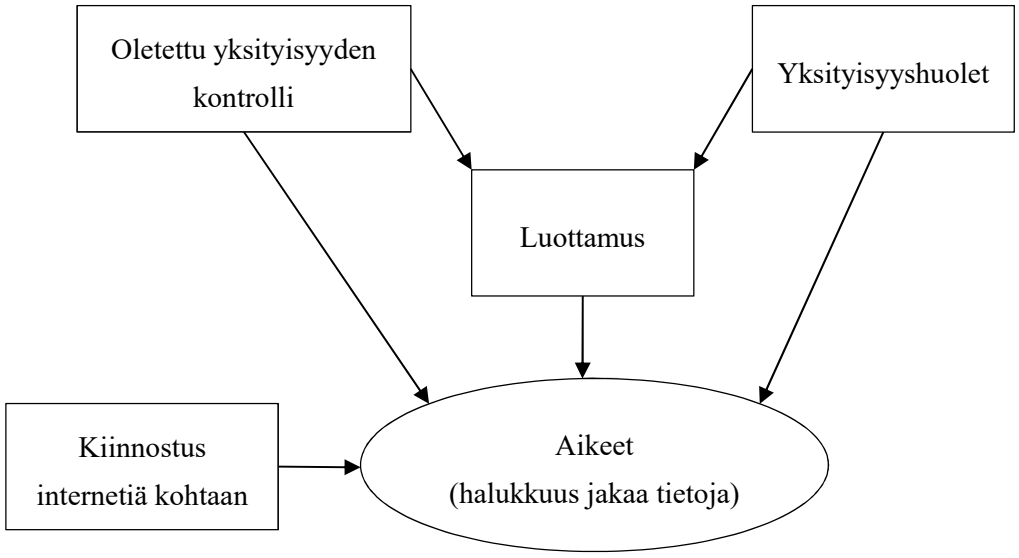


Kuvio 11. Käyttöliittymän vaikutukset yksilön käyttäytymiseen (Hughes-Roberts & Kani-Zahibi 2014)

Hughes-Robertsin ja Kani-Zahibin (2014) malli muistuttaa enemmän perinteistä suunnitellun käyttäytymisen teoriaa kuin aikaisemmat Dincellin ja Goelin (2017) ja Hallamin ja Zanellan (2017) tutkimukset, sillä asenteet, subjektiiviset normit ja oletettu käytöksen kontrolli ovat yhteneviä osia alkuperäisen suunnitellun käyttäytymisen teorian kanssa. Hughes-Roberts ja Kani-Zahibi (2014) jättivät kuitenkin yksilön aikeet pois tarkastelusta toisin kuin Dincelli ja Goel (2017) sekä Hallam ja Zanella (2017). Dincellin ja Goelin (2017) mallin kulttuurillisten arvojen sijaan tarkasteltiin käyttöliittymän vaikutusta käytökseen ja muihin suunnitellun käyttäytymisen teorian tekijöihin. Kun käyttöliittymässä annetaan käyttäjälle ohjeita, suosituksia ja informaatiota muiden käyttäjien toiminnasta sekä oman tiedonjaon vaikutuksista, havaittiin selkeitä muutoksia yksilöiden tietojen ja-

kamisessa (käytöksessä). Esimerkiksi tietojen syöttämiseen tarkoitettavat kentät värikoodaamalla voidaan antaa käyttäjälle suosituksia ja tietoja mahdollisista vaikutuksista (esimerkiksi vihreä värikoodi tarkoittaa neutraaleja tietoja ja pientä vaaraa, kun taas keltainen värikoodi tarkoittaa arkaluontoisempia tietoja ja korkeampaa riskiä yksityisyyden suojan heikkenemiseen). Värikoodaus on esimerkki käyttäjän asenteisiin vaikuttamisesta. Subjektiivisia normeja voidaan taas kontrolloida antamalla yleisiä suosituksia tai tarkempia tietoa muiden käyttäjien yleisimmistä valinnoista. Oletettuun käytöksen kontrolliin liittyen voidaan esimerkiksi antaa numeroasteikolla oleva arvo yksityisyyden suojan tasosta tai riskeistä. Mitä selkeämmin käyttäjälle annetaan tietoa riskeistä ja yksityisyyden suojan heikkenemisestä, sitä vähemmän tietoja luovutettiin eikä käyttäytyminen siten ollut yhtä ristiriitaista. Toisin sanoen, suunnitellun käyttäytymisen teorian mukaiset asenteet, subjektiiviset normit ja oletettu käytöksen kontrollin vaikuttivat käytökseen, verkkosivuun liittyvien käyttöliittymäelementtien lisäksi. Internetin käyttäjät tutustuisivat mieluummin tietosuojaselosteisiin ja käyttöehtoihin käyttöliittymän kautta pitkien tekstiformaattien sijasta. Koska useissa tapauksissa ei ole organisaation etujen mukaista rohkaista käyttäjää jättää luovuttamatta tietoja, voitaisiin käyttöliittymään liittyviä käyttäjien yksityisyyden suojaan liittyviä ominaisuuksia implementoida esimerkiksi selaimeen kehitettävien laajennusten avulla yksilön yksityisyyden suojan edistämiseksi ja paradoksiin liittyvän kuilun kaventamiseksi. Myös lainsäädännöllä voitaisiin luoda velvoitteita organisaatioille käyttöliittymään liittyvistä elementeistä tarpeen vaatiessa. (Hughes-Roberts & Kani-Zahibi 2014, 226–230.)

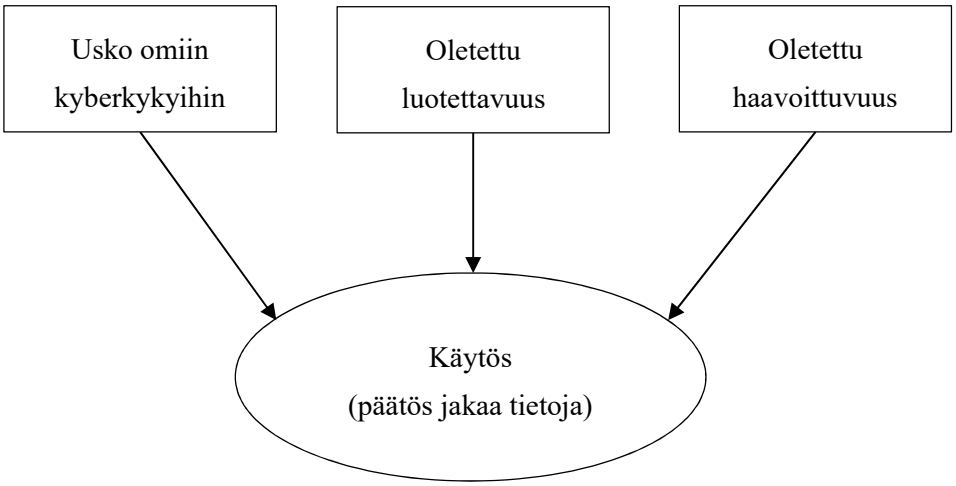
Suunnitellun käyttäytymisen teorian mukaista, Hughes-Robertsin ja Kani-Zahibinkin (2014) soveltamaa, oletettua käytöksen kontrollia on sovellettu Zorotheoksen ja Kafezan (2009) tutkimuksessa oletettuna yksityisyyden kontrollina. Zorotheoksen ja Kafezan (2009) tutkimuksen tulosten mukaan yksityisyyteen liittyviin aikeisiin vaikuttavat yksilön henkilökohtainen kiinnostus internetiä kohtaan, oletettu kontrolli yksityisyydestä verkossa, koetut yksityisyyshuolet ja luottamus verkon organisaatiota kohtaan. Ainoastaan yksityisyyshuolet vähentävät yksilön aikeita luovuttaa tietoja, kun taas mallin muut tekijät lisäävät yksilön halukkuutta jakaa tietoja verkossa. Oletetulla yksityisyyden kontrollilla oli luottamusta kohottava vaikutus, kun taas yksityisyyshuolilla oli luottamusta heikentäviä vaikutuksia. (Zorotheos & Kafeza 2009, 141–149.) Zorotheoksen ja Kafezan (2009) johtopäätökset ovat koottu kuvioon 12.



Kuvio 12. Zorotheoksen ja Kafezan (2009) sovellus suunnitellun käyttäytymisen teoriasta

Kuten luvun 3.1 Norbergin ym. (2007) tutkimuksenkin perusteella, Zorotheoksen ja Kafezan (2009) mukaan luottamus vaikuttaa aikeisiin. Zorotheoksen ja Kafezan (2009) havainnot yksityisyyshuolten vaikutuksista aikeisiin ovat linjassa myös Dincellin ja Goelin (2017) sekä Hallamin ja Zanellan (2017) tulosten kanssa. Tarkasteltaessa Zorotheoksen ja Kafezan (2009) mallia huomataan, että muut suunnitellun käyttäytymisen teoriaan perustuvat tutkimukset eivät tarkastelleet yksilön internetiin liittyvän kiinnostuksen vaikutuksia ollenkaan.

Suunnitellun käyttäytymisen teoriaa hyödynnettiin myös osittain Boothin ja Hon (2019) tekemässä tutkimuksessa (kuvio 13), jonka mukaan aikeisiin vaikuttavat oletettu luotettavuus, oletettu haavoittuvuus ja usko omaan verkkoon liittyvään kyberosaamiseen. Luotettavuudella tarkoitetaan Boothin ja Hon (2019) tutkimuksen kontekstissa yksilön muodostamaa subjektiivista arviota tietoja keräävän organisaation luotettavuudesta. Haavoittuvuudella viitataan yksityisyyden suojan heikentymisen mahdollisuuteen, joka on käytännössä esimerkki yksityisyysriskeistä. Oletettu käytöksen kontrolli määriteltiin tutkimuksen puitteissa yksilön uskoksi omaan verkkoon liittyvään kyberosaamiseen, joka tarkoittaa yksilön uskomusta omiin kykyihinsä tunnistaa onko tietojen luovuttaminen turvallista päätöksentekotilanteessa ja arvioida kuinka paljon hän itse pystyy vaikuttamaan tietojen käyttöön. (Booth & Ho 2019, 167–169, 175.) Kuten luvussa 2.4 huomattiin, oletetun käytöksen kontrollin voidaan ajatella muodostuvan uskosta tai luottamuksesta omiin kykyihin ja oletetusta kontrolloitavuudesta käytökseen ja lopputulemaan liittyen.



Kuvio 13. Boothin ja Hon (2019) malli käytökseen vaikuttavista tekijöistä

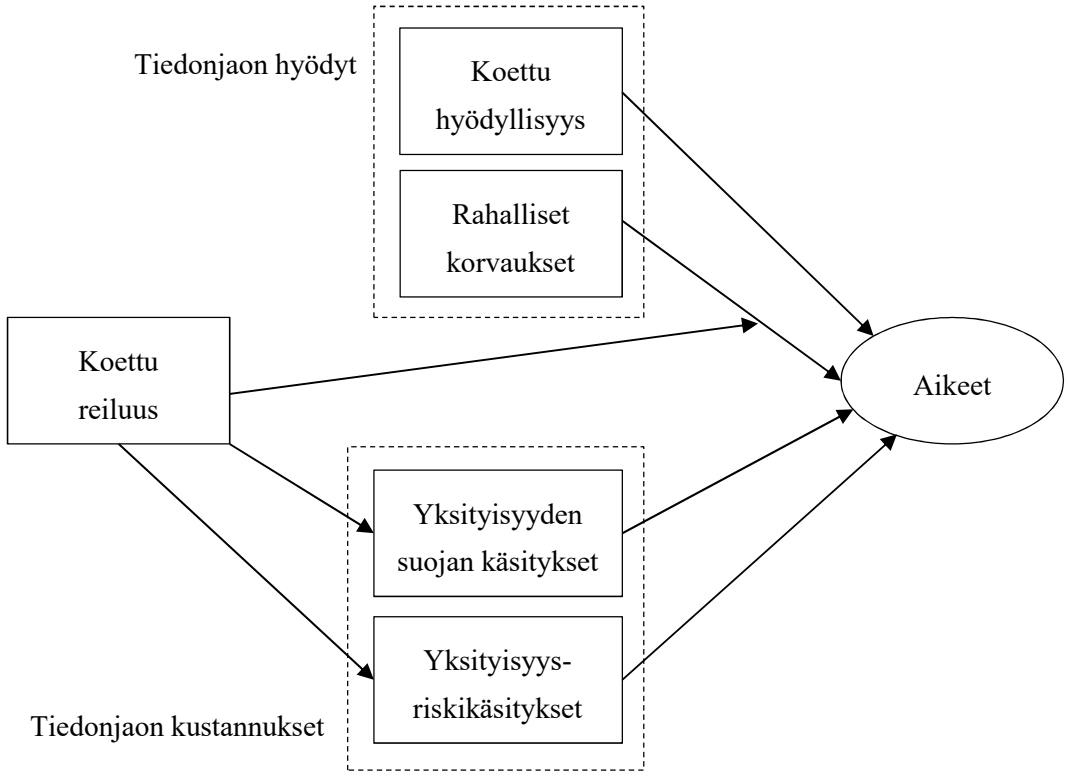
Boothin ja Hon (2019) mallissa oletetun luotettavuuden vaikutus käytökseen vastaa Joinsonin ym. (2006) tuloksia ja kyberkykyihin liittyvät uskomukset puolestaan vastaavat Hughes-Robertsin ja Kani-Zahibin (2014) löydöksiä oletetun käytöksen kontrollin vaikutuksista.

3.3 Privacy calculus -teoriaan perustuvat mallit

Tieteellisessä kirjallisuudessa paljon hyödynnetyn suunnitellun käyttäytymisen teorian lisäksi erityisesti privacy calculus -teoriaa on käytetty pohjana usein yksityisyyden paradoksiin liittyvässä tutkimuksessa. Privacy calculus -teoriaan liittyvissä malleissa korostuvat yleisesti vähintäänkin yksilön kokemat tiedonjaosta aiheutuvat oletetut hyödyt ja haitat. Privacy calculus -teoria esiteltiin aikaisemmin tämän tutkielman luvussa 2.10.

Lin ym. (2010) tutkimuksen mukaan yksilön yksityisyyteen liittyviin aikeisiin vaikuttavat tiedonjaolla saavutettavat hyödyt (rahalliset hyödyt ja koettu hyödyllisyys) sekä tiedonjaon kustannukset (yksityisyyden suojaan liittyvät käsitykset ja yksityisyysriskikäsitykset). Koska yksilöt luovuttavat tietonsa koettujen hyötyjen ylittäessä koetut kustannukset, tulokset tukevat privacy calculus -teoriaa. Yksityisyysriskeihin liittyvät käsitykset tarkoittavat yksilön odotuksia yksityisyyden suojan heikkenemisestä ja yksityisyyden suojaan liittyvät uskomukset puolestaan tarkoittavat omakohtaista näkemystä henkilökohtaisten tietojen tietosuojasta ja riskitasosta, kun tiedot on luovutettu organisaatiolle. (Li ym. 2010, 62, 65–68.)

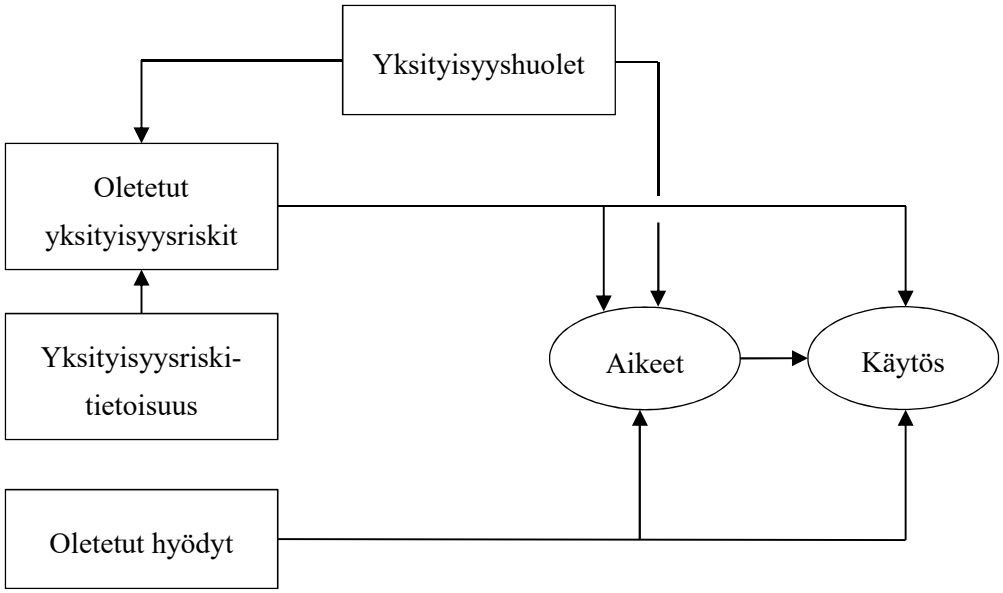
Kirjallisen ja lainmukaisen sopimuksen lisäksi tiedonvaihtoon liittyy usein niin sanottu epäsuora sosiaalinen sopimus, joka perustuu sopimuksen osapuolten yhteisiin ja yleisiin normeihin kummankin osapuolen velvollisuuksista ja oikeuksista. Sosiaalisten sopimusten teorian (engl. Social Contract Theory, SCT) mukaan yksilöiden päätöksentekoon liittyy rajoittunutta moraalista rationaalisuutta. Verkkopalveluiden käyttäjillä ei ole yleisesti tarpeeksi informaatiota tehdä täysin paikkansapitäviä arvioita organisaatiosta tai sivustosta ja seuraukset voivat tästä syystä olla yksilöille tuntemattomia. Sosiaalisen sopimuksen pohjalta yksilöt tarkastelevat tietojenluovutusta reiluuden näkökulmasta. Yleisesti tiedonjaon reiluus voidaan määritellä näkemykseksi siitä, että yksilöltä pyydettävät tiedot ovat liiketoimen kannalta relevantteja ja tarpeellisia organisaatiolle. Tietojen jakamiseen liittyvä reiluus voidaan esimerkiksi yhdistää organisaation reiluun tietokäytäntöön (engl. Fair Information Practice Principles, FIPP). Reiluutta arvioidaan muun muassa sen vuoksi, että yksityisyydellä ei ole tarkkaa hintaa tai taloudellista arvoa. Koettu reiluus, eli tietojen koettu relevanssi transaktiossa, vaikuttaa tiedonjaon koettuihin kustannuksiin: kun yksilöt kokevat pyydettävien tietojen olevan relevantteja, riskikäsitykset lieventyvät ja usko yksityisyyden suojaan kasvaa. Reiluuden havaittiin myös säätelevän rahallisen korvauksen ja yksityisyyteen liittyvien käyttäytymisaikeiden välistä suhdetta. Esimerkiksi tapauksissa, joissa yksilöt kokivat kysyttävien tietojen olevan epärelevantteja, rahallisen korvauksen tarjoaminen heikensi yksilöiden aikeita luovuttaa tietoja. Yksilön ja organisaation välinen sosiaalinen sopimus, ja siihen kuuluva vaikutelma reiluudesta, on siis tärkeässä osassa henkilökohtaisten tietojen jakamisessa eikä rahallinen korvauksen tarjoaminen välttämättä aina tuota odotettua tulosta tietojen pyytämiseen liittyen. Rahallisilla korvauksilla houkutteleminen epärelevanttien tietojen saamiseen voidaan ajatella eräänlaisena sosiaalisen sopimuksen rikkomuksena yksilön näkökulmasta. Organisaatioiden näkökulmasta tämän seikan huomioiminen voi olla hyvinkin keskeistä asiakassuhteiden solmimisessa ja ylläpitämisessä. Reiluus ei vaikuttanut kuitenkaan suoraan yksilön aikeisiin. (Li ym. 2010, 62, 64–68.) Lin. ym. (2010) tutkimuksen tulokset esitellään kuviossa 14.



Kuvio 14. Lin ym. (2010) sovellus privacy calculus -teoriasta

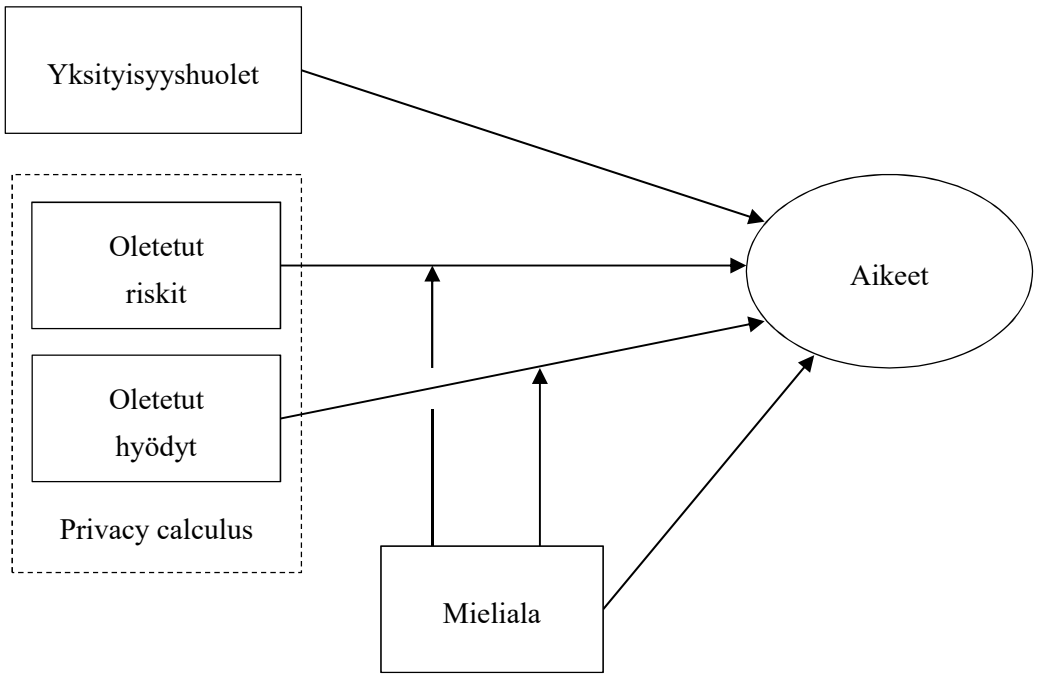
Lin ym. (2010) havainnot tiedonjakoon liittyvien kustannusten, eli yksityisyysriskeihin ja yksityisyyshuoliin liittyvät seikat, vastaavat läheisesti muun muassa luvun 3.1 Norbergin ym. (2007) tuloksia yksityisyyteen liittyvien riskien vaikutuksista yksilön aikeisiin. Lin ym. (2010) mallissa koettuun hyödyllisyyteen nähdään kuuluvaksi kaikki ei rahallinen lisäarvo, kuten esimerkiksi tuotteen tai palvelun tuoma tyytyväisyys. Esimerkiksi luvussa 3.2 Hallamin ja Zanellan (2017) tutkimuksessa todettiin sosiaalisen tyydytyksen, eli sosiaalisen kanssakäymiseen liittyvän tyytyväisyyden, vaikuttavan aikeisiin.

Toisin kuin Li ym. (2010), Keith ym. (2013) tarkastelivat privacy calculus -teoriaan liittyvien hyötyjen, huolten ja riskien vaikutusta aikeiden lisäksi myös käytökseen. Oletetut yksityisyysriskit vähensivät käyttäjien tietojenluovutukseen liittyviä aikeita ja käytöstä, kun taas oletetut hyödyt lisäsivät sekä aikeita että käytöstä. Yksityisyyshuolet vaikuttivat oletettuja riskejä lisäävästi ja aikeita vähentävästi. Yksityisyyshuolilla ei havaittu merkittäviä vaikutuksia käytökseen. Yksityisyysriskeihin liittyvä tietoisuus lisäsi oletettuja yksityisyysriskejä. Yksityisyysriskitietoisuuden vaikutuksia aikeisiin tai käytökseen ei tutkittu tai testattu. Keithin ym. (2013) tutkimuksessa esitetyt paradoksiin vaikuttavat tekijät ovat havainnollistettu kuviossa 15.



Kuvio 15. Privacy calculus -teorian yhteys paradoksiin (Keith ym. 2013)

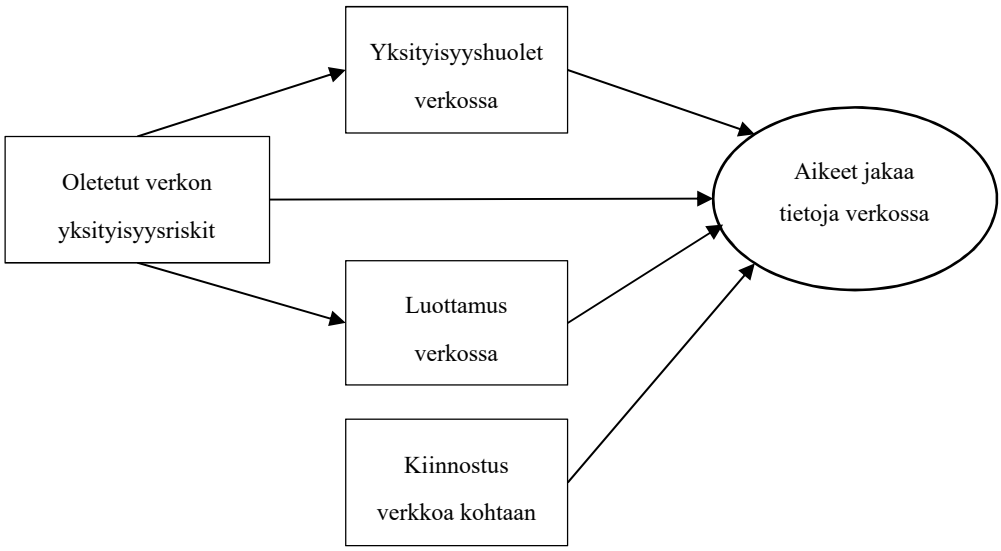
Alashoor ym. (2018) hyödynsivät myös tutkimuksessaan privacy calculus -teoriaan pohjautuvaa mallia (kuvio 16). Heidän mallissaan tutkittiin oletettujen hyötyjen ja riskien sekä yksityisyyshuolten vaikutuksia aikeisiin, kuten esimerkiksi edellä esitelty Keithin ym. (2013) mallikin, mutta tarkasteluun otettiin myös mielialan vaikutus aikeisiin. Alashoorin ym. (2018) mukaan aikeisiin vaikuttivat yksityisyyshuolet, privacy calculus -teorian mukaiset oletetut riskit ja hyödyt sekä mieliala. Alashoor ym. (2018) eivät tarkastelleet yksityisyyshuolia osana kustannus-hyötyanalyysia. Positiivisen mielialan vaikutuksen alaisena yksilö on halukkaampi jakamaan tietojaan, kun taas negatiivisella mielialalla oli aikeita vähentävä vaikutus. Huolet ja riskit vähensivät yksilön tietojen luovuttamiseen liittyviä aikeita, kun taas hyödyt vaikuttivat aikeisiin positiivisesti. Mieliala vaikutti aikeisiin myös välillisesti: kun yksilöllä on positiivinen (negatiivinen) mieliala, oletettujen yksityisyysriskien vaikutus aikeisiin on heikompi (vahvempi) ja positiivinen (negatiivinen) mieliala lisää (vähentää) oletettujen hyötyjen vaikutusta aikeisiin. Mielialalla ja yksityisyyshuolilla ei havaittu olevan yhteisvaikutusta aikeisiin. (Alashoor ym. 2018, 5–11.) Mielialan vaikutusta voidaan ajatella esimerkiksi aikaisemmin mainitun tunteisiin pohjautuvan vinouman näkökulmasta: tunteet ohjaavat yksilöä.



Kuvio 16. Alashoorin ym. (2018) tutkimus privacy calculus -teorian, yksityisyys-huolten ja mielialan vaikutuksista aikeisiin

Dinev ja Hart (2006) tarkastelevat artikkelissaan muunnetun privacy calculus -teoriaan perustuvan mallin (kuvio 17) avulla sitä, miten yksilön luottamus internetissä, yksityisyyshuolet, uskomukset yksityisyysriskeistä ja kiinnostus verkkoa kohtaan vaikuttavat yksilön aikeisiin luovuttaa henkilökohtaisia tietoja verkossa transaktioita varten. Toisin kuin Lin ym. (2010), Keithin ym. (2013) ja Alashoorin ym. (2018) tutkimuksissa, Dinev ja Hart (2006) jättivät hyötyjen vaikutukset tarkastelun ulkopuolelle. Dinevin ja Hartin (2006) mallissa esiintyvät yksityisyysriskit voivat olla yksilöstä riippuen vaihtelevia ja suhteellisen subjektiivisia, mutta yleisesti yksityisyyden suojaan liittyvät riskit viittaavat organisaation mahdollisuuteen käyttäytyä opportunistisesti (kuten esimerkiksi aiemmin tutkielman luvussa 2.8.3 mainitun poaching-ilmiön mukaisesti), käyttäjille aiheutuviin taloudellisiin menetyksiin, henkilökohtaisten tietojen väärinkäyttöön tai varastamiseen. Muita esimerkkejä opportunistisesta käyttäytymisestä ovat esimerkiksi tietojen myyminen tai jakaminen transaktion ulkopuolisille osapuolille. Yksilön olettamat yksityisyysriskit vaikuttavat yksilön aikeisiin, mutta myös koettuihin yksityisyyshuoliin ja luottamukseen. Yksityisyyshuolet ovat Dinevin ja Hartin (2006) mukaan yksilön epävarmoja käsityksiä siitä, ketkä voivat hyödyntää luovutettuja tietoja ja mihin luovutettuja tietoja hyödynnetään. Luottamus taas määritellään lyhyesti yksilön positiivisiksi mielikuviksi

toisesta osapuolesta ja odotuksiksi siitä, ettei toinen osapuoli käyttäydy opportunistisesti. Luottamuksessa on kyse luotettavuuden tunteesta, turvallisuudesta ja organisaation ammattitaidosta. Viimeisenä vaikuttava tekijänä mallissa on käyttäjän kokema kiinnostus verkkoa kohtaan. Yksilön kiinnostus verkkoa kohtaan on yksilöstä itsestään lähtöisin oleva motivaatiotekijä ja sillä tarkoitetaan halukkuutta osallistua verkossa tapahtuvaan toimintaan ja vuorovaikutukseen. (Dinev & Hart 2006, 63–68.)



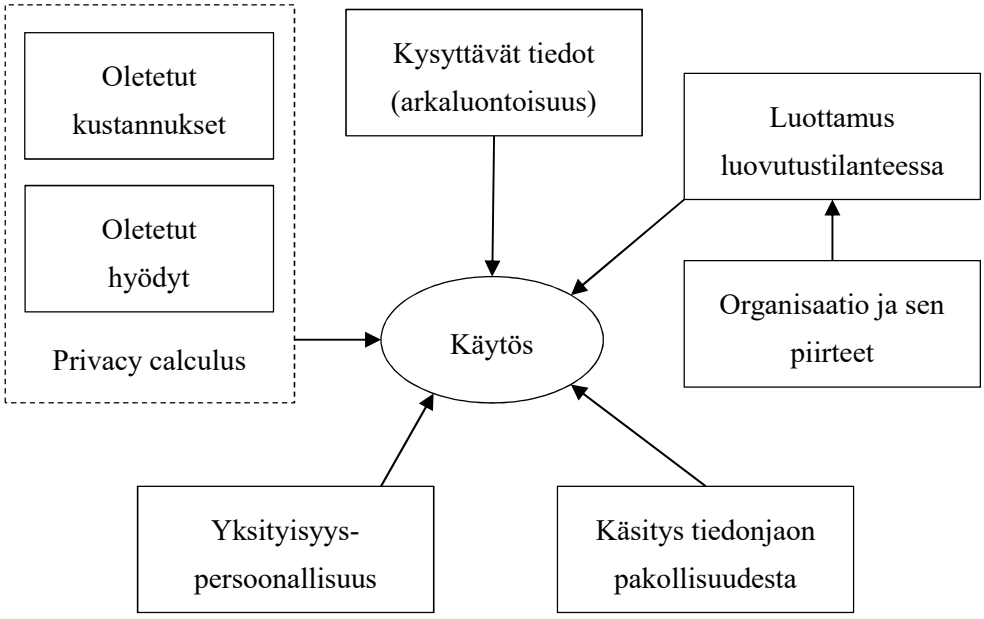
Kuvio 17. Dinevin ja Hartin (2006) mukaiset aikeisiin vaikuttavat tekijät

Dinevin ja Hartin (2006) tulosten mukaan yksilöiden yksityisyyshuolet ja yksityisyysriskit hillitsevät aikeita transaktioihin osallistumista, kun taas yksilön kokema luottamus verkossa ja kiinnostus internetin käyttöä kohtaan puolestaan rohkaisevat tietojen jakamiseen verkossa. (Dinev & Hart 2006, 61–73.) Dinevin ja Hartin (2006) tulokset ovat linjassa yksityisyysriskien ja yksityisyyshuolten osalta edellä käsiteltyjen privacy calculus -teorioihin perustuvien mallien kanssa. Verkkoon liittyvän kiinnostuksen osalta samankaltaisia tuloksia aikeisiin liittyen saivat Zorotheos ja Kafeza (2009) sekä luottamuksen vaikutuksista aikeisiin Norberg ym. (2007) ja Zorotheos ja Kafeza (2009).

Myös Marwickin ja Hargittain (2019) tutkimus vahvistaa privacy calculus -teorian mukaisen ajatuksen yksilöiden suorittamasta kustannus-hyötyarviosta. Siinä missä privacy calculus -teoriaa on usein sovellettu aikeiden tai aikeiden ja käytöksen tutkimukseen, kuten edellä esitellyistä tutkimuksistakin voidaan havaita, ovat Marwick ja Hargittai

(2019) soveltaneet privacy calculus -teoriaa pelkän käyttäytymisen tutkimisessa. Marwickin ja Hargittain (2019) mukaan tiedonjakopäätöksiin (käytökseen) vaikuttavat kysyttävän tiedon tyyppi (arkaluontoisuus), luottamus tietoja keräävään osapuoleen, käsitys tiedonjaon pakollisuudesta ja yksityisyyteen liittyvät persoonallisuuden piirteet privacy calculus -teorian hyötyjen ja psykologisten kustannusten lisäksi. Hyötyjä Marwickin ja Hargittain (2019) mukaan ovat esimerkiksi verkkopalvelun korkea laatu, personointi ja mukavuus, kun taas kustannuksia on esimerkiksi lisääntynyt riski verkossa tapahtuvalle yksityisyyden suojan häirinnälle. Luottamukseen liittyen tutkimuksessa nousi esiin organisaatioon liittyvät piirteet, esimerkiksi organisaation koko tai se onko kyseessä julkinen vai yksityinen toimija. Käyttäjät ajattelivat esimerkiksi yritysten olevan tyypillisesti alttiimpia tietomurroille ja yritysten tarkoitusperien ajatellaan olevan taloudellisten motiivien ajamia. Tutkimuksessa havaittiin yksilöillä persoonallisia piirteitä yksityisyyden suojaan suhtautumisessa, esimerkiksi osa yksilöistä suhtautuu yksityisyyden suojaan luontaisesti välinpitämättömämmin. (Marwick & Hargittai 2019, 1697–1710.) Yksityisyyteen liittyviä persoonallisuuspiirteitä käsitellään tarkemmin luvussa 3.7.1.

Marwicking ja Hargittain (2019) tutkimuksessa nousi esiin paradoksiin liittyvissä tutkimuksissa poikkeuksellisen vähän esillä ollut seikka: yksilöiden käsitys pakollisuudesta. Tietojen luovutus koetaan jopa pakolliseksi tai välttämättömäksi ja tietojen luovuttaminen voi olla siten yksilöiden näkökulmasta ainoa vaihtoehto. Usein tietojen luovuttaminen organisaatiolle toimii eräänlaisena ehtona palvelun käytölle. Myös esimerkiksi opiskeluun tai harrastuksiin liittyviä projekteja voidaan tehdä sosiaalisen median alustoilla tai työpaikkaa verkosta hakiessa tietojen jakaminen on edellytys rekrytoinnissa onnistumiselle. Kun käyttäjät kokevat tietojen luovuttamisen olevan pakollista, päädytään tietoja luovuttamaan herkemmin. Pakollisuuden käsitykseen liittyen artikkelissa ehdotetaankin, että tietoisuutta lisäämällä tai yleisiä käytäntötapoja muuttamalla voitaisiin lieventää pakollisuutta tai vähintäänkin yksilöiden pakollisuuden käsitystä. (Marwick & Hargittai 2019, 1702–1710.) Marwickin ja Hargittain (2019) tutkimuksen tulokset esitellään kuviossa 18.

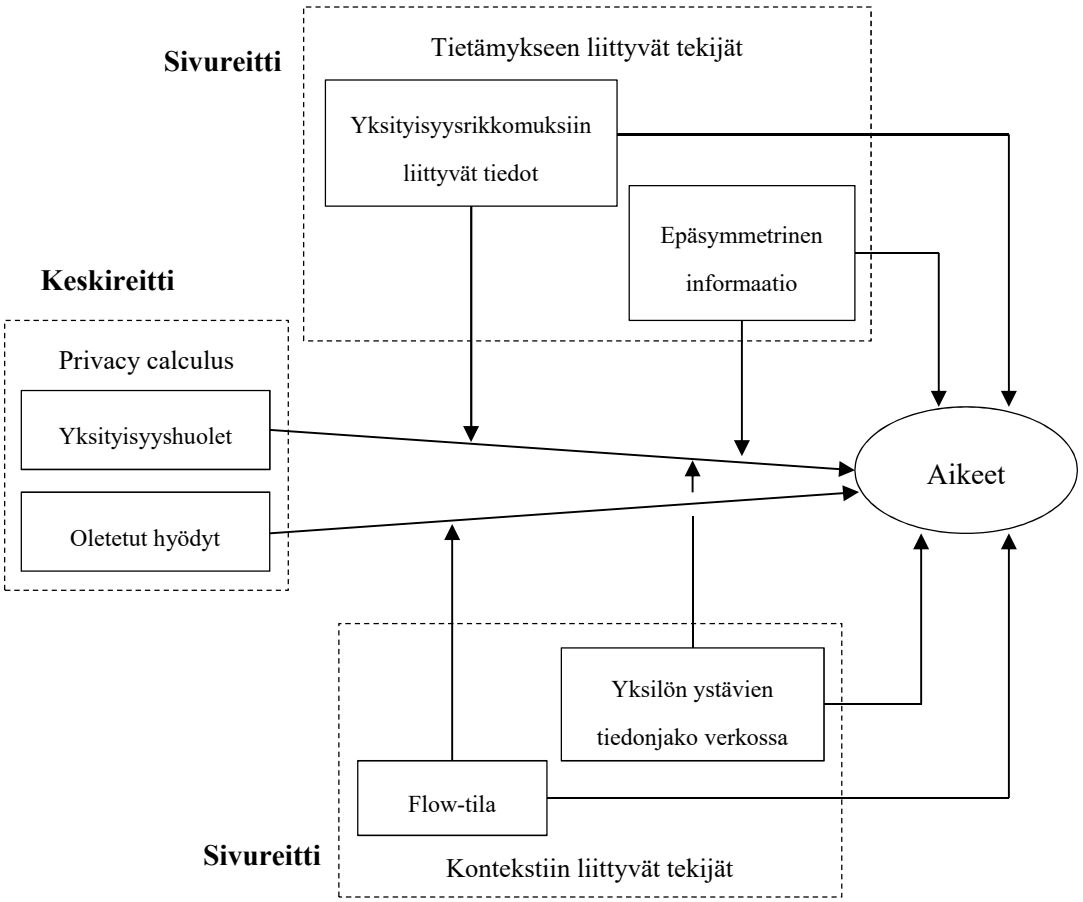


Kuvio 18. Marwickin ja Hargittain (2019) sovellus privacy calculus -teoriasta käytöksen tutkimisessa

Marwickin ja Hargittain (2019) tutkimus nosti esiin useita tekijöitä käytökseen vaikuttavista tekijöistä, joita ei esiintynyt muissa privacy calculus -teoriaan liittyvissä tutkimuksissa, kuten yksityisyyspersoonallisuus, käsitys tiedonjaon pakollisuudesta ja kysyttävien tietojen koettu arkaluontoisuus. Luottamuksen vaikutus käytökseen todettiin aikaisemmin esitellyissä luvun 3.2 Boothin ja Hon (2019) sekä luvun 3.1 Joinsonin ym. (2006) tutkimuksissa.

Wangin ym. (2020) tutkimuksessa tarkasteltiin yksityisyyden paradoksia hyödyntämällä sekä privacy calculus -teoriaa että harkinnan todennäköisyyden teoriaa (engl. elaboration likelihood theory). Privacy calculus -teoria huomioi aikeisiin liittyvän päätöksenteon rationaalisen puolen, kun taas harkinnan todennäköisyyden teoria huomioi irrationaalisemman ja heuristisemman puolen. Wang ym. (2020) luokittelevat yksilön privacy calculus -analyysin muodostuvan oletetuista hyödyistä ja yksityisyyshuolista. Artikkelin mukaan yksilön yksityisyyteen liittyvät aikeet kehittyvät keskireitin ja sivureittien yhdistelmänä. Kun keskireitti on hallitsevampi, muistuttavat yksilön aikeet enemmän privacy calculus -teorian mukaista rationaalista kustannus-hyötyanalyysiä. Jos sivureitit ovat hallitsevampia, perustuu käytös enemmän heuristisiin perusteihin. Sivureittejä on kahdenlaisia. Tietämykseen liittyvä sivureitti perustuu yksityisyysrikkomuksiin liittyviin tietoihin ja yksilön sekä organisaation väliseen oletettuun epäsymmetrisen informaation

määrään. Oletettuun epäsymmetriseen informaation määrän liittyen nostetaan esiin yksityisyyden suojaan ja datan käsittelyyn liittyvät tiedot ja ymmärrys. Kontekstiin liittyvistä tekijöistä muodostuva sivureitti puolestaan muodostuu yksilön ystävien tietojen luovutuksesta ja flow-tilasta, joka tarkoittaa yksilön täydellistä syventymistä tilanteeseen tai aktiviteettiin. (Wang ym. 2020, 353–361, 366–369.) Keski- ja sivureittien vaikutukset ovat esitetty kuviossa 19.



Kuvio 19. Privacy calculus -teorian tarkastelu keski- ja sivureittejä hyödyntämällä (Wang ym. 2020)

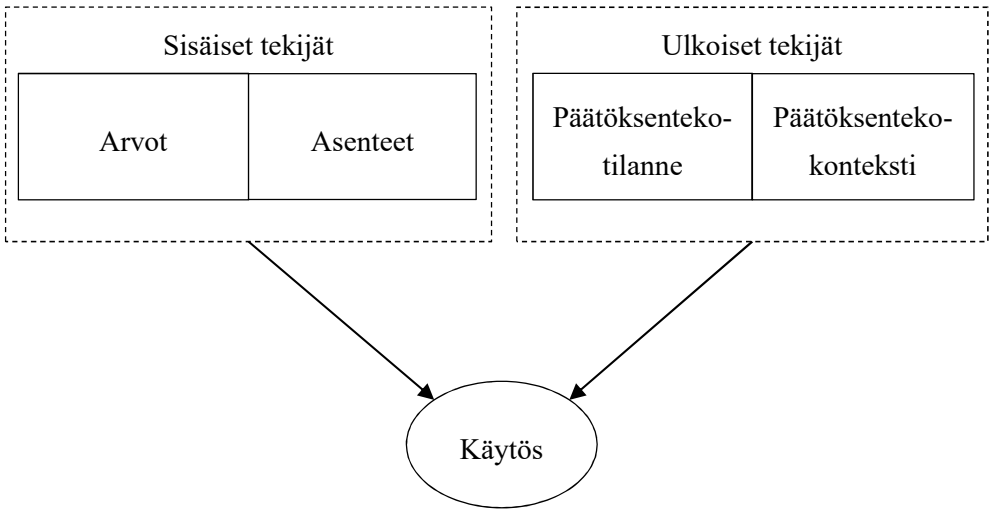
Wangin ym. (2020) tietämykseen liittyvien tekijöiden vaikutus aikeisiin eroaa luvussa 3.2 esitellyistä Dincellin ja Goelin (2017) havainnoista, sillä Dincelli ja Goel (2017) eivät havainneet yhteyttä aikeiden ja internetin lukutaidon välillä. Esimerkiksi kontekstiin liittyvään sivureittiin kuuluvia tekijöitä, eli flow-tilaa ja yksilön ystävien tietojenjakoa, ei olla tarkasteltu muissa tässä tutkielmassa aikaisemmin esitellyissä malleissa. Yksilön ys-

tävien tiedonjakoon liittyvä tekijä voidaan kuitenkin nähdä osana subjektiivisiin normeihin liittyvää määritelmää, sillä yksilöiden muilta ihmisiltä saadut vaikutteet tai paineet ovat yksi esimerkki subjektiivisista normeista. Wangin ym. (2020) havainnot privacy calculus -teorian vaikutuksesta aikeisiin vastaavat muun muassa Lin ym. (2010), Keithin ym. (2013) ja Alashoorin ym. (2018) tuloksia. Wangin ym. (2020) tutkimuksen pohjalta voidaan nostaa esiin seuraavia huomioita:

- Yksityisyyshuolet vähentävät yksilön aikeita luovuttaa tietoja.
- Oletetut hyödyt lisäävät yksilön aikeita luovuttaa tietoja.
- Yksityisyysrikkomuksiin liittyvät tiedot vaikuttavat aikeita vähentävästi.
- Mitä korkeampi on yksilön olettama epäsymmetrisen informaation määrä, sitä vähemmän yksilöllä on aikomuksia luovuttaa tietoja.
- Yksilön ollessa flow-tilassa, sitä enemmän yksilöllä on aikeita luovuttaa tietoja.
- Tiedot yksityisyysrikkomuksista ja oletettu epäsymmetrinen informaatio lisäävät yksityisyyshuolten negatiivista vaikutusta aikeisiin.
- Flow-tila vahvistaa oletettujen hyötyjen positiivista vaikutusta aikeisiin.
- Yksilön ystävien tietojen luovutus vähentää yksityisyyshuolten negatiivista vaikutusta aikeisiin.

3.4 Strukturaatioteoria

Edellisessä alaluvussa esiteltyihin privacy calculus -teoriaan pohjautuviin tutkimuksiin liittyvät tulokset keskittyvät enemmän päätöksenteon rationaaliseen puoleen, eivätkä esimerkiksi usein juurikaan huomioi ympäristön vaikutusta. Zaiferopoulou ym. (2013) korostavat tutkimuksessaan erityisesti sitä, miten privacy calculus -teorian mukaisen kustannus-hyötyanalyysin lisäksi yksilöiden päätöksenteko muistuttaa myös strukturaatioteorian periaatteita. Strukturaatioteorian mukaan yksilön käytös on yhdistelmää ympäröivien rakenteiden, sääntöjen ja resurssien sekä yksilön oman vapaan harkinnan vaikutuksista. Zaiferopouloun ym. (2013) mukaan yksilön omat arvot ja asenteet (sisäiset tekijät) vaikuttavat tietoja luovuttavaa käyttäytymistä vähentäen, kun taas tilanteisiin ja konteksteihin liittyvät seikat (ulkoiset, rakenteelliset tekijät) lisäävät käyttäjän alttiutta käyttäytyä ja luovuttaa tietoja. (Zaiferopoulou ym. 2013, 463–471.) Kuvio 20 kuvastaa strukturaatioteorian mukaiset vaikutukset yksityisyyteen liittyvään käytökseen.



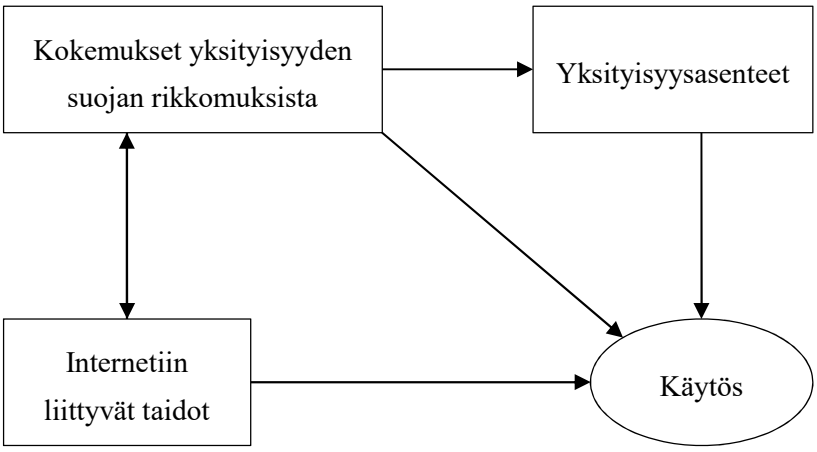
Kuvio 20. Sisäisten ja ulkoisten tekijöiden vaikutus käytökseen strukturaatioteorian mukaan (Zaiferopoulou ym. 2013)

Vaikka luvussa 3.2 esitellyssä mallissa Dincell ja Goel (2017) rajasivat suunnitellun käyttäytymisen teorian tutkimuksessaan arvojen tarkastelun kulttuurillisiin arvoihin, heidän tutkimuksensa tulokset vastaavat Zaiferopouloun ym. (2013) havaintoja arvojen vaikutuksista käytökseen. Asenteiden vaikutus käytökseen puolestaan huomattiin myös luvussa 3.2 Hughes-Robertsin ja Kani-Zahibin (2014) suunnitellun käyttäytymisen teoriaan perustuvassa mallissa. Hughes-Roberts ja Kani-Zahibi (2014) totesivat myös verkkoalustan tai -sivuston käyttöliittymän vaikuttavan käytökseen, joka on päätöksentekotilanteeseen liittyvä kontekstista ja päätöksentekoympäristöstä riippuva tekijä.

3.5 Internetiin ja yksityisyyteen liittyvät taidot

Aikaisemmin tässä tutkielmassa muun muassa mainittiin, miten Barnes (2006) pohdiskeli muun muassa käyttäjien tietoisuuden ja osaamisen lisäämistä yhdeksi potentiaaliseksi ratkaisuksi paradoksiin tai sen lieventämiseksi. Luvussa 2.2 esitellyn mielipiteisiin orientoituneen teorian mukaan yksityisyyden paradoksiin liittyy yksilöiden rajallista tietämystä ja ymmärrystä yksityisyyteen liittyvissä asioissa (Baek 2014). Myös aikaisemmin luvussa 3.2 esitellyssä Dincellin ja Goelin (2017) tutkimusten tulosten mukaan internetiin liittyvillä taidoilla on vaikutuksia yksilön yksityisyyteen liittyvään käyttäytymiseen, muttei aikeisiin. Lisäksi luvussa 3.3 Wang ym. (2020) huomioivat tutkimuksessaan yksilön tietämykseen ja ymmärrykseen liittyviä tekijöitä sekä havaitsivat näiden vaikutukset aikeisiin.

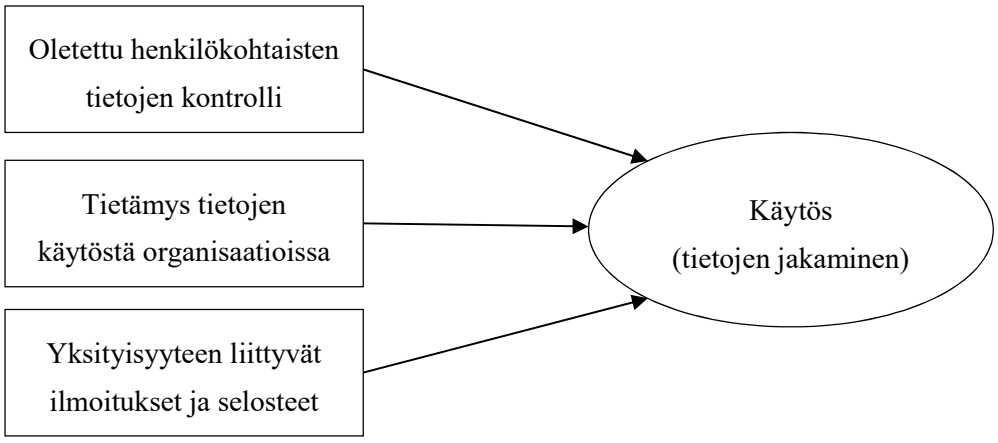
Internetin käyttäminen itsessään vaatii yksilöltä jonkinasteista teknistä osaamista. Kuitenkin myös tietojen jakamista tai yksityisyyttä suojelevia toimenpiteitä pohdittaessa yksilölle on hyötyä datankeruun ja internetiin liittyvästä ymmärryksestä ja osaamisesta. Esimerkiksi organisaatioiden datankeruumetodien ymmärtäminen ja datan analysointiin liittyvien prosessien hahmottaminen voi huomattavasti vaikuttaa yksilöön. Büchin ym. (2016) tutkimuksen mallin mukaan internetiin liittyvät taidot vaikuttavat suoraan yksilön yksityisyyteen liittyvään käytökseen, sillä taidokkaammat yksilöt käyttäytyvät enemmän yksityisyyttä suojaavasti. Tämän lisäksi käytökseen vaikuttavat Büchin ym. (2016) mukaan myös yksityisyyteen liittyvät asenteet sekä aikaisemmat kokemukset yksityisyyden suojaan kohdistuneesta häirinnästä tai muista rikkomuksista; aikaisemmat ongelmat yksityisyyden suojaan liittyen johtavat varovaisempaan käytökseen. Yksityisyyden suojan rikkomukset ovat tyypillisesti esimerkiksi yksilöön liittyvän datan luvatonta keräämistä, myymistä, hyödyntämistä tai julkaisemista. Yksityisyyteen liittyvillä asenteilla (engl. privacy attitudes) tarkoitetaan alun perin yksilön asenteita ja suhtautumista erilaisiin yksityisyyteen liittyviin käytöstapoihin, mutta usein käsitteellä voidaan tarkoittaa myös yksilön omaa arviota hänen kokemistaan yksityisyyshuolista tai yksityisyysriskeistä. Rikkomukset vaikuttavat käytöksen lisäksi myös yksilön yksityisyysasenteisiin. Internetiin liittyvien taitojen ja yksityisyyden suojan rikkomusten välillä havaittiin myös yhteys: taidokkaammat internetin käyttäjät kokevat useammin yksityisyyden suojan rikkomuksia. (Büchi ym. 2016, 1261, 1264–1274.) Büchin ym. (2016) internetiin liittyviin taitoihin perustuva malli esitetään kuviossa 21.



Kuvio 21. Büchin ym. (2016) malli yksityisyyttä suojaavaan käytökseen vaikuttavista tekijöistä

Büchi ym. (2016) tuloksista yksityisyyteen liittyvien asenteiden vaikutukset käytökseen havaittiin muun muassa luvussa 3.4 Zaiferopouloun ym. (2013) tutkimuksessa sekä luvussa 3.2 Hughes-Robertsin ja Kani-Zahibin (2014) tutkimuksessa. Büchin ym. (2016) malli on ainoa tässä tutkielmassa esiteltävä malli, jossa tarkasteltiin yksilön aikaisempien kokemusten vaikutuksia käytökseen.

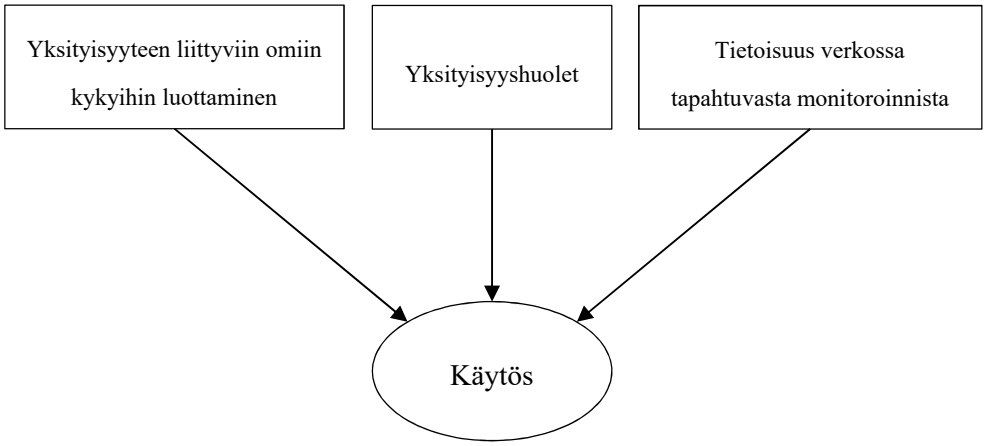
Benson ym. (2015) tarkastelivat tutkimuksessaan (kuvio 22) tietojen käyttöön liittyvän tietämyksen lisäksi yksityisyyteen liittyvien ilmoitusten ja selosteiden sekä oletetun kontrollin vaikutusta tietojen luovuttamiseen (käytökseen). Bensonin ym. (2015) artikkelin tulosten mukaan mitä suurempi yksilön olettama kontrolli omista henkilökohtaisista tiedoistaan on, sitä vähemmän tietoja luovutetaan. Mitä enemmän yksilöillä oli tietoinen sosiaalisen median sivustojen henkilökohtaisten tietojen käytöstä, eli mitä parempi tietämys yksilöllä on yksityisyyteen ja datan käyttöön liittyvissä asioissa, sitä enemmän luovutettiin tietoa. Myös selosteet yksityisyyden suojasta tai ilmoitukset yksityisyyteen liittyen lisäsivät käyttäjän tietojen luovutusta. Selosteiden ja ilmoitusten vaikutus voi johtua esimerkiksi niiden luomasta luotettavammasta ja ammattimaisemmasta vaikutelmasta organisaation käytänteistä. (Benson ym. 2015, 426–435.)



Kuvio 22. Bensonin ym. (2015) malli käytökseen vaikuttavista tekijöistä

Weinberger ym. (2017) huomasivat opiskelijoita koskevassa tutkimuksessaan yksityisyyshuolten ja yksityisyyteen liittyvien omiin kykyihin liittyvän uskomisen noustessa paradoksinmukaisen käyttäytymisen vähenevän. Yksityisyyteen liittyviin omiin kykyihin

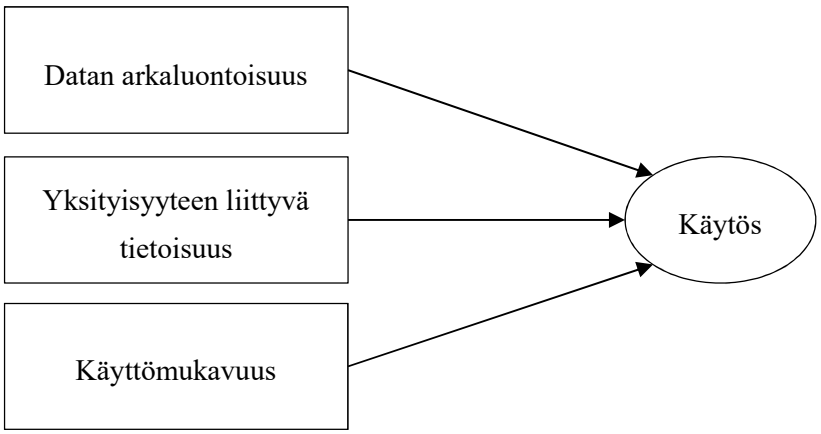
uskominen voidaan nähdä osana yksilön oletettua kontrollia. Näiden lisäksi parempi tietoisuus ja ymmärrys verkossa tapahtuvasta organisaation suorittamasta yksilön tietojen monitoroinnista ja keräämisestä yllättäen vähensivät yksityisyyttä suojaavaa käytöstä. Weinbergerin ym. (2017) mukaan yksityisyysriskeihin liittyvä tietoisuus ei vaikuttanut käytökseen merkittävästi, mutta verkon monitorointiin ja datankeruuseen liittyvät tiedot ja taidot vaikuttivat. (Weinberger ym. 2017, 10–13.) Weinbergerin ym. (2017) malli on hyvin lähellä Bensonin ym. (2015) mallia, sillä molemmat tarkastelevat internetiin ja yksityisyyteen liittyvän tietoisuuden sekä yksilön kontrolliin liittyvien seikkojen vaikutuksia käytökseen. Weinbergerin ym. (2017) tulokset käytökseen vaikuttavista tekijöistä ovat koottu kuvioon 23.



Kuvio 23. Weinbergerin ym. (2017) tutkimus internetiin ja yksityisyyteen liittyvistä kyvykkyyksistä

Williamsin ym. (2019a; 2019b) tutkimuksissa havaittiin älykellojen avulla hyödynnettävien yksityisyyteen perustuvien pelien kaventavan yksilöiden käytöksen ja asenteiden välistä eroa. Peleissä pelaajia ohjeistettiin ja opetettiin yksityisyyttä suojaavista toimenpiteistä. Tutkimuksissa keskeistä oli lisätä yksilöiden tietoisuutta yksityisyydestä ja edistää yksityisyyden suojaa. Yksityisyyden suojaa edistävien pelien avulla yksilön tietoisuutta lisäämällä nähtiin yksilön käyttäytyvän enemmän yksityisyyttä suojaavasti. Tutkimuksissa havaittiin käytökseen vaikuttaviksi tekijöiksi kerättävän datan arkaluontoisuus, yksityisyyteen liittyvä tietoisuus ja palveluun liittyvä käyttömukavuus. Käyttömukavuus on esimerkki yksilön kokemista hyödyistä. Paradoksiin liittyvää aikeiden ja käytöksen välistä kuilua voidaan osittain kaventaa tutkimusten mukaan lisäämällä yksilöiden tietoi-

suutta yksityisyydestä ja tiedon keräämisestä, sillä usein yksilöt eivät tiedosta yksityisyyttään vaarantavaa käytöstä. (Williams ym. 2019a, 121, 133–134; Williams ym. 2019b, 38–40, 50.) Nämä tulokset ovat linjassa myös aikaisemmin luvussa 3.2 esitellyn Hughes-Robertsin ja Kani-Zahibin (2014) tutkimuksen kanssa, joka havaitsi käyttöliittymässä esitettävien kannustimien, tiedonantojen tai suositusten vaikuttavan yksilöön. Myös esimerkiksi Fatiman ym. (2019, 1) tutkimus yksityisyyteen liittyvän tietoisuuden ja taitojen vahvistamisesta havaitsi vastaavanlaisen peliasetelman kautta paremman tietoisuuden ja taitojen vähentävän yksilöiden tietojen luovutusta. Williamsin ym. (2019a; 2019b) tutkimuksien muutkin tulokset ovat samankaltaisia aikaisempien mallien kanssa, sillä kysyttävien tietojen arkaluontoisuuden vaikutuksen käytökseen huomasivat Marwick ja Hargittai (2019) ja hyötyjen vaikutuksen käytökseen muun muassa Keith ym. (2013) sekä Marwick ja Hargittai (2019) luvussa 3.3. Molempien älykellopeleihin liittyvien tutkimusten tulokset ovat havainnollistettu kuviossa 24.



Kuvio 24. Yksilön tietoisuutta lisäävän tutkimuksen tulokset (Williams ym. 2019a; 2019b)

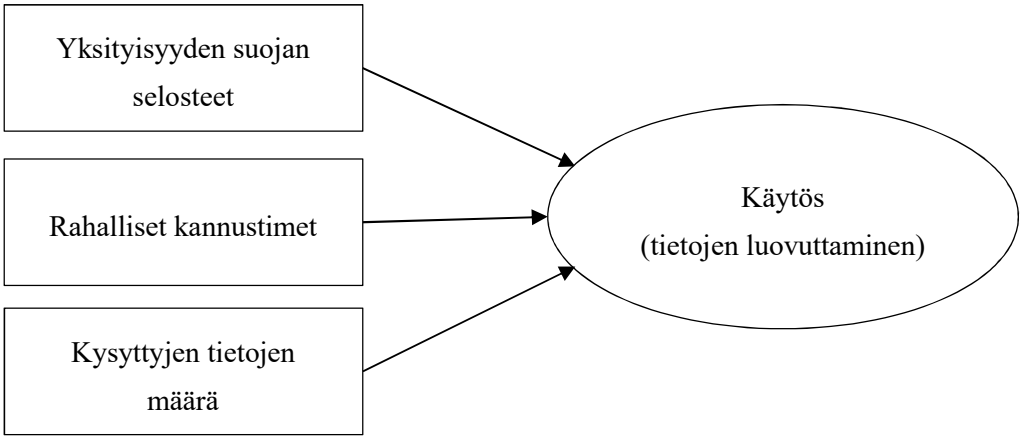
Tässä alaluvussa esitellyistä malleissa, eli Bensonin ym. (2015), Büchin ym. (2016), Weinbergerin ym. (2017) ja Williamsin ym. (2019a; 2019b) tutkimuksissa internetiin ja yksityisyyteen liittyvien taitojen ja ymmärryksen vaikutuksia tarkasteltiin ainoastaan käytökseen. Aikaisemmin tämän tutkielman luvussa 3.3 Wangin ym. (2020) käsitelty tutkimus havaitsi verkkoon liittyvän tietämyksen vaikuttavan myös aikeisiin.

3.6 Verkkosivustot ja tietosuojaselosteet

3.6.1 Tietosuojaselosteet

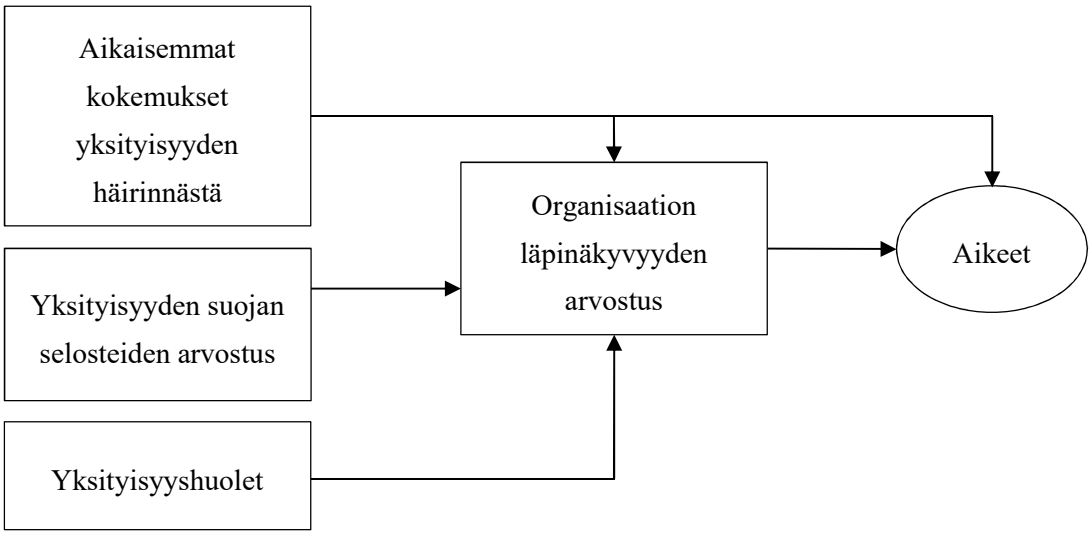
Organisaatioille on yhä yleisempää pyrkiä vakuuttamaan yksilöt sivustonsa tai palvelunsa yksityisyyden suojasta. Usein tätä voidaan tehdä muun muassa yksityisyyden suojaan liittyvien viestien, selosteiden tai merkkien muodossa. Luvussa 3.5 Bensonin ym. (2015) internetiin ja yksityisyyteen liittyvään ymmärrykseen keskittyvä tutkimus havaitsi yksityisyyteen liittyvien ilmoitusten ja selosteiden vaikuttavan yksilöiden käytökseen.

Hui ym. (2007) tutkivat tutkimuksessaan yksityisyyteen liittyvien lupausten, vakuuttelujen ja merkkien vaikutusta yksilöiden tietojen jakamiseen (käytökseen). Tulosten mukaan tietosuojaselosteet lisäsivät yksilöiden tietojen luovutusta, kun taas yksityisyyteen liittyvillä merkeillä, tunnustuksilla tai sineteillä (esimerkiksi TRUSTe-sertifikaatti) ei ollut vaikutuksia käytökseen. Tietosuojaselosteiden ja yksityisyysmerkkien vaikutus oli täysin samanlainen yksilön ymmärryksestä huolimatta. Yksilön ymmärryksen ja tietämyksen vaikutus on rajoittunutta; esimerkiksi muulla internetiin liittyvällä ymmärryksellä on havaittu olevan vaikutuksia käytökseen (ks. esim. Benson ym. 2015; Büchi ym. 2016; Dincelli & Goel 2017; Weinberger ym. 2017; Williams ym. 2019a; 2019b), mutta yksilöiden ymmärrys tietosuojaselosteista tai yksityisyysmerkeistä ei siis merkinnyt mitään. Selosteen olemassaolo itsessään siis vaikuttaa yksilöihin. Tämän lisäksi tutkimuksessa havaittiin taloudellisten kannusteiden tai hyötyjen lisäävän tietojen luovutusta. Kysyttyjen tietojen määrän lisääntyessä yksilöt olivat haluttomampia jakamaan tietoja, mutta Huin ym. (2007) tutkimuksen mukaan kysyttyjen tietojen arkaluontoisuudella ei havaittu vaikuttavan merkittävästi tietojen luovutukseen. (Hui ym. 2007, 19–29.) Sen sijaan aikaisemmin esiteltyjen luvun 3.3 Marwickin ja Hargittain (2019) sekä luvun 3.5 Williamsin ym. (2019a; 2019b) mallien mukaan arkaluontoisuus vaikutti käytökseen. Huin ym. (2007) tutkimuksen tulokset on esitetty kuviossa 25.



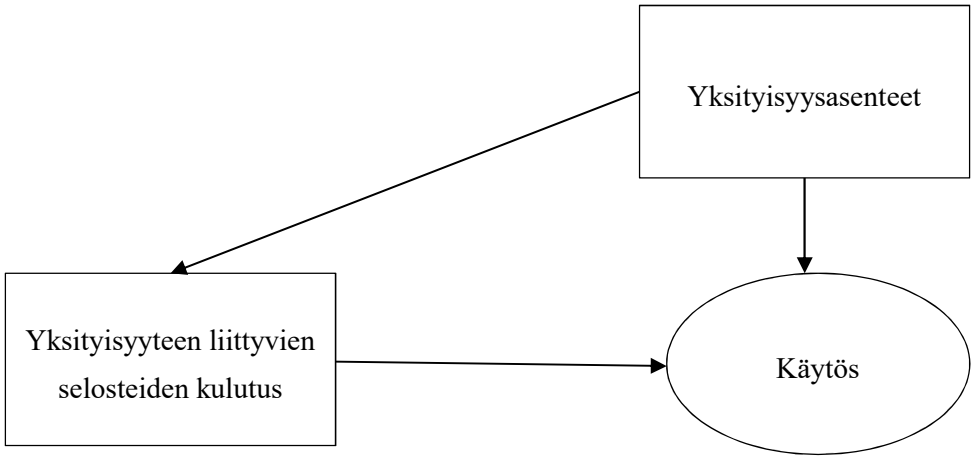
Kuvio 25. Huin ym. (2007) tulokset selosteisiin liittyvästä tutkimuksesta

Huin ym. (2007) ja luvussa 3.5 esitetyn Bensonin ym. (2015) mallien lisäksi Awadin ja Krishnanin (2006) mallissa esiintyi yksityisyyden suojan selosteiden arvostukseen liittyvä tekijä. Awadin ja Krishnanin (2006) tutkimuksen tulosten mukaan (kuvio 26) aikeisiin vaikuttavat aikaisemmat kokemukset yksityisyyden suojan häirinnästä (luovutettujen tietojen avulla tehdyn personoidun mainonnan kohdalla) ja organisaation läpinäkyvyyden arvostus. Aikaisemmat kokemukset ja läpinäkyvyyden arvostus vaikuttivat aikeisiin negatiivisesti. Awadin ja Krishnanin (2006) havaintoa aikaisempien kokemusten vaikutuksista aikeisiin täydentää aikaisemmin luvussa 3.5 esitellyn Büchin ym. (2016) mallin havaintoja aikaisempien kokemusten vaikutuksista käytökseen. Yksityisyyden suojan selosteiden arvostus, yksityisyyshuolet ja aikaisemmat kokemukset vaikuttivat kaikki positiivisesti läpinäkyvyyden arvostukseen. Selosteiden arvostuksen yhteyttä aikeisiin ei kuitenkaan tarkasteltu. (Awad & Krishnan 2006, 13–26.)



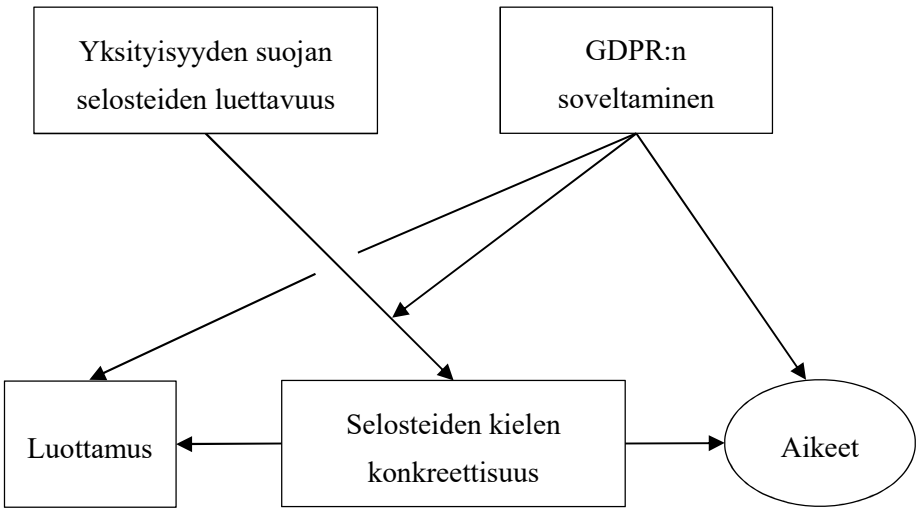
Kuvio 26. Awadin ja Krishnanin (2006) paradoksiin liittyvien aikeiden tutkimuksen tulokset

Siinä missä Huin ym. (2007) tutkimus tarkasteli yksityisyyden suojan selosteiden olemassaolon vaikutusta yksilön käytökseen, Stutzman ym. (2011) tutkivat artikkelissaan sitä, miten yksityisyyden suojaan liittyvien selosteiden tunteminen ja lukeminen vaikuttavat käyttäytymiseen. Myös Stutzman ym. (2011) löysivät tukea yksilöiden yleisestä tavasta jättää selosteet huomiotta. Jopa 47 prosenttia ei ole koskaan lukenut selosteita, noin 47 prosenttia on silmäillyt selosteita vähintään kerran ja ainoastaan noin kuusi prosenttia lukevat selosteita valtaosin tai kokonaan. Gerberin ym. (2018, 227) mukaan noin 59 prosenttia verkon käyttäjistä ainoastaan silmäilevät käyttöehdot verkossa tehtävien transaktioiden yhteydessä ja 14 prosenttia yksilöistä ei lue käyttöehtoja ollenkaan. Artikkelissa jaettiin käytös erikseen tietojen luovuttamiseen sekä yksityisyyteen liittyviin toimenpiteisiin (kuten esimerkiksi yksityisyysasetusten muuttaminen), mutta tässä tutkielmassa käytökseen liittyviä käsitteitä tarkastellaan yksittäisen saman termin (yksityisyyteen liittyvä käytös) alla. Tutkimuksessa tarkasteltiin lisäksi yksityisyyteen liittyvien asenteiden vaikutusta käytökseen. Lopputuloksena Stutzman ym. (2011) esittävät, että yksityisyysasenteet vaikuttavat käytökseen sekä suojaavia toimenpiteitä kasvattavasti että tietojen luovutusta vähentävästi ja asenteet lisäävät yksityisyysselosteiden kulutusta, lukemista ja käyttöä. Selosteiden kulutus ja lukeminen puolestaan vähentää tietojen luovutusta. (Stutzman ym. 2011, 590–598.) Tutkimuksen tulokset esitetään kootusti kuviossa 27.



Kuvio 27. Stutzmanin ym. (2011) yksityisyyden suojan selosteita ja yksityisyysasenteita tutkiva malli

Vaikka GDPR on Euroopan unionin jäseniä ja EU:n alueella dataa kerääviä organisaatioita sitova, voivat myös muut valtiot soveltaa GDPR:n mukaisia tietosuojakäytäntöjä halutessaan omilla toiminta-alueillaan. Zhang ym. (2019) tarkastelivat tutkimuksessaan (kuvio 28) sitä, miten GDPR:n mukaisten käytänteiden noudattaminen ja organisaatioiden yksityisyyden suojaan liittyvien selosteiden konkreettisuus vaikuttavat yksilön aikeisiin. Heidän tulostensa mukaan GDPR:n mukaisten käytänteiden soveltaminen lisäsi sekä yksilöiden halukkuutta luovuttaa tietoja verkossa toimivalle organisaatiolle että luottamusta yritystä kohtaan. Yksityisyyden suojan selosteiden ollessa selkolukuisia ja kielellisesti konkreettisia, oli vaikutus luottamukseen ja aikeisiin myös positiivinen. Toisin sanoen jo pelkät selosteen muotoseikat vaikuttavat yksilöön. Tyypillisesti organisaatioiden yksityisyyden suojan liittyvät selosteet, ilmoitukset ja tiedonannot ovat vaikealukuisia ja pitkiä. Tuloksissa havaittiin myös luettavuuden vaikutuksen olevan suurempi, mikäli GDPR:n käytänteitä sovellettiin. Luettavuudella tarkoitetaan mallissa ennen kaikkea sitä, että selosteet ovat helposti ymmärrettävissä kirjoitustavan ansiosta. (Zhang ym. 2019.)



Kuvio 28. Zhangin ym. (2019) tutkimus selosteiden konkreettisuuden ja GDPR:n soveltamisen vaikutuksista aikeisiin

Selosteiden vaikutuksista voidaan siis sanoa, että pelkkä selosteiden olemassaolo (Hui ym. 2017) kasvattaa yksilöiden tietojen jakoa, selosteiden lukeminen vähentää tietojen jakoa (Stutzman ym. 2011) ja selosteiden konkreettisuus kasvattaa yksilön aikomuksia jakaa tietoja (Zhang ym. 2019).

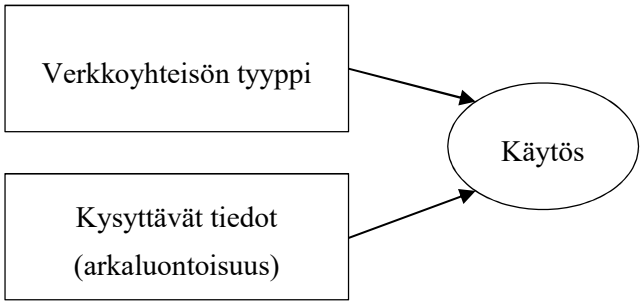
3.6.2 Verkkosivustoihin liittyvät tekijät

Kuten aikaisemmin luvussa 3.2 Hughes-Robertsin ja Kani-Zahibin (2014) tutkimusten tulosten yhteydessä todettiin, käyttöliittymällä voidaan vaikuttaa yksilön tietojen jakoon liittyvään käyttäytymiseen. Tämän pohjalta onkin aiheellista tarkastella, onko muilla verkkosivustoon tai verkon päätöksentekotilanteisiin liittyvillä tekijöillä vaikutuksia yksilöön.

Schrammel ym. (2009) jakavat verkkosivustojen ja -yhteisöjen tyypit neljään luokkaan. Ammatti- ja työelämään liittyviä sivustoja, kuten esimerkiksi verkkoyhteisöpalvelu LinkedIniä, käytetään työelämään liittyvien suhteiden solmimiseen, hallitsemiseen ja ylläpitämiseen. Verkkosisältöön ja median jakamiseen liittyvissä verkostoissa, kuten esimerkiksi videopalvelu YouTubessa tai Flickr-kuvapalvelussa, pääideana on jakaa sekä julkaista kuvia, videoita, ääntä tai muuta multimediaa. Pääfokus on siis itse sisällössä, mutta sivustoissa on myös yhteisöllisiä elementtejä. Sosiaaliset verkostot ja yhteisöt ovat puolestaan pääasiassa henkilökohtaisten suhteiden ja yksityiselämän kommunikointiin

tarkoitettuja sivustoja. Esimerkiksi sosiaalisen median sivusto Facebook lukeutuu sosiaalisiin verkostoihin. Sosiaaliset uutissivustot, kuten esimerkiksi Digg, ovat tarkoitettuja uutisten ja artikkelien jakamiseen. (Schrammel ym. 2009, 277.)

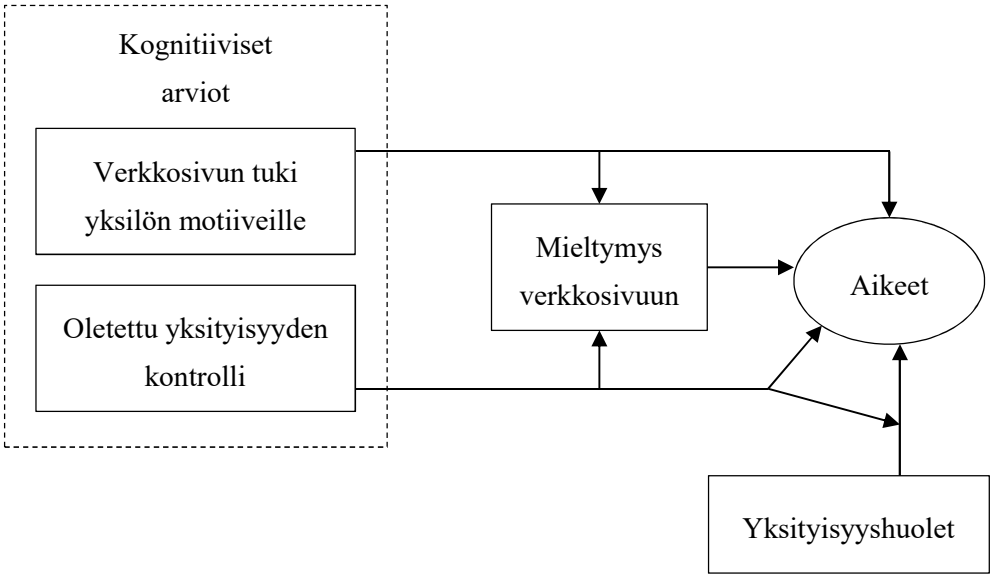
Schrammelin ym. (2009) tutkimuksen mukaan (kuvio 29) verkkoyhteisön tyypillä on vaikutusta tietojen jakamiseen liittyvään käyttäytymiseen. Esimerkiksi sosiaalisissa verkostoissa ja työelämään liittyvissä sivustoissa tietoja luovutettiin herkemmin kuin verkkosisältöön tai uutisiin perustuvissa yhteisöissä. Tutkimuksessa huomattiin myös kysyttävän tiedon tyypillä ja arkaluontoisuudella olevan vaikutuksia käytökseen. Mitä arkaluontoisemmaksi tieto koettiin, sitä epätodennäköisemmin käyttäjä luovutti tiedon. Muun muassa nimi tai syntymäpäivä luovutetaan huomattavasti herkemmin kuin esimerkiksi kotiosoite tai puhelinnumero. (Schrammel ym. 2009, 275–282.) Aikaisemmin mainitun Huin ym. (2007) tutkimuksen perusteella puolestaan arkaluontoisuudella ei ollut vaikutusta käytökseen, kun taas Marwickin ja Hargittain (2019) sekä Williamsin ym. (2019a; 2019b) mukaan arkaluontoisuus vaikutti käytökseen.



Kuvio 29. Verkkoyhteisön tyypin ja tietojen arkaluontoisuuden vaikutus käytökseen (Schrammel ym. 2009)

Schrammel ym. (2009) tarkastelivat verkkoyhteisön tyypin vaikutusta, kun taas Li ym. (2017) tarkastelivat tutkimuksessaan yksityisyyteen liittyvää käyttäytymistä soveltamalla MD-teoriaa (engl. multidimensional developmental theory, MDT) ja tarkastelemalla muun muassa verkkosivustoihin liittyvää mieltymystä ja sivuston koettua tukea yksilön henkilökohtaisille motiiveille. MD-teorialla on kaksi oletusta. Ensimmäiseksi, yksilöt yrittävät kontrolloida päätöksentekotilanteita eikä heillä ole täydellistä informaatiota yksityisyyteen liittyvissä päätöksentekotilanteissa. Toiseksi, yksilöllä on rajallinen määrä mahdollisuuksia olla vuorovaikutuksessa sosiaalisen ja fyysisen ympäristönsä kanssa ja yksityisyydessä on lähtökohtaisesti kyse näiden vuorovaikutusten hallitsemisesta. MD-

teoria ottaa siis huomioon sekä yksilöllisiä että ympäristöön liittyviä tekijöitä huomioon. (Li ym. 2017, 1012–1015.) MD-teoriasta sovellettu malli yksityisyyteen liittyvän käytöksen tutkimuksessa on esitelty kuviossa 30.



Kuvio 30. Lin ym. (2017) tutkimus yksilöön ja ympäristöön liittyvistä tekijöistä

Lin ym. (2017, 1015–1019) mallin tulokset ovat tiivistetysti sanottuna seuraavanlaiset:

- Mieltymys verkkosivuun sekä kognitiiviset arviot (sivuston tuki yksilön motiiveille ja oletettu yksityisyyskontrolli) vaikuttavat positiivisesti yksilön aikeisiin luovuttaa tietoja, yksityisyyshuolet puolestaan vaikuttivat negatiivisesti aikeisiin luovuttaa tietoja.
- Käsitellyt kognitiiviset arviot lisäävät yksilön mieltymystä verkkosivustoa kohtaan.
- Oletettu yksityisyyden kontrollilla oli vaikutuksia yksityisyyshuolten ja aikeiden väliseen suhteeseen; mitä korkeampi oletettu yksityisyyskontrolli oli, sitä voimakkaampi oli yksityisyyshuolten negatiivinen vaikutus.

3.7 Teorioita ja malleja muista yksilöön liittyvistä tekijöistä

Useissa tässä pääluvussa aikaisemmin käsitellyissä malleissa, teorioissa ja tuloksissa on esiintynyt yksilöön liittyviä tekijöitä, kuten esimerkiksi yksilön oletuksia yksityisyyden kontrollista (ks. esim. Zorotheos & Kafeza 2009; Hughes-Roberts & Kani-Zahibi 2014; Benson ym. 2015; Weinberger ym. 2017), yksilön oma käsitys tietojen arkaluontoisuudesta (ks. esim. Schrammel ym. 2009; Marwick & Hargittai 2019; Williams ym. 2019a;

2019b) tai yksilön kykyihin ja tietämykseen liittyviä tietoja (ks. esim. Benson ym. 2015; Büchi ym. 2016; Dincelli & Goel 2017; Weinberger ym. 2017; Williams 2019a; 2019b; Wang ym. 2020). Seuraavaksi kuitenkin tarkastellaan tarkemmin huomattavasti yksilökohtaisempia ominaisuuksia.

3.7.1 Yksityisyyspersoonallisuus

Yksilöillä on usein lukuisissa ominaisuuksissa, tavoissa tai ajattelutavoissa persoonallisia piirteitä, taipumuksia tai käytäntötapoja. Yksilöitä erotellaan tai vertaillaan persoonallisuuteen liittyvien ominaisuuksiensa perusteella ja sama pätee yksilön tapoihin suhtautua yksityisyyden suojaan tai yksityisyyteen liittyviin päätöksentekotilanteisiin. Verkon käyttäjiä pystytään luokittelemaan yksityisyyteen suhtautumiseen perustuen, sillä ihmisten keskuudessa on havaittu piirteitä erilaisten yksityisyyspersoonallisuuksien olemassaolosta. Hannin ym. (2007) mukaan yksilöt jakautuvat kolmeen ryhmään: yksityisyyden suojelijoihin (engl. privacy guardians), mukavuudenhaluisiin (engl. convenience seekers) ja tietojen myyjiin (engl. information sellers). Hannin ym. (2007) mukaan eri ryhmään kuuluvilla havaittiin eroja käyttäytymisessä. Lee ym. (2011) nimittävät ryhmiä puolestaan yksityisyyteen fundamentaalisesti suhtautuviksi (engl. the privacy fundamentalists), yksityisyyteen pragmaattisesti suhtautuviksi (engl. the privacy pragmatists) ja yksityisyyden suhteen huolettomiksi (engl. the privacy unconcerned). Yksityisyyden suojelijat sekä fundamentalistit suojelevat tiukasti yksityisyyttään eivätkä lähtökohtaisesti luovuta tietojaan verkossa tai osallistu personointiin. Pragmatistit ja mukavuudenhaluiset luovuttavat tietojaan maltillisesti käyttömukavuuden lisäämiseksi ja edellyttävät jonkinasteista yksityisyyden suojaa. Huolettomille ja tietojaan myyville on tyypillistä luovuttaa henkilökohtaisia tietoja helposti, huolettomasti ja usein taloudellisten hyötyjen toivossa. (Hann ym. 2007, 30, 33–34; Lee ym. 2011, 425–426.)

James (2014) puolestaan jakaa yksityisyyteen suhtautumisen liittyvät tavat kolmeen luokkaan nuorten keskuudessa. Yksityisyyden hylänneet ajattelevat yksityisyyden olevan mahdotonta saavuttaa verkossa. Yksityisyyden sosiaalisesta näkökulmasta näkevät ihmiset ajattelevat sosiaalisten kontaktiensa toimintatapoja omissa valinnoissaan ja ajattelevat myös sosiaalisten kontaktiensa noudattavan samaa periaatetta. Viimeinen ryhmä taas ajattelee yksityisyyden suojan olevan täysin kiinni omista valinnoistaan; yksilön on itse nähtävä vaivaa yksityisyyden suojan luomiseksi ja ylläpitämiseksi. (James 2014, Kimin 2015, 1168–1169 mukaan.)

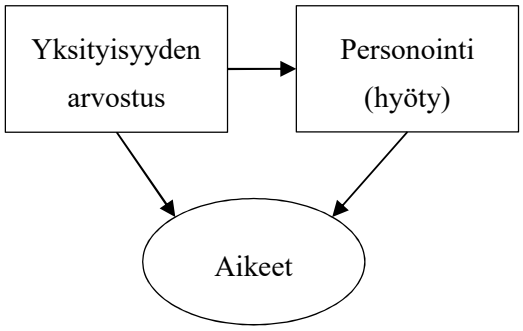
Adorjan ja Ricciardelli (2019) tunnistivat yksilöiden keskuudessa uudenlaisen asenteen, erityisesti teini-ikäisten ja nuorten keskuudessa: yksilöt kokevat, että heillä ei ole mitään salattavaa tai menetettävää eikä yksityisyys ole enää relevanttia verkossa ja tämän takia yksityisyyttä suojaavia toimenpiteitä, eli käytöstä, ei suoritettu. Yksityisyyden heikkenemisestä on tullut toisin sanoen hyväksyttävää ja luonnollinen osa internetiä. Yksityisyys on tärkeää vasta, jos tekee jotain salassa pidettävää, väärää tai tuomittavaa. Tämänkaltaisen ajattelumallin omaavilla oli myös tyypillisempää se, että yksityisyyshuolet kohdistuivat vähemmän viranomaisiin tai organisaatioihin ja enemmän muita yksilöitä kohtaan. (Adorjan & Ricciardelli 2019, 8, 21–22.) Toisin sanoen, yksityisyyshuolet ovat painottuneempia luvussa 2.3 esiteltyyn yksityisyyshuolten sosiaaliseen näkökulmaan kuin institutionaaliseen näkökulmaan.

Adorjan ja Ricciardelli (2019) ehdottavat niin sanottua ”nothing to hide” -ajattelutapaa lisäykseksi Jamesin (2014) esittämiin ryhmiin. Vaikka yksilö ajatteleekin, ettei hänellä ole mitään salattavaa ulkopuolisilta, on ajattelumallissa yhä ongelmia. Yksilön tietoja voidaan yhä varastaa tai käyttää luvattomasti, vaikka yksilö ei tietoja kokisikaan arkaluontoisiksi tai salassa pidettäviksi. (Adorjan & Ricciardelli 2019, 8, 21–22.) Myös aikaisemmin luvussa 3.3 esitetyssä Marwickin ja Hargittain (2019, 1798–1709) tutkimuksessa löytyi tukea yksilöiden ajattelutavalle, ettei heillä ole mitään salattavaa ja yksityisyyden suhteen ei ole mitään menetettävää; yksityisyyteen liittyvillä persoonallisilla piirteillä oli vaikutuksia käytökseen. Yksilöt ajattelevat samalla, että yksityisyyttä ei voi saavuttaa lähtökohtaisesti internetin aikakaudella ja yksityisyyden suojan rikkomukset sekä heikkeneminen ovat väistämättömiä verkossa; yksityisyyden suoja on mahdollista vain tilanteissa, joissa on valinnanvaraa ja verkon käyttö koetaan nykyään pakolliseksi osaksi elämää (Adorjan & Ricciardelli 2019, 8, 21–22).

Schomakers ym. (2019) jakavat yksilöt puolestaan yksityisyyden suojelijoihin, yksityisyyden kyynikkoihin ja yksityisyyden pragmatisteihin. Ryhmät ovat lähellä Hannin ym. (2007) sekä Leen ym. (2011) edellä mainittuja ryhmiä, mutta ovat selkeämmin yksityisyyden paradoksiin liitettävissä. Kaikilla ryhmillä on toiminnastaan huolimatta yksityisyyshuolia. Schomakersin ym. (2019) mukaan eri ryhmiin kuuluvat käyttäytyivät toisistaan eroavasti ja eri ryhmään kuuluvien yksityisyysasenteet erosivat toisistaan. Suojelijat arvostavat yksityisyyttään sekä heillä on usein paljon yksityisyyshuolia ja sen mukaisesti tietoja luovutetaan hillitysti ja suojaavia toimenpiteitä tehdään kohtuullisesti. Kyynikot eivät suojele yksityisyyttään korkeista huolistaan huolimatta. Kyynikot ovat yleensä teknisesti vähemmän osaavia, jolla he perustelevat ristiriitaisuuksia aikeidensa ja

käyttäytymisensä välillä. Viimeiseen ryhmään kuuluvat eli pragmatistit suojelevat yksityisyyttään tehokkaasti huomattavasti alhaisemmista yksityisyyshuolistaan huolimatta. Pragmatistit ovat hyvin tietoisia yksityisyyden suojan heikkenemisestä. Schomakersin ym. (2019) tutkimuksessa ei löydetty tukea huolettoman persoonallisuuden tai ryhmän olemassaololle. Kyynikoiden piirteisiin nojaten voidaan myös sanoa, että internetiin liittyvillä taidoilla ja ymmärryksellä voisi olla paradoksia lieventävä vaikutus. (Schomakers ym. 2019, 742–744.) Vaikka tarkemmissa määrittelyissä esiintyykin pieniä eroavaisuuksia, voidaan lyhyesti sanottuna todeta yksityisyyspersoonallisuuden ja siihen liittyvien piirteiden vaikuttavan siis yksilöiden aikeisiin ja käyttäytymiseen.

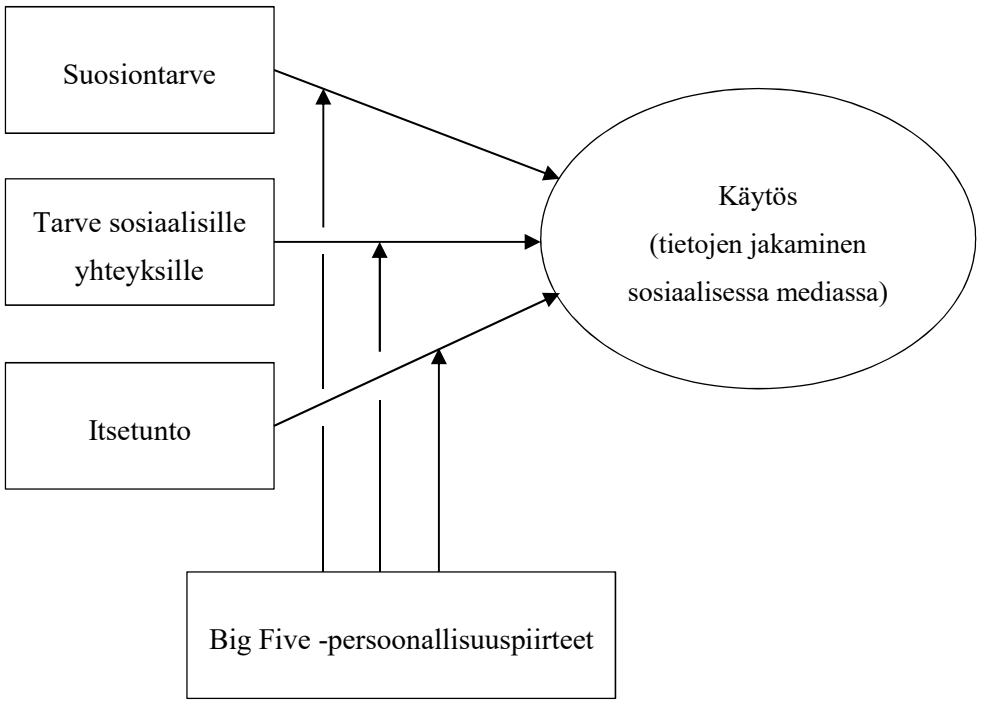
Karwatzki ym. (2017, 372) puolestaan nimittävät eroja yleisten yksityisyyteen liittyvien preferenssien välillä yksityisyyden arvostukseksi (engl. disposition to value privacy, DTVP). Yksityisyyden arvostus on heidän mukaansa yksilöllinen ja persoonallisuuteen liittyvä tekijä, joka kuvastaa arvostuksen lisäksi yksilön tarvetta yksityisyydelle. Mitä alhaisemmin yksilö arvostaa yksityisyyttä, sitä halukkaampia ja valmiimpia yksilöt ovat luovuttamaan tietojaan, eli toisin sanoen yksityisyyden arvostuksella on vaikutuksia myös aikeisiin. Yksityisyyden arvostus vaikutti myös personointiin; mitä enemmän yksilö arvostaa yksityisyyttään, sitä vähemmän yksilö haluaa personointia. Karwatzkin ym. (2017) mukaan personointi motivoi yksilöä jakamaan henkilökohtaisia tietojaan organisaatioille. Personointi, joka on käytännössä yksi hyödyistä, kasvatti yksilön käsitystä kokonaishyödyistä ja siten halukkuutta jakaa tietoja. Nämä johtopäätökset ovat esitetty kuviossa 31. Heidän tutkimuksessaan havaittiin myös, että organisaation prosessien ja käytäntöjen läpinäkyvyyteen liittyvien ominaisuuksien olemassaolo ei vaikuta itsessään yksilöiden halukkuuteen jakaa tietoja. (Karwatzki ym. 2017, 372, 387–392.)



Kuvio 31. Karwatzkin ym. (2017) tutkimus personoinnin ja yksityisyyden arvostuksen vaikutuksista

3.7.2 Sosiaaliset tarpeet ja itsetunto

Yksityisyyteen liittyvien persoonallisuuspiirteiden lisäksi, yksityisyyden paradoksiin liittyvässä tutkimuksessa on tarkasteltu muiden persoonallisten tekijöiden vaikutusta käytökseen. Chen ym. (2015) tutkivat yksilön sosiaalisen suosion halukkuuden, sosiaalisten yhteyksien tarpeen ja itsetunnon vaikutuksia tietojen jakamiseen (käytökseen) sosiaalisen median sivustoille. Tämän lisäksi he tarkastelivat viiden suuren persoonallisuuden piirteen (engl. Big Five personality traits) välillisiä vaikutuksia käytökseen. Nämä viisi piirrettä ovat ekstroversio eli ulospäinsuuntautuneisuus, avoimuus, tunnollisuus, tunnevakaus ja sovinnollisuus eli tunteellinen yhteys muihin. Persoonallisuuspiirteiden vaikutusta käytökseen suoraan ei tutkittu, mutta piirteet vaikuttivat kolmen edellä mainitun tekijän, eli sosiaalisen suosion ja yhteyksien tarpeen sekä itsetunnon kautta välillisesti käyttäytymiseen. Tutkimuksen malli ja tulokset ovat havainnollistettuna kuviossa 32. (Chen ym. 2015, 815–818, 825–829.)

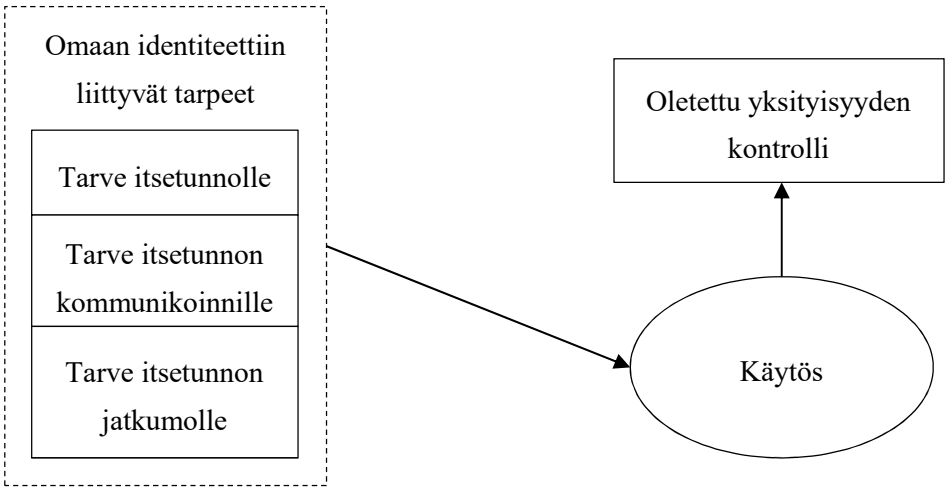


Kuvio 32. Sosiaalisten tarpeiden ja itsetunnon vaikutukset yksilön käytökseen (Chen ym. 2015)

Korkea tarve suosiolle ja sosiaalisille yhteyksille sekä alhainen itsetunto lisäsivät yksilöiden tietojen luovutusta. Muutamia esimerkkejä Big Five -persoonallisuuspiirteiden vaikutuksesta Chenin ym. (2015) tutkimuksessa olivat muun muassa:

- Kun tarve sosiaalisille yhteyksille on korkea ja yksilön tunnevakaus, avoimuus ja tunnollisuus ovat alhaiset, luovutettiin tietoja herkemmin.
- Hyvä itsetunto ja sovinnollisuus vähensivät yksilön tietoja luovuttavaa käytöstä.
- Korkea suosiontarve ja ekstroversio lisäsivät yksilön tietoja luovuttavaa käyttäytymistä.

Itsetuntoon ja sosiaalisiin tarpeisiin liittyviä seikkoja sivusi tutkimuksessaan myös Wu (2019). Hänen tutkimuksensa keskipisteessä olivat yksilön identiteetin tarpeeseen liittyvien seikkojen vaikutukset käytökseen. Tarkemmin katseltuna yksilön oman identiteetin tarpeella voidaan sanoa olevan kolme ulottuvuutta: tarve tuntea itsensä, tarve ylläpitää oman identiteetin jatkumoa menneisyydestä nykypäivään ja tarve ilmaista itseään muille. Itsensä tuntemiseen liittyvät seikat liittyvät itsetuntoon, kun taas esimerkiksi itseilmaisuun liittyvät tarpeet liittyvät sosiaalisiin tarpeisiin. Artikkelissa käsiteltiin yksityisyyttä suojaavaa käytöstä ja tietojen luovuttamiseen liittyvää käytöstä erikseen. Tässä tutkielmassa sekä yksityisyyttä edistävää että heikentävää käytöstä tarkastellaan saman käsitteen kautta, joten kuviossa 33 tuloksia esitettävässä mallissa molemmat käytökseen viittaavat termit ovat yhdistetty yleisemmin käytös-termin alle. Oman identiteetin tarpeiden nähtiin lisäävän sekä tietoja luovuttavaa käytöstä että tietoja suojaavaa käytöstä. Tutkimuksessa selvisi lisäksi, että yksilön aikaisemmalla (yksityisyyttä suojaavalla) käytöksellä on vaikutuksia oletettuun yksityisyyden kontrollin käsitykseen. Oletetun yksityisyyden kontrollin ei havaittu vaikuttavan tietoja luovuttavaan käytökseen eikä vaikutuksia yksityisyyttä suojaavaan käytökseen tarkasteltu ollenkaan Wun (2019) tutkimuksessa. (Wu 2019, 207–215.) Wun (2019) tutkimus on ainoa tässä tutkielmassa esitetyistä malleista, joka ei löytänyt tukea oletetun kontrollin vaikutuksista käytökseen (vrt. Hughes-Roberts & Kani-Zahibi 2014; Beldad & Koehorst 2015; Benson ym. 2015; Weinberger ym. 2017; Booth & Ho 2019; Xie ym. 2019).

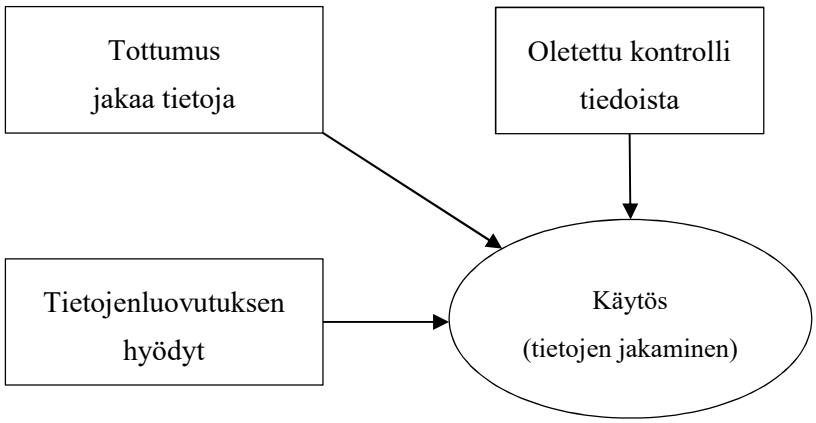


Kuvio 33. Identiteettitarpeiden vaikutukset käytökseen (Wu 2019)

Itsetuntoon ja sosiaalisiin tarpeisiin liittyvät tekijät ovat jääneet vähäiselle huomiolle tutkimuksissa Chenin ym. (2015) ja Wun (2019) malleja lukuun ottamatta. Luvun 3.2 Hallamin ja Zanellan (2017) mallissa käsiteltiin sosiaalista tyydytystä, mutta yksilön kokemien hyötyjen näkökulmasta.

3.7.3 Yksilön irrationaalinen tottumus luovuttaa tietoja

Beldad ja Koehorst (2015) ottivat yksityisyyteen liittyvää käyttäytymistä koskevassa tutkimuksessaan tarkastelun keskipisteeksi yksilöiden tottumukset ja tavat henkilökohtaisten tietojen jaossa. Koska yksityisyyteen liittyvistä päätöksistä on tullut keskeinen osa internetin käyttöä, tutkimuksessa havaittiin tietojen luovutuksesta muodostuneen irrationaalinen ja tiedostamaton käytöstapa yksilöiden keskuudessa. Tutkimuksen yhteydessä havaittiin myös oletetun luovutettujen tietojen kontrollin ja tietojenluovutuksella oletettujen saavutettavien hyötyjen vaikuttavan käytökseen. Artikkelin empiirisessä tutkimuksessa tarkasteltiin myös luottamuksen vaikutusta käytökseen, mutta vaikutus ei ollut merkittävää. (Beldad & Koehorst 2015, 186–199.) Beldadin ja Koehorstin (2015) tutkimuksen tulokset käytökseen vaikuttavista tekijöistä esitetään kuviossa 34.



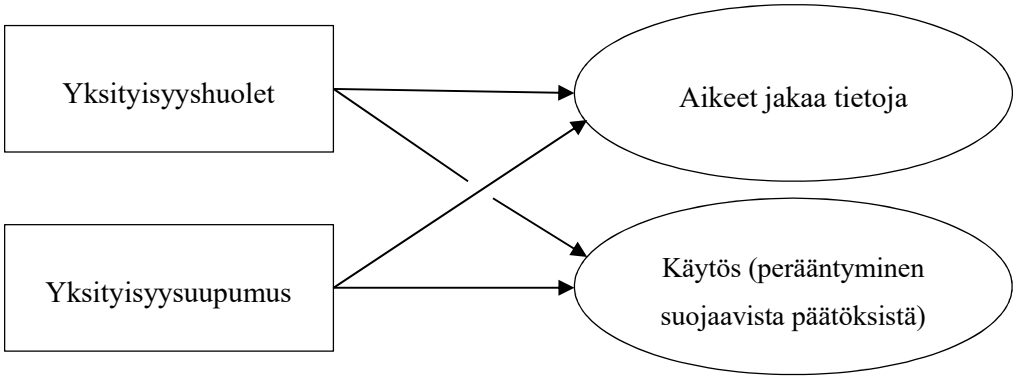
Kuvio 34. Beldadin ja Koehorstin (2015) tutkimuksen mukaiset vaikutukset yksilön käytökseen

Tekijää, joka tarkastelee yksilön tottumuksia jakaa tietoja ei Beldadin ja Koehorstin (2015) mallin lisäksi esiinny muissa tässä tutkielmassa tarkastelluista malleista, mutta oletetun kontrollin vaikutus käytökseen on havaittu useissa malleissa (ks. esim. Hughes-Roberts & Kani-Zahibi 2014; Benson ym. 2015) ja hyötyjen vaikutus esimerkiksi luvussa 3.3 Marwickin ja Hargittain (2019) sekä Keithin ym. (2013) artikkeleissa. Luvussa 3.6.1 Stutzmanin ym. (2011) kuitenkin huomattiin yksityisyyteen liittyvien selosteiden tutustumiseen liittyvien tottumusten vaikutukset käytökseen.

3.7.4 Yksityisyysuupumus

Verkkoon liittyvät yksityisyyden suojan rikkomukset, datankeruuprosessien monimutkaisuus ja verkkoon liittyvä epävarmuus ovat aiheuttaneet yksilöissä yksityisyyden suojaan liittyvää turhautuneisuutta, epävarmuutta ja uupumusta. Ilmiö tunnetaan englannin kielessä termillä ”privacy fatigue”. Suomenkielistä vastinetta termille ei ole, mutta tässä tutkielmassa termiä nimitetään yksityisyysuupumukseksi. Yksityisyysuupumusta kokevat yksilöt ajattelevat yksityisyyden suojaamisen ja tiedonjakoon liittyvien päätösten tekemisen olevan poikkeuksellisen haastavaa. Heille on tyypillistä myös valita helpoin ja yksinkertaisin vaihtoehto vaivan minimoiseksi. Esimerkiksi yksityisyysasetukset jätetään tyypillisesti oletustilaan. Yksityisyysuupumukseen liittyy myös usein yleistä kyynisyyttä ja uupumusta. Yksityisyysuupumuksen on saanut toistaiseksi vähän huomiota tutkimuksissa. Choi ym. (2018) kuitenkin tutkivat yksityisyysuupumuksen ja yksityisyyshuolten

vaikutusta yksilön yksityisyyteen liittyviin aikeisiin ja yksityisyyttä suojaavien toimenpiteiden perääntymiseen liittyvään käytökseen. Heidän tutkimuksensa tulokset on esitetty kuviossa 35. (Choi ym. 2018, 42–44.)



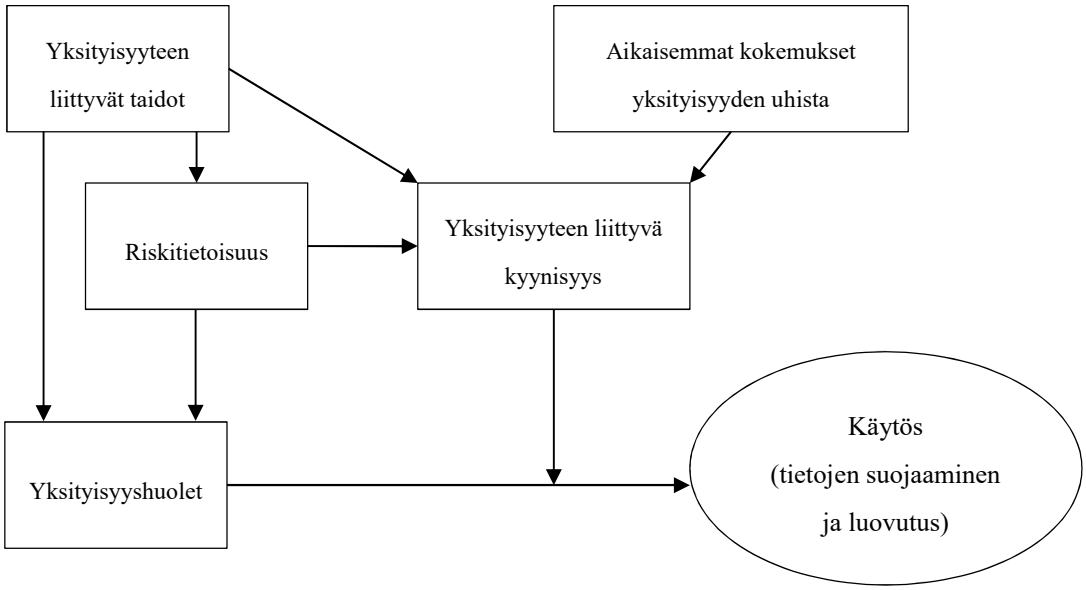
Kuvio 35. Yksityisyysuupumuksen ja yksityisyyshuolten vaikutukset yksilön aikeisiin ja käytökseen (Choi ym. 2018)

Tulosten mukaan sekä yksityisyysuupumus että yksityisyyshuolet vaikuttavat yksilön aikeisiin ja käytökseen. Mitä enemmän yksilöllä oli huolia, sitä varovaisemmin tietoja luovutettiin ja sitä epätodennäköisemmin peräännyttiin yksityisyyttä suojaavista päätöksistä. Yksityisyysuupuneilla puolestaan yksityisyyttä suojaavista toimenpiteistä peräännyttiin helpommin ja aikeet tietojen jakamiseen olivat suuremmat. Tulosten mukaan yksityisyysuupumus vaikuttaa aikeisiin huomattavasti enemmän ja herkemmin kuin yksityisyyshuolet. (Choi ym. 2018, 43–49.) Yksityisyyshuoliin liittyvät tulokset ovat samankaltaisia esimerkiksi luvun 3.1 Joinsonin ym. (2006) sekä luvun 3.2 Dincellin ja Goelin (2017) mallien kanssa, mutta yksityisyysuupumuksen vaikutuksia ei tarkasteltu muissa tässä tutkielmassa esitellyissä tutkimuksissa kuin Choin ym. (2018) tutkimuksessa.

3.7.5 Kyynisyys

Yksilöille on tyypillistä muodostaa kyynisiä asenteita yksityisyyden suojaan liittyen kohdatessaan ylivoimaisia uhkia ja riskejä verkossa. Yksityisyyteen liittyvä kyynisyys määritellään lyhyesti voimattomuuden, epävarmuuden ja luottamuksen puutteen tunteiksi ja asenteiksi verkossa tapahtuvaa henkilökohtaisten tietoja käsittelyä kohtaan. Yksityisyyteen liittyvän kyynisyyden takia verkon käyttäjät päätyvät käyttäytymään yksityisyyttä laiminlyövästi ja kokevat yksityisyyttä suojaavat toimenpiteet hyödyttömiksi. Kyyni-

syyttä voi kehittyä muun muassa epävarmuudesta tai rajoittuneista kyvyistä verkkoon liittyen. Hoffmannin ym. (2016) kehittelemän viitekehyksen mukaan (kuvio 36) yksityisyyteen liittyvään kyynisyyteen vaikuttavat aikaisemmat kokemukset yksityisyyteen liittyvistä uhista, yksityisyyden suojaamiseen liittyvät taidot ja riskitietoisuus. Suoraan käytökseen vaikuttavana tekijänä tunnistettiin ainoastaan kuitenkin yksityisyyshuolet. Yksityisyyteen liittyvä kyynisyys vaikuttaa ainoastaan välillisesti käyttäytymiseen yksityisyyshuolia moderoiden, eli kyynisyys heikentää yksityisyyshuolten vaikutusta käyttäytymiseen. Yksityisyyteen liittyvien taitojen havaittiin vaikuttavan yksilön kyynisyyteen, riskitietoisuuteen ja yksityisyyshuoliin, joka puolestaan vaikutti myös yksityisyyshuoliin. (Hoffman ym. 2016.) Vaikka mallissa ei tutkittu useiden tekijöiden vaikutuksia käytökseen ollenkaan, on Hoffmanin ym. (2016) havainto yksityisyyshuolten vaikutuksesta käytökseen yhtenäinen esimerkiksi Joinsonin ym. (2006) ja Weinbergerin ym. (2017) kanssa, mutta ristiriidassa esimerkiksi Keithin ym. (2013) sekä Hallamin ja Zanellan (2017) kanssa.



Kuvio 36. Yksityisyyteen liittyvä kyynisyys (Hoffmann ym. 2016)

3.7.6 Rationaalinen fatalismi

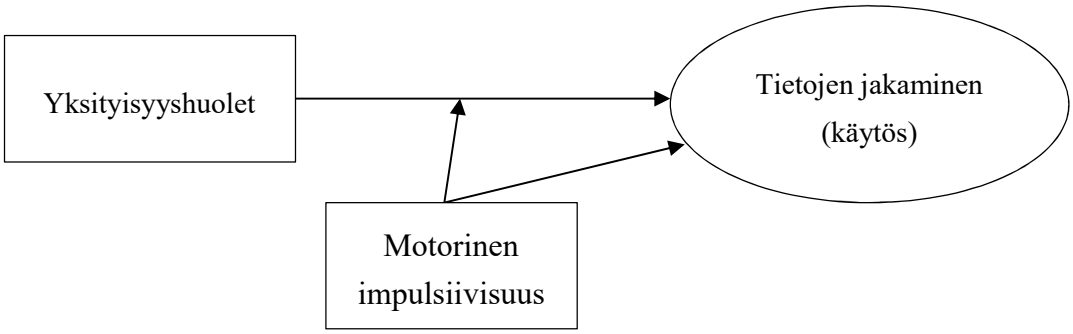
Xie ym. (2019) hyödynsivät tutkimuksessaan rationaalisen fatalismin teoriaa yksityisyyden paradoksin tutkimiseksi. Rationaalisen fatalismin teorian mukaan yksilöt ottavat enemmän riskejä, mikäli he kokevat vaikutusmahdollisuuksien puutetta jonkin tilanteen

lopputulemaan. Toisin sanoen rationaalinen fatalisti ajattelee lopputuloksen tapahtuvan omasta toiminnastaan huolimatta, joten riskien ottamisella, kuten esimerkiksi tietojen luovuttamisella, ei ole mitään vaikutuksia lopputulokseen. Tulosten mukaan mitä enemmän yksilöt ajattelevat kokevansa rationaalisen fatalismin teorian mukaista kontrollin puutetta, sitä vähemmän yksilöt käyttäytyvät yksityisyyttä suojaavasti. (Xie ym. 2019, 742–746, 751–756.) Rationaalinen fatalismi on esimerkki yksilön oletetun kontrollin vähäisyydestä johtuvasta seurauksesta. Yksilön olettaman kontrollin vaikutuksen käytökseen havaitsivat muun muassa luvussa 3.2 Hughes-Robertsin ja Kani-Zahibin (2014), luvussa 3.7.3 Beldadin ja Koehorstin (2015) sekä luvussa 3.5 Bensonin ym. (2015) käsitellyt tutkimukset.

3.7.7 Yksilön impulsiivisuus

Viimeisenä aikaisempana tutkimuksena ja mallina tarkastellaan tässä tutkielmassa Aivazpourin ja Raon (2020) yksilön impulsiivisuuteen perustuvaa tutkimusta. Heidän mukaansa ihmisen motorinen impulsiivisuus vaikuttaa yksilön tietojen luovutukseen (käytökseen) sekä yksityisyyshuolten ja tietojenluovutuksen väliseen vuorovaikutukseen. Motorisella impulsiivisuudella tarkoitetaan ihmisen tarvetta toimia spontaanisti ilman toiminnan ja sen seurausten ajattelua. Tutkimuksessa tutkittiin myös huomioon liittyvän impulsiivisuuden (vaikeus keskittyä tilanteisiin) ja suunnittelemattomuuden impulsiivisuuden (vaikeus tehdä suunnitelmia) yhteyttä käytökseen, mutta vaikutuksia ei havaittu. (Aivazpour & Rao 2020, 14–15, 18, 24–30.)

Aivazpourin ja Raon (2020) tutkimuksen tulokset on esitetty kuviossa 37. Yksityisyyshuolet vähentävät yksilöiden tietojen jakamista ja motorinen impulsiivisuus lisää tietojen jakamista. Motorinen impulsiivisuus myös vaikuttaa yksityisyyshuolten ja käytöksen väliseen suhteeseen; mitä impulsiivisempi yksilö on, sitä pienempi on yksityisyyshuolten vaikutus käytökseen. (Aivazpour & Rao 2020, 14–15, 18, 24–30.)



Kuvio 37. Motorisen impulsiivisuuden vaikutus käytökseen (Aivazpour & Rao 2020)

Tutkimuksensa yhteydessä Aivazpour ja Rao (2020, 14–15) jakoivat yksityisyyden paradoksia selittävät teoriat karkeasti neljään luokkaan: kognitiiviset vinoumat ja heuristiikat (irrationaalinen toiminta), privacy calculus (kustannus-hyötyanalyysit), sosiaaliset teoriat (yksilön tarve jakaa tietoja sosiaalisen yhteenkuuluvuuden saavuttamiseksi) sekä rajoittunut rationaalisuus ja epätäydellinen informaatio (rajallinen määrä tietoa saatavilla). Aivazpour ja Rao (2020) ehdottavat tutkimuksensa perusteella yksilöllisten tekijöiden vaikutusta viidenneksi luokaksi selityksiin edeltäviin luokkiin. Tässä pääluvussakin esitellyistä tutkimuksista useat, erityisesti yksityisyyspersoonallisuuteen liittyviä tekijöitä tarkastelleet tutkimukset (ks. esim. Karwatzki ym. 2017; Marwick & Hargittai 2019) tukevat ajatusta yksilöllisten tekijöiden vaikutuksista paradoksiin.

4 JOHTOPÄÄTÖKSET

Tässä pääluvussa esitetään johtopäätökset tutkielmassa tarkastellun ja hyödynnetyn aiemman tieteellisen kirjallisuudessa esiintyneiden asioiden perusteella. Teoreettisen ja tulkitsevan käsiteanalyyttisen otteen avulla tässä tutkielmassa tarkasteltiin päätutkimusongelmana sitä, miksi yksilöiden aikeet ja käyttäytyminen eroavat toisistaan yksityisyyden suhteen. Alatutkimuskysymyksinä hyödynnettiin kahta seuraavaa kysymystä:

- Mitä yksityisyydellä tarkoitetaan ja miten yksityisyyden käsitteen merkitys on muuttunut?
- Minkälaiset tekijät vaikuttavat yksilöiden aikeisiin ja käyttäytymiseen henkilökohtaisten tietojen luovutuksessa?

Seuraavaksi tarkastellaan vastauksia tutkimuskysymyksiin ja -ongelmiin. Tämän jälkeen tarkastellaan tutkielmaan liittyviä rajoitteita ja annetaan ehdotuksia tulevaisuudessa tapahtuvalle tutkimukselle. Johtopäätösluvun lopussa tarkastellaan tutkielman merkitystä teoriaan ja käytäntöön.

4.1 Yksityisyyden käsite ja sen kehitys

Ensimmäisenä alatutkimuskysymyksenä tarkasteltiin sitä, mitä yksityisyydellä tarkoitetaan ja miten käsitteen merkitys on muuttunut. Modernin yksityisyyden käsitteen juuret ovat vuodessa 1890, jolloin Warren ja Brandeis (1890) korostivat sitä, miten yksityisyyden tulee taata yksilölle oikeus olla rauhassa. Yksityisyys tunnistettiin ensimmäistä kertaa laajempana yksilön oikeutena, eikä se rajoittunut enää pelkästään yksilön fyysiseen koskemattomuuteen tai omaisuuden turvaan. Yksilöiden älykkyyden, tietämyksen ja yksityisyyselämän tulee olla suojassa ulkopuolisilta. Yksityisyyttä alettiin tunnistamaan lainsäädännöllisenä oikeutena, joka huomioi myös yksilön aineettomia ominaisuuksia, kuten yksityiselämän turvaa. Seuraava merkittävä kulmakivi yksityisyyden kehityksessä oli vuoden 1948 Yhdistyneiden kansakuntien yleismaailmallinen ihmisoikeusjulistus, jossa yksityisyys laajeni yksilön lainsäädännöllisestä oikeudesta universaaliksi, kaikille kuuluvaksi oikeudeksi (United Nations 2020).

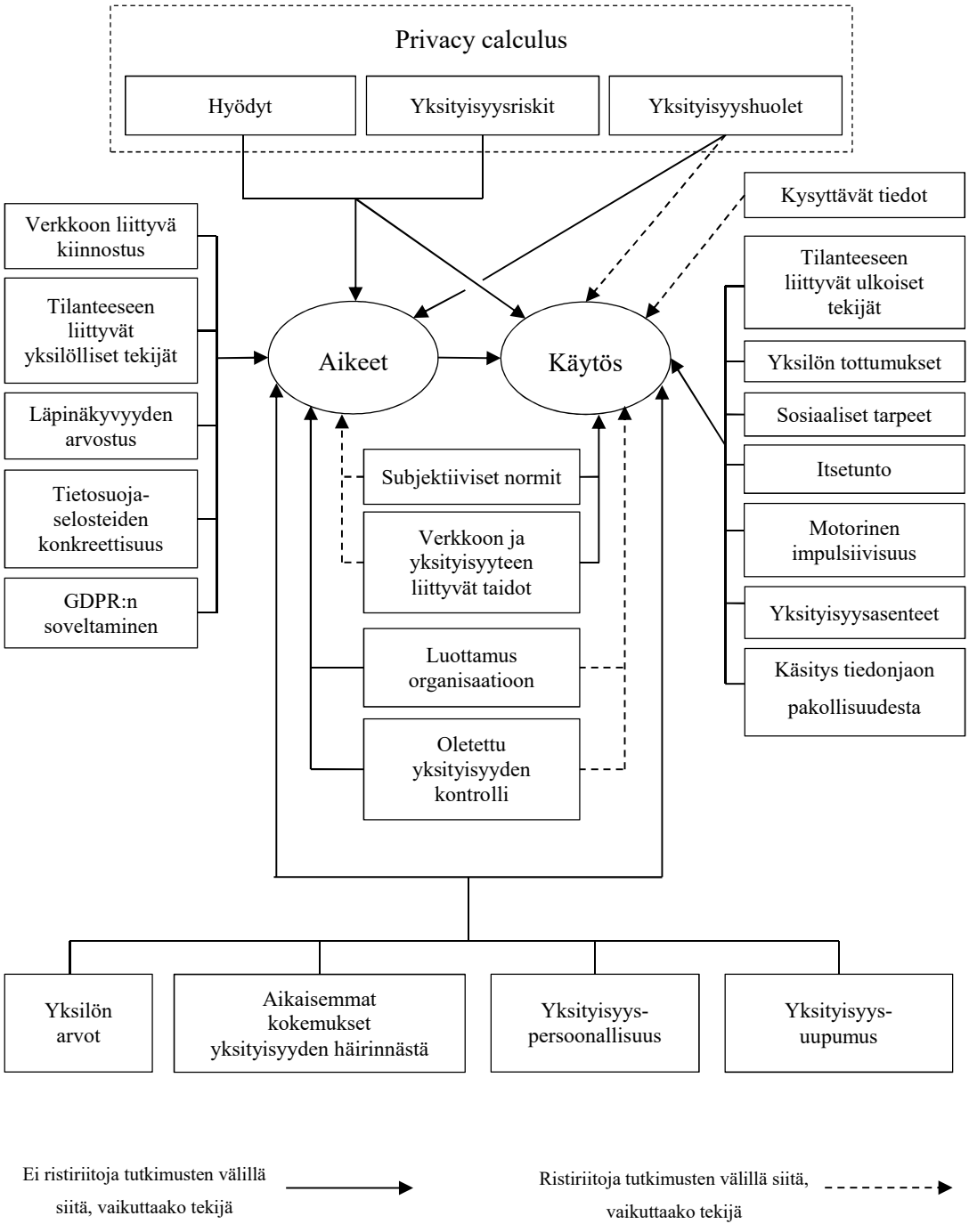
Yksityisyyden kehitys ei kuitenkaan lakannut ihmisoikeusjulistukseen, vaan kehitys on nopeutunut entisestään. Gavison (1980) määritteli täydellisen yksityisyyden käytännön olosuhteissa mahdottomaksi tilaksi ja tiedosti sen, miten yksityisyydellä on arvoa yksilöille. Clarke (1999) ja Westin (2003) määrittelivät yksityisyyden yksilön halukkuu-

deksi paitsi kontrolloida ulkopuolisten tietämystä yksilöön liittyen, mutta myös haluk-kuudeksi ylläpitää omaa henkilökohtaista tilaa. Clarke (1999) mainitsi myös tietojen yk-sityisyyden käsitteen (engl. ”information privacy”), josta on sittemmin muovautunut ny-kyajan hallitsevin yksityisyyskäsite. Tietojen yksityisyydellä viitataan lähtökohtaisesti yksilön henkilökohtaisten tietojen kontrollin ylläpitämiseen ja tietojen leviämisen estä-miseen. Tietojen yksityisyyden tarkoituksena on turvata yksilön kommunikoinnin ja hen-kilökohtaisten tietojen yksityisyys. Tietojen yksityisyyden käsitteen ilmaantuminen on liittynyt tiiviisti informaatioteknologian eli IT:n kehitykseen. Mitä pidemmälle IT on ke-hittynyt, sitä tärkeämmäksi yksilön henkilökohtaisten tietojen suojeleminen on koettu. (Smith ym. 2011.) Esimerkiksi Bélanger ja Crossler (2011) sekä Conger ym. (2013) ko-rostavat sitä, miten tiedot voivat päätyä helposti ulkopuolisten käyttöön tai saataville. Ny-kyaikana yksityisyyttä toteutetaan muun muassa yksilön tuottaman digitaalisen datan suojelemisena (Conger ym. 2013). Vaikka tietojen yksityisyydestä on tullut hallitsevin näkökulma, varsinkin tietojärjestelmätieteessä, yksityisyys on nykytietoon perustuen mo-niulotteinen käsite. Yksityisyyttä voidaan tarkastella lisäksi esimerkiksi fyysisestä, alu-eellisesta, psykologisesta tai sosiaalisesta näkökulmasta (ks. esim. Trepte ym. 2014; Ko-kolakis 2015). Tietojen yksityisyys on muodostunut modernin tietoyhteiskunnan yhdeksi suurimmaksi ja keskeisimmäksi keskustelunaiheeksi. Viime aikoina yksityisyyden ar-voon liittyvässä keskustelussa on noussut esiin näkemys yksityisyydestä hyödykkeenä: yksityisyyttä voidaan käyttää yksilön ja organisaation välisen vaihdannan välineenä (Wil-son & Valacich 2012). Nykyään onkin yleistä, että yksilöt luovuttavat tietojaan yrityk-sille, viranomaisille ja muille organisaatioille.

4.2 Yksityisyyden paradoksin aikeisiin ja käytökseen vaikuttavat tekijät

Toisen alatutkimuskysymyksen tarkoituksena oli tutkia sitä, minkälaiset tekijät vaikutta-vat yksilöiden aikeisiin ja käyttäytymiseen henkilökohtaisten tietojen luovutuksessa. Kol-mannessa pääluvussa käsiteltyjen tieteellisessä tutkimuksessa ja kirjallisuudessa esiinty-neiden mallien ja teorioiden avulla tarkasteltiin yksilöiden henkilökohtaisten tietojen luo-vuttamiseen ja suojelemiseen liittyviä tekijöitä. Näiden mallien ja teorioiden pohjalta muodostetaan uusi teoreettinen viitekehys yksilön aikeisiin ja käyttäytymiseen vaikutta-vista tekijöistä henkilökohtaisten tietojen luovutuksessa. Vaikuttavia tekijöitä kuvaava ja tätä tutkielmaa varten kehitetty teoreettinen viitekehys esitellään kuviossa 38. Yksityi-

syyden paradoksin yksilön aikeita ja käytöstä selittävä viitekehys ja siihen sisältyvien tekijöiden määritelmät, vaikutukset ja lähdeviitteet ovat esitettynä lisäksi taulukkomuodossa tutkielman liitteessä 1.



Kuvio 38. Viitekehys yksityisyyden paradoksiin yksilön aikeisiin ja käyttäytymiseen vaikuttavista tekijöistä

Viitekehyksen pohjana toimivat privacy calculus -teorian mukaiset yksilön olettamat hyödyt, yksityisyysriskit ja yksityisyyshuolet. Hyödyt voivat olla joko konkreettisia ja rahallisia, kuten hinnanalennuksia, tai abstrakteja ja yksilön omaan kokemukseen sekä mielipiteisiin perustuvia, kuten esimerkiksi kokemus käyttömukavuudesta tai personoitu verkkosisältö (Hui ym. 2007; Li ym. 2010; Keith ym. 2013; Beldad & Koehorst 2015; Hallam & Zanella 2017; Karwatzki ym. 2017; Li ym. 2017; Alashoor ym. 2018; Marwick & Hargittai 2019; Williams ym. 2019a; 2019b; Wang ym. 2020). Hyötyjen lisäksi yksityisyysriskeihin perustuvat psykologiset kustannukset ovat keskeinen osa yksilöiden päätöksentekoprosesseja (Dinev & Hart 2006; Norberg ym. 2007; Li ym. 2010; Keith ym. 2013; Alashoor ym. 2018; Booth & Ho 2019; Marwick & Hargittai 2019). Yksityisyyshuolet ovat lähellä yksityisyysriskin käsitettä, mutta lukuisissa tutkimuksissa yksityisyyshuolia tarkasteltiin yksityisyysriskeistä eroavana käsitteenä ja usein myös osana privacy calculus -teoriaan perustuvia malleja (ks esim. Dinev & Hart 2006; Keith ym. 2013; Alashoor ym. 2018; Wang ym. 2020). Hyödyt ja yksityisyysriskit vaikuttavat sekä yksilöiden aikeisiin että käytökseen. Hyödyt lisäävät yksilöiden aikeita luovuttaa tietoja ja lisäävät tietoja luovuttavaa käytöstä. Yksityisyysriskit puolestaan vähentävät yksilöiden aikeita ja käytöstä luovuttaa tietoja sekä lisäävät tietoja suojaavia aikeita ja käytöstä. Yksityisyyshuolet puolestaan vaikuttavat aikeisiin (Dinev & Hart 2006; Zorotheos & Kafeza 2009; Keith ym. 2013; Dincelli & Goel 2017; Hallam & Zanella 2017; Li ym. 2017; Alashoor ym. 2018; Choi ym. 2018; Wang ym. 2020), mutta huolten vaikutuksista käytökseen esiintyi eroavia tuloksia. Yksityisyyshuolet vähensivät tietojen luovutukseen liittyvää ja lisäsivät yksityisyyttä suojaavaa käytöstä. Valtaosa tutkimuksista, jotka tarkastelivat yksityisyyshuolten vaikutuksia käytökseen, havaitsivat huolten vaikuttavan käytökseen (Joinson ym. 2006; Hoffman ym. 2016; Weinberger ym. 2017; Choi ym. 2018; Aivazpour & Rao 2020), mutta Hallamin ja Zanellan (2017) sekä Keithin ym. (2013) mukaan huolet eivät vaikuttaneet käytökseen.

Aikaisempien tutkimusten pohjalta löytyi useita pelkästään aikeisiin vaikuttavia tekijöitä. Yksilön verkkoon liittyvä kiinnostus, eli henkilökohtainen halukkuus tai mieltymys käyttää verkkoa, lisäsi yksilön halukkuutta jakaa henkilökohtaisia tietoja (Dinev & Hart 2006; Zorotheos & Kafeza 2009; Li ym. 2017). Viitekehyksen tilanteeseen liittyvillä yksilöllisillä tekijöillä tarkoitetaan yksilöstä riippuvaisia päätöksentekotilanteisiin liittyviä tekijöitä, joita ovat yksilön mieliala ja mahdollinen flow-olotila. Positiivinen mieliala ja flow-tunne lisäsivät yksilön aikeita, kun taas negatiivinen mieliala tai flow-tuntemuksen puute vähensivät yksilön aikomuksia luovuttaa tietoja. (Alashoor ym. 2018; Wang

ym. 2020.) Läpinäkyvyyden arvostuksella tarkoitetaan yksilön organisaation datan keräämiseen, analysoimiseen ja käyttöön liittyvän avoimuuden arvostamista. Mitä enemmän yksilö arvostaa läpinäkyvyyttä, sitä alhaisemmat ovat yksilön aikeet luovuttaa tietoja. (Awad & Krishnan 2006.) Zhang ym. (2019) nostivat esiin tutkimuksessaan sekä tietosuojaselosteiden konkreettisuuden että Euroopan yleisten tietosuojakäytänteiden soveltamisen vaikutukset aikeisiin luovuttaa tietoja. Selosteiden konkreettisuudella tarkoitetaan organisaation tietosuojaselosteiden selkeyttä, yksityiskohtaisuutta ja ymmärrettävyyttä. Mitä konkreettisimpia selosteet olivat, sitä halukkaampia yksilöt olivat jakamaan tietojaan. Myös GDPR:n hyödyntämisellä oli tietoja luovuttavia aikeita lisäävä vaikutus. (Zhang ym. 2019.)

Pelkästään käytökseen vaikuttavia tekijöitä havaittiin useita aikaisempien tutkimusten pohjalta. Yksilöltä kysyttävien tietojen määrällä ja arkaluontoisuudella oli vaikutuksia yksilön käyttäytymiseen. Mitä enemmän tietoja (Hui ym. 2007) ja mitä arkaluontoisempia tietoja (Schrammel ym. 2009; Marwick & Hargittai 2019; Williams 2019a; 2019b) yksilöltä kysyttiin, sitä vähemmän yksilöt luovuttivat henkilökohtaisia tietojaan. Kysyttävien tietojen arkaluontoisuuden vaikutuksista käytökseen kuitenkin esiintyi ristiriitaisia tuloksia Huin ym. (2007) tutkimuksessa. Aikaisempien tutkimusten pohjalta tehtiin havaintoja päätöksentekotilanteeseen liittyvistä ulkoisista, yksilöstä riippumattomista tekijöistä. Tämän tutkielman uudessa viitekehyksessä tilanteesta riippuvaisiin ulkoisiin tekijöihin lukeutuvat yksityisyyden suojaan liittyvien selosteiden ja ilmoitusten olemassaolo ja sisältö (Hui ym. 2007; Benson ym. 2015), päätöksentekotilanne ja konteksti verkossa (Zaiferopoulou ym. 2013), verkkoyhteisön tyyppi (Schrammel ym. 2009) ja käyttöliittymä (Hughes-Roberts & Kani-Zahibi 2014). Esimerkiksi käyttöliittymällä ja yksityisyyteen liittyvillä ilmoituksilla voidaan ohjata yksilöitä helpommin luovuttamaan tietoja. Stutzmanin ym. (2011) havainnot yksilöiden eroavista tavoista tutustua yksityisyyden suojan selosteisiin sekä Beldadin ja Koehorstin (2015) johtopäätökset yksilön tottumuksista luovuttaa tietoja sisällytettiin viitekehykseen yksilöiden tottumuksina. Mallissa sosiaalisilla tarpeilla tarkoitetaan yksilön kokemaa tarvetta suosiolle, kommunikoinnille ja sosiaalisille yhteyksille. Sosiaaliset tarpeet lisäsivät tietojen luovutusta. Itsetunto puolestaan tarkoittaa yksilön tietoisuutta ja tuntemusta itseensä sekä omaan identiteettiinsä liittyen. Heikko itsetunto ja itsetuntoon liittyvät tarpeet lisäsivät tietoja luovuttavaa käytöstä. (Chen ym. 2015; Wu 2019.) Aivazpour ja Rao (2020) havaitsivat motorisen impulsiivisuuden, eli yksilön persoonallisen ominaisuuden ja tarpeen toimia seurauksia ajattele-

matta, vaikuttavan käytökseen. Motorista impulsiivisuutta ei sisällytetty esimerkiksi yksilön tottumuksiin liittyvään tekijään, sillä motorinen impulsiivisuus on enemmän persoonallisuuteen ja luonteeseen liittyvä piirre eikä niinkään opittu tai omaksuttu toimintatapa. Yksityisyysasenteilla tarkoitetaan yksilön suhtautumistapoja ja ajatusmalleja yksityisyyteen liittyvään toimintaan sekä käytökseen liittyvää arviota tai arvostusta. Mitä positiivisimpia asenteita yksilöillä on tietojen luovuttamista kohtaan, sitä helpommin tietoja luovutetaan. (Stutzman ym. 2011; Zaiferopoulou ym. 2013; Hughes-Roberts & Kani-Zahibi 2014; Büchi ym. 2016.) Viimeisenä pelkkään käytökseen vaikuttavana tekijänä mallissa on käsitys tiedonjaon pakollisuudesta, jolla tarkoitetaan yksilön ajatusmallia yksityisyyden suojan ylläpitämiseen liittyvistä vaihtoehtojen vähyydestä tietojen luovutukseen liittyvissä tilanteissa. Yksilöt saattavat kokea, että tiedonjako on tilanteessa välttämätöntä eikä muita vaihtoehtoja ole. (Marwick & Hargittai 2019.)

Aikaisemmin mainitun privacy calculus -teorian lisäksi aikaisemmasta kirjallisuudesta voidaan havaita lukuisia muita tekijöitä, jotka vaikuttavat sekä aikeisiin että käyttäytymiseen. Subjektiivisilla normeilla, joilla tarkoitetaan yksilön omia näkemyksiä ulkopuolisten ja ympäröivien ihmisten odotuksista ja mielipiteistä jotakin toimintaa kohtaan, havaittiin olevan vaikutuksia yksityisyyden paradoksiin liittyviin aikeisiin ja käytökseen. Subjektiivisiin normeihin voidaan lukea myös yksilön kokemat sosiaaliset paineet tai vaikutteet. Wang ym. (2020) havaitsivat yksilön läheisten ystävien tietojen jakamisen vaikuttavan yksilön aikeisiin. Hughes-Robertsin ja Kani-Zahibin (2014) sekä Dincellin ja Goelin (2017) mukaan subjektiiviset normit vaikuttavat yksilön käyttäytymiseen. Dincelli ja Goel (2017) kuitenkaan eivät löytäneet tukea subjektiivisten normien vaikutuksista aikeisiin. Koska verkossa tapahtuva datankeruu ja organisaatioiden yksityisten tietojen käyttö tapahtuu yhä enemmän yksilön huomaamatta tai tietämättä, tarvitsee yksilö ymmärrystä ja tietämystä verkkoon liittyvistä tiedonkeruuprosesseista ja organisaatioiden tavoista hyödyntää tietoa. Verkkoon ja yksityisyyteen liittyviä taitoja on kutsuttu ajoittain myös internetiin liittyväksi lukutaidoksi. Yksilön verkkoon liittyvillä taidoilla on ollut Bensonin ym. (2015) mukaan ollut tietojen luovutusta lisäävä vaikutus, kun taas Büchin ym. (2016) ja Williamsin ym. (2019a; 2019b) yksityisyyden suojaa edistävä käytös lisääntyy parempien taitojen myötä. Weinbergerin ym. (2017) mukaan yksilön parempi tietoisuus verkossa tapahtuvasta seurannasta taas vähensi yksityisyyttä suojaavaa käytöstä. Tutkimukset olivat siis yksimielisiä siitä, että verkkoon ja yksityisyyteen liittyvät taidot vaikuttavat käytökseen, mutta tekijän vaikutuksesta käytökseen esiintyi tutkimusten välillä eroavaisuuksia. Wangin ym. (2020) mukaan parempi ymmärrys vähensi

tietojen luovuttamiseen liittyviä aikeita. Sen sijaan Dincelli ja Goel (2017) eivät löytäneet yhteyttä internetiin liittyvän lukutaidon ja aikeiden välillä.

Ristiriitaisia tuloksia löytyi lisäksi luottamukseen ja oletettuun yksityisyyden kontrolliin liittyen. Luottamuksella tarkoitetaan yksilön käsitystä organisaation luotettavuudesta ja arviota siitä, että organisaatio ei toimi opportunistisesti. Dinevin ja Hartin (2006), Norbergin ym. (2007) sekä Zorotheoksen ja Kafezan (2009) mukaan luottamus vaikuttaa yksilön aikeita lisäävästi, kun taas Joinsonin ym. (2006), Boothin ja Hon (2019) sekä Marwickin ja Hargittain (2019) mukaan luottamus lisää yksilön tietoja luovuttavaa käyttäytymistä. Norberg ym. (2007) sekä Beldad ja Koehorst (2015) eivät löytäneet tukea kuitenkaan luottamuksen vaikutuksista käytökseen. Viimeinen mallin tekijä, jossa havaittiin ristiriitaisia tuloksia, on yksilön olettama yksityisyyteen liittyvä kontrolli. Yksilön yksityisyyteen liittyvällä kontrollilla tarkoitetaan yksilön olettamuksia omasta henkilökohtaisiin tietoihin liittyvästä kontrollista verkossa. Suunnitellun käyttäytymisen teorian mukaisesti käsitteeseen sisältyy myös yksilön uskomukset omiin yksityisyyteen liittyviin kykyihin (Ajzen 2002). Yksilön kontrolli vaikutti sekä aikeisiin (Zorotheos & Kafeza 2009; Li ym. 2017) että käytökseen (Hughes-Roberts & Kani-Zahibi 2014; Beldad & Koehorst 2015; Benson ym. 2015; Weinberger ym. 2017; Booth & Ho 2019; Xie ym. 2019). Ainoastaan Wu (2019) ei löytänyt tukea oletetun kontrollin vaikutuksista käytökseen. Kontrollin vaikutuksista esiintyi myös pieniä ristiriitaisuuksia: esimerkiksi Bensonin ym. 2015 mukaan mitä korkeammaksi omiin tietoihin liittyvä kontrolli koettiin, sitä vähemmän pääsääntöisesti tietoja luovutettiin, mutta esimerkiksi Zorotheoksen ja Kafezan (2009) mukaan koettu kontrolli lisäsi tietojen luovutusta.

Viitekehykseen on sisällytetty yksilön arvoihin liittyvä aikeisiin ja käytökseen vaikuttava tekijä Dincellin ja Goelin (2017) sekä Zaiferopouloun ym. (2013) tutkimuksiin perustuen: esimerkiksi kulttuurillisiin arvoihin ja piirteisiin perustuen yksilöt saattavat arvostaa omien tietojen kontrollia eri tavoin. Yksilön omat henkilökohtaiset kokemukset yksityisyyden suojaan kohdistuneesta häirinnästä tai rikkomuksista vähensivät yksilöiden aikeita (Awad & Krishnan 2006) ja käytöstä (Büchi ym. 2016) tietojen luovutukseen liittyen. Mallin yksityisyyspersoonallisuuteen liittyvä tekijä on yksilökohtainen ja persoonallinen piirre, jonka perusteella yksilöissä voidaan havaita eroja yksityisyyteen liittyvissä aikeissa ja käytöksessä. Yksityisyyspersoonallisuudet voidaan esimerkiksi jaotella yksityisyyden suojelijoihin, mukavuudenhaluisiin ja tietojen myyjiin (Hann ym. 2007) tai fundamentaalisesti, pragmaattisesti ja huolettomasti suhtautuviin yksilöihin (Lee ym. 2011). Erityisesti niin sanotun ”nothing to hide” -ajattelutavan ja persoonallisuuden on

huomattu yleistyneen viime aikoina. Tämän ajattelutavan mukaisesti ajattelevat yksilöt kokevat yksityisyyden suojan menettäneen merkityksensä, eikä heillä ole oman ajatusmaailmansa perusteella salassa pidettäviä tietoja. (Adorjan & Ricciardelli 2019.) Viimeinen mallin vaikuttava tekijä on nimeltään yksityisyysuupumus. Choi ym. (2018) tunnistivat tutkimuksessaan yksityisyysuupumuksen lisäävän yksilön aikeita jakaa tietoja ja taipumusta perääntyä tietoja suojaavista toimenpiteistä. Yksityisyysuupumus ilmenee esimerkiksi päätöksenteon ylivoimaisuutena ja mahdollisimman vaivattoman ratkaisun valitsemisena. Yksityisyysuupumus sisällytettiin siten viitekehyksessä aikeisiin ja käytökseen vaikuttavana tekijänä.

Yksityisyyden paradoksiin liittyvä tutkimus on ollut monipuolista, mutta selkeästi privacy calculus -teorian ja suunnitellun käyttäytymisen teorian pohjautuviin sovelluksiin painottunutta. Privacy calculus -teorian ajatukset muodostivat keskeisen osan tässäkin tutkielmassa kehitetystä viitekehyksestä. Myös suunnitellun käyttäytymisen teoriassa alun perin esiintyneiden tekijöiden sovelluksia, kuten subjektiiviset normit, yksilön yksityisyyteen liittyvät asenteet ja yksilön olettama kontrolli omasta yksityisyydestään ovat kaikki tässäkin viitekehyksessä esiintyviä tekijöitä. Alkuperäisessä suunnitellun käyttäytymisen teoriassa asenteet ja subjektiiviset normit vaikuttivat ainoastaan aikeisiin ja oletettu kontrolli sekä aikeisiin että käytökseen. Kuitenkin toisin kuin alkuperäisessä suunnitellun käyttäytymisen teoriassa, yksityisyyteen liittyvässä tutkimuksessa havaittiin pääosin, että asenteet vaikuttivat ainoastaan käytökseen ja subjektiiviset normit sekä oletettu kontrolli aikeisiin ja käytökseen.

Vaikka aikeisiin ja käytökseen löytyy lukusia yhteisiä vaikuttavia tekijöitä, merkittävää viitekehyksessä on havainto muun muassa siitä, kuinka suuri joukko tekijöitä vaikuttaa ainoastaan aikeisiin, tai vaihtoehtoisesti ainoastaan käyttäytymiseen. Tilanteeseen liittyvien tekijöiden osalta merkittävä huomio on myös se, että tilanteeseen liittyvät yksilölliset tekijät (yksilön mieliala ja flow-tila) vaikuttivat aikeisiin ja tilanteeseen liittyvät ulkoiset tekijät (käyttöliittymä, päätöksentekotilanne, konteksti, yksityisyyteen liittyvät ilmoitukset ja selosteet sekä verkkoyhteisön tyyppi) vaikuttivat käyttäytymiseen. Tämä viitekehys osoittaa myös selkeästi, miten yksityisyyden paradoksiin liittyy suuri määrä yksilöön liittyviä persoonallisia ja yksilöllisiä tekijöitä, kuten esimerkiksi yksityisyyspersoonallisuus, itsetunto, sosiaaliset tarpeet, arvot, aikaisemmat kokemukset yksityisyyden häirinnästä, yksilön kokema yksityisyysuupumus, motorinen impulsiivisuus ja verkkoon liittyvä kiinnostus.

Päätutkimusongelmaan vastaten voidaan aikaisemman tutkimuksen ja tässä tutkielmassa kehitetyn viitekehyksen pohjalta sanoa, että yksityisyyden paradoksi on seurausta vaikuttaviin tekijöihin liittyvistä eroavaisuuksista. Vaikuttavat tekijät myös selittävät eroja yksilön aikeiden ja käytöksen välillä. Toisin sanoen, yksilön aikeita ja käytöstä muodostavat yhdistävien tekijöiden lisäksi joukko eroavia tekijöitä. Koska paradoksin taustalla vaikuttavissa tekijöissä on taustalla päätöksentekotilanteisiin liittyviä ulkoisia ja yksilöllisiä tekijöitä sekä hyvin yksilökohtaisia ja persoonallisuudenpirteisiin liittyviä tekijöitä, on jokainen päätöksentekotilanne ja päätöksentekijä myös erilainen. Esimerkiksi rationaalinen privacy calculus -teorian mukainen kustannus-hyötyanalyysi muodostaa vain pienen osan vaikuttavista tekijöistä. Tämän lisäksi, hyötyihin, riskeihin ja huoliin liittyvät arviot ovat usein yksilöstä riippuvaisia. Aikeiden ja käyttäytymisen ennustaminen on haastavaa ja erittäin monimutkaista.

Tarkasteltaessa yksityisyyden paradoksin taustalla vaikuttavia tekijöitä, on aiheellista epäillä sitä, onko paradoksia edes mahdollista ratkaista. Vaikuttavien tekijöiden verkostot vaikuttavat monimutkaisilta ja laajoilta. Koska paradoksiin liittyviin aikeisiin ja käyttäytymiseen vaikuttaa suuri määrä ihmiseen liittyviä yksilöllisiä tekijöitä, kuten persoonallisuuteen, arvoihin ja itsetuntoon liittyvät asiat, sekä joukko ympäristöön ja päätöksentekotilanteisiin liittyviä tekijöitä, kuten flow-tila ja päätöksenteon konteksti, tuntuu paradoksin aikeiden ja käyttäytymisen ennustaminen ja kuilun sulkeminen erittäin haastavalta tehtävältä. Jokainen päätöksentekotilanne on lähtökohtaisesti hieman erilainen, yksilöiden omat sidosryhmäverkostot eroavat muiden yksilöiden vastaavista ja ihmisen yksilöllisten ominaisuuksien määräytymiseen usein vaikuttavat myös yksilön perimätieto ja ympäristön vaikutukset. Yksilö ei myöskään käyttäydy täysin rationaalisesti, eikä saatavilla ole täydellistä informaatiota. Tiedostettuun ja rationaaliseenkin toimintaan voi liittyä rajoittavia tekijöitä. Yksilöt pyrkivät säästämään aikaa tai he saattavat toimia kiireen painostamina. Yksityisyyden paradoksin aikeiden ja käyttäytymisen ennustamisessa ja kuilun kaventamisessa voidaan mahdollisesti saavuttaa parempia tuloksia, mutta paradoksin ratkaiseminen on asia erikseen. Yksityisyyden paradoksi voi myös muuttua odottamattomaan suuntaan ympäröivää yksityisyyden ja teknologian kehitystä mukaillen. On hyvin mahdollista, että yksityisyyden paradoksista on muodostunut kiinteä osa yksilöiden toimintaa, jolle ei ole löydettävissä selkeää ja yksiselitteistä ratkaisua.

4.3 Tutkielman rajoitteet ja aiheita jatkotutkimukselle

On olennaista myös tarkastella ja tiedostaa tähän tutkielmaan liittyviä rajoitteita. Esimerkiksi yhtenä selkeänä rajoitteena artikkelien valinnassa oli tieteellisten artikkelien kieli; kielimuuri on artikkelien valintaa rajoittava tekijä. Yksityisyyden paradoksin parempaa mallinnusta ja selittämistä silmällä pitäen esimerkiksi pitkän ja lyhyen aikavälin aikeet ja käytös tarkasteltiin ilman erottelua pitkään ja lyhyeen aikaväliin. Myös käytöstä tarkasteltiin näkökulmasta, joka sisälsi sekä yksityisyyden suojaa edistävän käytöksen että tietojen luovutukseen liittyvän käytöksen. Samoin aikeissa huomioitiin yksityisyyttä suojaava ja sitä heikentävä käytös. Viitekehyksessä yleisempien tasojen käsitteiden hyödyntäminen, vaikuttavien tekijöiden välisten suhteiden ja välillisten vaikutuksien pois jättäminen pelkistävät ilmiötä jonkin verran, mutta tämä oli välttämätöntä tutkielman rajaamiseksi ja mittakaavan hallitsemiseksi. Myös hyödynnettävien sähköisten tietokantojen valinta rajaa hyödynnettävää aineistoa. Uusia tutkimuksia julkaistaan myös jatkuvasti lisää, joten johtopäätökset rajoittuvat tätä ajankohtaa ennemmin tehtyyn tieteelliseen tutkimukseen. Esimerkiksi GDPR:n ollessa suhteellisen uusi muutos, ollaan GDPR:n soveltamisen vaikutuksia tutkittu vain aikeisiin. Viitekehys voi siten antaa osittain rajoittuneen kuvan yksittäisistä tekijöistä. Koska yksityisyyden paradoksi on monimutkainen ja laaja ilmiö, joudutaan viitekehyksessä ryhmittelemään ja tiivistämään asioita. Tämä voi antaa osittain pelkistetymmän kuvan yksityisyyden paradoksista. Kuitenkin tämän tutkielman tarkoituksena oli laatia viitekehys yksityisyyden paradoksin yksilön aikeisiin ja käytökseen vaikuttavista tekijöistä, eikä vaikuttavien tekijöiden välisistä suhteista tai niiden taustatekijöistä. Rajoitteistaan huolimatta, tämän tutkielman ja kehitetyn viitekehyksen avulla on voitu tehdä keskeisiä havaintoja ja synteesiä yksityisyyden paradoksiin liittyvästä tutkimuksesta ja ilmiöstä yleisemmin.

Yksityisyyden paradoksiin liittyvä tutkimus on keskittynyt paljon privacy calculus -malliin ja suunnitellun käyttäytymisen teoriaan. Molempiin teorioihin liittyvien tekijöiden vaikutukset ovat suhteellisen hyvin tunnettuja, joten tiedeyhteisö voisi hyötyä myös vaihtoehtoisten mallien ja teorioiden etsimisestä tai testaamisesta. Erityisesti yksilön rationaaliseen päätöksentekoon liittyvät piirteet, kuten kustannus-hyötyanalyysit, ovat jo saaneet osakseen merkittävää huomiota ja ovat tiedeyhteisössä yleisesti tunnistettuja. Yksityisyyden paradoksiin liittyvä tutkimus hyötyisi myös ehdottomasti vakiintuneempien käsitemääritelmien laatimisesta. Esimerkiksi yksityisyyden paradoksiin liittyvissä tutki-

muksissa usein aikeiden ja käytöksen määritelmät voivat olla häilyviä, mutta myös esimerkiksi yksityisyysasenteiden, -huolten ja -riskien määritelmät vaikuttavat ajoittain vaihtelevilta. Yksityisyyden paradoksi on jo itsessään monimutkainen ilmiö, joten vaihtelevien ja keskenään läheisten käsitemääritelmien näkökulmasta tiukempi rajanveto määritelmille voisi olla eduksi.

Erityisesti yksilöön liittyvien ominaisuuksien, luonteenpiirteiden ja persoonallisuuksiin liittyvien tekijöiden tutkiminen voisi tuottaa uusia tieteellisiä havaintoja ja näkökulmia, sillä nämä ovat olleet toistaiseksi suhteellisen vähäisellä huomiolla. Myös esimerkiksi alkuperäiseen suunnitellun käyttäytymisen teoriaan liittyvät taustatekijät olivat jätetty pois yksityisyyteen liittyvissä tutkimuksissa. Kuten viitekehyksestä voidaan kuitenkin nähdä, vaikuttaa paradoksin taustalla paljon yksilöllisiä tekijöitä. Myös ympäristöllä, ympäröivillä ihmisillä ja organisaatioilla voi olla lukuisissa tilanteissa vaikutuksia yksilön tekemiin päätöksiin myös yksityisyyteen liittyvissä asioissa. Näitäkään vaikutuksia ei tule aliarvioida tai unohtaa. Esimerkiksi päätöksentekotilanteisiin liittyvien ympäristöön liittyvien tekijöiden ja ärsykkeiden vaikutusta voi olla mielekästä tutkia myös lisää. Yksityisyysuupumukseen, tietojen luovutukseen liittyvän pakollisuuden sekä yksilöiden ajan ja vaivan säästämiseen liittyvät näkökulmat ovat myös saaneet osakseen poikkeuksellisen vähän tutkimusta.

4.4 Tutkielman merkitys teoriaan ja käytäntöön

Tämän tutkielman tieteellisenä kontribuutiona on yksityisyyden paradoksiin liittyvä uudenlainen teoreettinen viitekehys yksilön aikeiden ja käyttäytymisen vaikuttavien tekijöiden tarkasteluun. Aikaisempi tutkimus on ollut monimuotoista ja paradoksin taustalla vaikuttavia tekijöitä yhteen kokoava viitekehys selkeyttää ilmiön syvällisempää ymmärtämistä ja hahmottamista. Viitekehyksen pohjalta voidaan esimerkiksi tutkia tarkemmin tieteellisessä tutkimuksessa esiintyneitä ristiriitoja tekijöiden vaikutuksista tai mallia voidaan hyödyntää aikaisemman tutkimuksen laajentamisessa uusille aihealueille tai uusien tekijöiden vaikutuksen tarkasteluun. Lisäksi esimerkiksi viitekehyksen tekijöiden keskinäisten vaikutussuhteiden tarkastelu voi paljastaa ilmiöstä uusia havaintoja. Tutkielmassa annetut tulevaisuuden tutkimukseen liittyvät suositukset ja näkökulmat ovat myös arvokasta tietoa tieteelliselle yhteisölle.

Viitekehyksen avulla voidaan myös haluttaessa kasvattaa yksilöiden, organisaatioiden ja yhteiskunnan ymmärrystä yksilön toiminnasta ja päätöksentekoprosessien taustalla

vaikuttavista tekijöistä. Yksityisyyden paradoksi esiintyy käytännön elämässä ja se koskettaa kaikkia yhteiskunnan yksilöitä, organisaatioita ja muita toimijoita. Hyvä esimerkki viitekehykseen liittyvien tietojen hyödyntämisestä voi olla esimerkiksi yrityksen suorittama segmentointi yksilön yksityisyyspersoonallisuuksien perusteella resurssien tehokkaammaksi kohdistamiseksi. Yksityisyyttään varjelevia ja tiedonjakoon yleisesti haluttomien yksilöiden suostutteluun käytetyt resurssit voitaisiin hyödyntää yksilöihin, jotka luovuttavat tietojaan mielellään ja arvostavat esimerkiksi personointia. Rajalliset resurssit pystyttäisiin mahdollisesti käyttämään siis tehokkaamminkin. Yksilöiden mahdollisuus luovuttaa tai olla luovuttamatta tietoja on hyvä ja nykyaikainen esimerkki kuluttajan neuvotteluvoimasta markkinoilla. Koska yksilöiltä saatavasta datasta on tullut kriittinen menestystekijä ja resurssi organisaatioille, on yrityksen näkökulmasta olennaista ymmärtää, mitkä asiat vaikuttavat yksilöiden päätöksentekoprosesseihin aikeita muodostettaessa ja käytökseen ryhtyessä. Tämän takia tässäkin tutkielmassa kehitetyssä viitekehyksessä esiintyvien tekijöiden tiedostaminen on keskeistä. Verkossa toimivat organisaatiot voivat myös osaltaan kannustaa yksilöitä tietojen luovutukseen ymmärtämällä potentiaalisten käyttäjiensä ja asiakkaidensa aikeisiin ja käytökseen vaikuttavia tekijöitä.

5 YHTEENVETO

Teknologisen kehityksen, internetin laajenemisen ja big datan myötä yksityisyydestä on tullut yhä ajankohtaisempi ilmiö. Vaikka yksityisyys liittyy ennen kaikkea yksilöön, yksityisyyden suojaan liittyvä lainsäädäntö luo velvoitteita organisaatioille. Yksilöä koskevien henkilökohtaisten tietojen keräämisestä on tullut keskeinen osa organisaatioiden toimintaa ja yksilöiden päivittäistä elämää. Yksityisyyden ajankohtaisuuden ja kehityksen pohjalta tämän tutkielman tarkoituksena oli tarkastella yksityisyyden paradoksin yksilön aikeisiin ja käytökseen vaikuttavia tekijöitä. Tässä tutkielmassa luotiin katsaus yksityisyyden käsitteeseen ja sen kehitykseen, dataan, organisaatioiden tietojen keruuseen ja käyttöön, yksityisyyden paradoksin monimutkaisiin taustatekijöihin ja malleihin. Tutkielma toteutettiin teoreettisena, soveltaen tulkitsevaa käsiteanalyyttistä tutkimusmetodia.

Yksityisyys on kehittynyt ennen kaikkea fyysisestä koskemattomuudesta ja omaisuuden turvasta kohti yksilön oikeutta kontrolloida ja vaikuttaa omien henkilökohtaisten tietojensa saatavuuteen ja käyttöön. Usein yksilön henkilökohtaisiin tietoihin liittyvää yksityisyyden suojaa nimitetään tietojen yksityisyydeksi. Yksityisyys on tämän lisäksi huomioitu lainsäädännössä ja yleismaailmallisessa ihmisoikeusjulistuksessa ihmisen oikeutena. Yksityisyyden kehitys on seurannut läheisesti informaatioteknologian kehitystä.

Tietojen yksityisyyden käsitteen ilmaantumiseen johtanut kehitys ja internetin laajeneminen ovat edesauttaneet uuden ristiriitaisen ilmiön, tietojen yksityisyyden paradoksin, tunnistamista. Yksityisyyden paradoksissa on kyse yksilön yksityisyyden suojaan liittyvien aikeiden ja käytöksen ristiriitaisuudesta. Yksilöt ovat haluttomia luovuttamaan henkilökohtaisia tietojaan organisaatioiden käyttöön ja halukkaita suojelemaan yksityisyyttään, mutta todellinen käytös on usein yksityisyyden suojaa heikentävää. Henkilökohtaisia tietoja luovutetaan organisaatioille yhä enemmän ja helpommin. Yksilön käyttäytymistä voidaan edelleen tarkastella rationaalisen ja irrationaalisen käyttäytymisen yhdistelmänä. Yleinen esimerkki yksilön rationaalisesta käyttäytymisestä on privacy calculus -teorian mukainen kustannus-hyötyanalyysi, kun taas irrationaaliseen käyttäytymiseen liittyy heuristisia piirteitä ja kognitiivisia vinoumia, eli taipumuksia painottaa toimintaa ja tehdä päätöksiä epäjohdonmukaisesti. Yksityisyyden paradoksiin liittyen yksilöillä on yleensä virheellisiä käsityksiä tai odotuksia yksityisyyden suojasta ja organisaation datankeruusta. Privacy calculus -teorian lisäksi muun muassa suunnitellun käyttäytymisen

teoriaa on yritetty usein hyödyntää yksilön käyttäytymisen ennustamisessa, mutta vaihtelevin tuloksin.

Organisaatioilla on myös lukuisia ja uudenlaisia mahdollisuuksia kerätä dataa yksilöistä huomaamattomasti. Yksilöstä kerätystä datasta voidaan edelleen jalostaa ymmärrettävissä olevaa informaatiota ja tietämystä päätöksenteon tueksi. Datan määrä ja monimuotoisuus ovat olleet huomattavassa kasvussa ja datan elinkaaresta on tullut pitkäkestoisempi. Organisaatiot voivat hyödyntää keräämiään tietoja yksilöistä esimerkiksi personointiin ja innovointiin. Myös datan luvaton käyttö on mahdollista ja yhä yleisempää. Yksilöön liittyvät tiedot voivat vaihdella tunnistettavuudeltaan. Anonyymit tiedot eivät paljasta yksilön henkilöllisyyttä, mutta voivat antaa hyödyllistä tietoja nimettömien profiilien luomiseen. Tunnistamattomat tiedot puolestaan mahdollistavat jo hieman tarkemman yksilöiden profiloinnin, muttei kuitenkaan yksilön identifiointia. Tunnistettavat tiedot paljastavat yksilön henkilöllisyyden ja ovat usein enemmän tai vähemmän arkaluontoisia ja hyvinkin yksityiskohtaisia tietoja.

Yksityisyyden paradoksin yksilön aikeisiin ja käytökseen vaikuttavia tekijöitä tarkasteltiin aikaisemman tieteellisen kirjallisuuden ja tutkimuksen valossa. Tutkielman johtopäätöksenä löydettiin suuri joukko paradoksin taustalla olevia vaikuttavia tekijöitä. Privacy calculus -teoria muodostaa tärkeän ja laajasti tutkitun osa-alueen paradoksista. Kustannus-hyötyanalyysiin havaittiin kuuluvan yksilön kokemat hyödyt, yksityisyysriskit ja yksityisyyshuolet. Privacy calculus -teoriaan liittyvillä tekijöillä on vaikutuksia sekä aikeisiin että käytökseen. Muita aikeisiin ja käytökseen vaikuttavia tekijöitä olivat yksilön verkkoon ja yksityisyyteen liittyvät taidot, luottamus organisaatioon, käsitys subjektiivisista normeista, oletettu yksityisyyteen liittyvä kontrolli, aikaisemmat kokemukset, arvot, yksityisyyteen liittyvä uupumus ja yksityisyyspersoonallisuus.

Pelkästään aikeisiin vaikuttavia tekijöitä olivat yksilön verkkoon liittyvä kiinnostus, tilanteeseen liittyvät yksilölliset tekijät, läpinäkyvyyden arvostus, tietosuojaselosteiden konkreettisuus ja GDPR:n mukaisten käytänteiden soveltaminen. Pelkkään käytökseen puolestaan vaikuttivat yksilöltä kysyttävien tietojen määrä ja arkaluontoisuus, tilanteeseen liittyvät ulkoiset tekijät, ihmisen motorinen impulsiivisuus, itsetunto, tottumukset ja sosiaaliset tarpeet, yksityisyysasenteet ja käsitys tiedonjaon pakollisuudesta.

Tulevaisuudessa tutkimus voisi siirtää painopistettä enemmän suunnitellun käyttäytymisen malleista ja privacy calculus -teoriasta kohti yksilöllisten ja ympäristöön liittyvien ominaisuuksien sekä taustatekijöiden tarkastelua. Yksityisyyspersoonallisuudet, yk-

sityisyysuupumus ja tietojen jakoon liittyvä pakollisuus ovat toistaiseksi varsin vähän tutkittuja aihealueita. Alan tutkimus hyötyisi myös selkeämpien ja yhtenäisempien käsitemääritelmien muodostamisesta. Tämän tutkielman pääasiallisia rajoitteita ovat muun muassa artikkelien valintaa rajaava kielimuuri, aikeiden ja käytöksen tarkastelussa hyödynnetty näkökulma, joka sisälsi sekä pitkän että lyhyen aikavälin tarkastelun ja lisäksi yksityisyyttä suojaavan ja tietoja luovuttavan toiminnan tarkastelun. Vaikuttavien tekijöiden väliset suhteet ja välilliset sekä epäsuorat vaikutukset jäivät viitekehyksen ulkopuolelle, joka rajoittaa viitekehyksen laajuutta. Näkökulma ja viitekehyksen rakentaminen saattavat osittain pelkistää ilmiötä ja siihen liittyviä tekijöitä.

Yksityisyyden suojaan ja mittavaan datankeruuseen liittyvät kehityssuunnat ovat olleet huolestuttavia. Datankeräämistä suoritetaan yhä huomaamattomammin ja yksilöstä on älykkäiden laitteiden yleistyessä saatavilla tarkempaa ja arkaluontoisempaa tietoa kuin koskaan aikaisemmin. Organisaatioiden on myös helppoa houkutella käyttäjät luovuttamaan henkilökohtaisia tietojaan, sillä personoidun mainonnan tai tuotteen saaminen ja palveluiden tai laitteiden käyttäminen edellyttävät usein käyttöehtojen hyväksymistä ja omien henkilökohtaisten tietojen luovutusta. Ainoa vaihtoehto yksityisyyden varjelemiseksi voi olla päätös olla käyttämättä palvelua. Tämä voi kuitenkin olla yksilölle epäsuotuisa vaihtoehto esimerkiksi subjektiivisiin normeihin liittyvän ryhmäpaineen nojalla. Datan määrän ja yksityiskohtaisuuden kasvaessa tulee organisaatioille myös lisähaasteita tietosuojasta huolehtimiseen ja siten yksilön yksityisyyden suojan takaamiseen. Suurista tietomurroista, datan luvattomasta käytöstä ja myymisestä on tullut yhä yleisempää. Ylipäänsä yksilön henkilökohtaisiin tietoihin ja yksityisyyden suojaan liittyvät näkökulmat ovat kiistanalaisia. Vaikka yksityisyydellä on arvoa, paitsi aineetonta ja abstraktia arvoa yksilöille itselleen ja taloudellista arvoa organisaatioilla, on eettisestä ja moraalisesta näkökulmasta kyseenalaista asettaa ihmisille kuuluvalle ihmisoikeudelle hintalappu tai käyttää sitä vaihdon välineenä. Yksilön tiedoista on kuitenkin tullut ehkä pysyvästi kriittinen resurssi organisaatioille.

Yksityisyyteen liittyvät päätöksentekotilanteet ovat yhä arkipäiväisempiä ja päätöksiä on tapana tehdä yhä nopeammin ja vähemmän harkitusti. Digitalisaation ja teknologian kehityksen myötä on myös herännyt ajatus siitä, onko mahdollista ylipäänsä saavuttaa minkäänlaista yksityisyyttä tai onko yksityisyys viimeistään tulevaisuudessa menettänyt merkityksensä ja asemansa. Kuten tässäkin tutkielmassa huomattiin, on yhä yleisempää suhtautua yksityisyyteen välinpitämättömästi tai huolimattomasti. Yksilöt kokevat usein, ettei heillä ole mitään menetettävää tietojensa luovuttamisessa ja yksityisyyden

suojan menettämisestä on tullut hyväksyttävä ja jopa välttämätön osa elämää tietointensiivisessä ja digitaalisessa yhteiskunnassa. Yksityisyyteen liittyvän tietoisuuden ja taitojen lisäämisellä oli useiden tutkimusten mukaan hyötyä aikeiden ja käytöksen välisen kuilun kaventamiseksi, yksityisyyttä suojaavan käytöksen edistämiseksi tai yksityisyyttä heikentävän käytöksen vähentämiseksi. Yksityisyyteen ja datankeruuseen liittyvä ymmärrys voisi olla hyödyllistä myös yleisemmästä näkökulmasta tarkasteltuna; parempi tietoisuus johtaa lisääntyneeseen keskusteluun yhteiskunnassa ja tämä puolestaan voi johtaa yksityisyyden suojaan liittyvän lainsäädännön tai käytäntöjen kehittymiseen.

On myös tiedostettava, että ilman yksityisyyden käsitteen kehitystä ei olisi tietojen yksityisyyttä, joka on puolestaan edesauttanut paradoksin tunnistamista ja tutkimista. Myös internet ja muu teknologia ovat muovanneet yksityisyyttä ja paradoksin ilmaantumista. Onkin odotettavaa, että tulevaisuuden kehitys yksityisyyden käsitteessä ja informaatioteknologiassa tulevat osaltaan vaikuttamaan myös yksityisyyden paradoksiin. Teknologian kehitys on johtanut yhteiskuntaa suuntaan, jossa yksilöistä on mahdollista kerätä dataa melkein missä, milloin ja miten tahansa. Yksityisyyspersoonallisuuksiin liittyvä kehitys on huolestuttavaa, sillä yksityisyyteen suhtaudutaan yhä enenevissä määrin välinpitämättömästi ja huolettomasti, esimerkkeinä toimivat niin sanottu uusi ”nothing to hide”-ajattelumalli tai yksityisyyden suhteen huolettomat yksilöt. Tietojen luovuttaminen on usein enemmän tai vähemmän yksilön näkökulmasta riippuen pakollista.

Tämän tutkielman kontribuutiona toimii uudenlainen aikaisemman tutkimuksen ja kirjallisuuden pohjalta kehitetty viitekehys, jossa esiteltiin yksilön henkilökohtaisten tietojen jakoon liittyviin aikeisiin ja käytökseen vaikuttavia tekijöitä. Viitekehys lisää yksityisyyden paradoksiin liittyvää ymmärrystä ja edesauttaa ilmiön hahmottamista ja jäsentelyä. Viitekehys korostaa ennen kaikkea sitä, miten monimutkainen ja laaja ilmiö yksityisyyden paradoksi on. Vaikka aikeisiin ja käytökseen vaikutti joukko yhteneviä tekijöitä, vaikuttaa ilmiön taustalla myös useita joko pelkästään aikeisiin tai käytökseen liittyviä tekijöitä. Yksilön aikeisiin ja käytökseen vaikuttaa suuri määrä ympäristöön ja henkilökohtaisiin ominaisuuksiin liittyviä tekijöitä. Aikeisiin ja käytökseen vaikuttavien tekijöiden eroista johtuen ja yksilöön sekä ympäristöön liittyvien tekijöiden vaikutuksista aikeiden ja käyttäytymisen ennustaminen on haastavaa. Paradoksiin liittyvästä aikeiden ja käytöksen välisestä ristiriidasta on tullut keskeinen osa yksilöiden elämää. Yksityisyyden käsitteen ja merkityksen kehitys voi vaikuttaa keskeisesti tulevaisuudessa yksityisyyden paradoksiin liittyvään kehitykseen. Ilman tietojen yksityisyyden moniulotteisuutta,

ajankohtaisuutta ja informaatioteknologian kehitystä yksityisyyden paradoksi tuskin olisi yhtä monimutkainen ilmiö.

LÄHTEET

Acquisti, A. (2004) Privacy in Electronic Commerce and the Economics of Immediate Gratification. *EC '04: Proceedings of the 5th ACM conference on Electronic commerce*, 21–29.

Adorjan, M. – Ricciardelli, R. (2019) A New Privacy Paradox? Youth Agentic Practices of Privacy Management Despite "Nothing to Hide" Online. *Canadian Review of Sociology*, Vol. 56 (1), 8–29.

Aguirre, E. – Mahr, D. – Grewal, D. – Ruyter, K. D. – Wetzels, M. (2015) Unraveling the Personalization Paradox: The Effect of Information Collection and Trust-Building Strategies on Online Advertisement Effectiveness. *Journal of Retailing*, Vol. 91 (1), 34–49.

Aivazpour, Z. – Rao, V. S. (C.) (2020) Information Disclosure and Privacy Paradox: The Role of Impulsivity. *Data Base for Advances in Information Systems*, Vol. 51 (1), 14–36.

Ajzen, I. (2002) Perceived Behavioral Control, Self-Efficacy, Locus of Control, and the Theory of Planned Behavior. *Journal of Applied Social Psychology*, Vol. 34 (4), 665–683.

Al Maskari, A. (2018) Theory of Planned Behavior (TPB) Ajzen (1988). *Technology Adoption and Social Issues*, 46-67.

Alashoor, T. – Al-Maidani, N. – Al-Jabri, I. (2018) The Privacy Calculus under Positive and Negative Mood States. *Thirty Ninth International Conference on Information Systems, San Francisco 2018*, 1–17.

Ansari, A. – Mela, C. F. (2003) E-customization. *Journal of Marketing Research*, Vol. 40 (2), 131–145.

Arass, M. E. – Tikito, I. – Souissi, N. (2017) Data lifecycles analysis: towards intelligent cycle. *2017 Intelligent Systems and Computer Vision (ISCV)*.

Awad, N. F. – Krishnan, M. S. (2006) The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. *MIS Quarterly*, Vol. 30 (1), 13–28.

Baek, Y. M. (2014) Solving the privacy paradox: A counter-argument experimental approach. *Computers in Human Behaviour*, Vol. 38, 33–42.

Barnes, S. B. (2006) A privacy paradox: Social networking in the United States. *First Monday*, Vol. 11 (9).

Barth, S. – de Jong, M. D.T. (2017) The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review. *Telematics and Informatics*, Vol. 34, 1038–1058.

Beldad, A. D. – Koehorst, R. (2015) It's Not About the Risks, I'm just Used to Doing It: Disclosure of Personal Information on Facebook Among Adolescent Dutch Users. Teoksessa: *Social Computing and Social Media 7th International Conference 2015 Proceedings*, toim. Gabriele Meiselwitz, 185–195. Springer International Publishing.

Bélanger, F. – Crossler, R. E. (2011) Privacy in the Digital Age: A Review of Information Privacy Research In Information Systems. *MIS Quarterly*, Vol. 35 (4), 1017–1041.

Benson, V. – Saridakis, G. – Tennakoon, H. (2015) Information disclosure of social media users. Does control over personal information, user awareness and security notices matter? *Information Technology & People*, Vol. 28 (3), 426–441.

Booth, C. – Ho, S. H. (2019) The Privacy Paradox in HCI: Calculus Behavior in Disclosing PII Online. Teoksessa: *HCI in Business, Government and Organizations. Information Systems and Analytics. HCII 2019. Lecture Notes in Computer Science*, Vol. 11589, toim. Fiona Fui-Hoon Nah – Keng Siau, 163–177. Springer International Publishing.

Braganza, A. (2004) Rethinking the data–information–knowledge hierarchy: towards a case-based model. *International Journal of Information Management*, Vol. 24, 347–356.

Bratman, B. (2002) Brandeis and Warren's the Right to Privacy and the Birth of the Right to Privacy. *Tennessee Law Review*, Vol. 69, 623–651.

Brown, B. (2001) Studying the Internet Experience. *HP Laboratories Technical Report*, (49), 1–23.

Büchi, M. – Just, N. – Latzer, M. (2016) Caring is not enough: the importance of Internet skills for online privacy protection. *Information, Communication & Society*, 1261–1278.

Caruana, A. (2002) Service loyalty: The effects of service quality and the mediating role of customer satisfaction. *European Journal of Marketing*, Vol. 36 (7-8), 811–828.

Chellappa, R. K. – Sin, R. G. (2005) Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma. *Information Technology and Management*, Vol. 6 (2-3), 181–202.

Chen, J. V. – Widjaja, A. E. – Yen, D. C. (2015) Need for Affiliation, Need for Popularity, Self- Esteem, and the Moderating Effect of Big Five Personality Traits Affecting Individuals' Self- Disclosure on Facebook. *International Journal of Human-Computer Interaction*, Vol. 31, 815–831.

Cho, H. – Fiorito, S. S. (2009) Acceptance of online customization for apparel shopping. *International Journal of Retail & Distribution Management*, Vol. 37 (5), 389–407.

Choi, H. – Park, J. – Jung, Y. (2018) The role of privacy fatigue in online privacy behavior. *Computers in Human Behavior*, Vol. 81, 42–51.

Christiansen, L. (2011) Personal privacy and Internet marketing: An impossible conflict or a marriage made in heaven? *Business Horizons*, Vol. 54 (6), 509–514.

Clarke, R. (1999) Internet Privacy Concerns Confirm the Case for Intervention. *Communications of the ACM*, Vol. 42 (2), 60–67.

Clemons, E. K. – Hitt, L. M. (2004) Poaching and the Misappropriation of Information: Transaction Risks of Information Exchange. *Journal of Management Information Systems*, Vol. 21 (2), 87–107.

Conger, S. – Pratt, J. H. – Loch, K. D. (2013) Personal information privacy and emerging technologies. *Information Systems Journal*, Vol. 23 (5), 401–417.

Cooper, P. (2016) Data, information, knowledge and wisdom. *Anaesthesia & Intensive Care Medicine*, Vol.18 (1), 55-56.

Crié, D. – Micheaux, A. (2006) From customer data to value: What is lacking in the information chain? *Database Marketing & Customer Strategy Management*, Vol. 13 (4), 282–299.

Deborah, J. T. – Hogg, M. A. – White, K. M. (1999) The theory of planned behaviour: Self-identity, social identity and group norms. *British Journal of Social Psychology*, Vol. 38 (3), 225–244.

Desouza, K. C. – Awazu, Y. (2005) What Do They Know? *Business Strategy Review*, Vol. 16 (1), 41–45.

Dienlin, T. – Trepte, S. (2015) Is the privacy paradox a relic of the past? An in-depth analysis of privacy attitudes and privacy behaviors. *European Journal of Social Psychology*, Vol. 45 (3), 285–297.

Dincelli, E. – Goel, S. (2017) Can Privacy and Security Be Friends? A Cultural Framework to Differentiate Security and Privacy Behaviors on Online Social Networks.

Proceedings of the 50th Hawaii International Conference on System Sciences, 4011–4020.

Dinev, T. – Hart, P. (2006) An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, Vol. 17 (1), 61–80.

Dinev, T. – Xu, H. – Smith, H. J. (2009) Information Privacy Values, Beliefs and Attitudes: An Empirical Analysis of Web 2.0 Privacy. *Proceedings of the 42nd Hawaii International Conference on System Sciences*, 1–10.

Dobias, J. (2010) Privacy Effects of Web Bugs Amplified by Web 2.0. Teoksessa: *Privacy and Identity Management for Life*, toim. Simone Fischer-Hübner – Penny Duquenoy – Marit Hansen – Ronald Leenes – Ge Zhang, 244–257. Springer, Berlin, Heidelberg.

European Commission 2018, Questions and Answers – General Data Protection Regulation <<https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_387>>, haettu 15.4.2020

European Commission 2020, What is personal data? <<https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en>>, haettu 22.3.2020.

Erevelles, S. – Fukawa, N. – Swayne, L. (2016) Big Data consumer analytics and the transformation of marketing. *Journal of Business Research*, 897–904.

Fan, H. – Poole, M. S. (2006) What Is Personalization? Perspectives on the Design and Implementation of Personalization in Information Systems. *Journal of Organizational Computing and Electronic Commerce*, Vol. 16 (3-4), 179–202.

Fatima, R. – Yasin, A. – Liu, L. – Wang, J. – Afzal, W. – Yasin, A. (2019) Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, Vol. 48, 1–16.

Gavison, R. (1980) Privacy and the Limits of Law. *The Yale Law Journal*, Vol. 89 (3), 421–471.

Gerber, N. – Gerber, P. – Volkamer, M. (2018) Explaining the privacy paradox: A systematic review of literature investigating privacy attitude and behaviour. *Computers & security*, Vol. 77, 226–261.

Hallam, C. – Zanella, G. (2017) Online self-disclosure: The privacy paradox explained as a temporally discounted balance between concerns and rewards. *Computers in Human Behavior*, Vol. 68, 217–227.

Hann, I.-H. – Hui, K.-L. – Lee, S.-Y. T. – Png, I. P.L. (2007) Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. *Journal of Management Information Systems*, Vol. 24 (2), 13–42.

Ho, S. Y. – Bodoff, D. (2014) The Effects of Web Personalization on User Attitude and Behavior: An Integration of the Elaboration Likelihood Model and Consumer Search Theory. *MIS Quarterly*, Vol. 38 (2), 497–520.

Hoffmann, C. P. – Lutz, C. – Ranzini, G. (2016) Privacy cynicism: A new approach to the privacy paradox. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, Vol. 10 (4).

Hughes-Roberts. T. – Kani-Zabihi, E. (2014) On-Line Privacy Behavior: Using User Interfaces for Salient Factors. *Journal of Computer and Communications*, Vol. 2 (4), 220–231.

Hui, K.-L. – Teo, H. H. – Lee, S.-Y. T. (2007) The Value of Privacy Assurance: An Exploratory Field Experiment. *MIS Quarterly*, Vol. 31 (1), 19–33.

Hussain, T. – Asghar, Dr. S. – Masood, Dr. N. (2010) Web Usage Mining: A Survey on Preprocessing of Web Log File. *2010 International Conference on Information and Emerging Technologies*.

Igo, S. E. (2018) Me and My Data. *Historical Studies in the Natural Sciences*, Vol. 48 (5), 616–626.

Jayachandran, S. – Hewett, K. – Kaufman, P. (2004) Customer Response Capability in a Sense-and-Respond Era: The Role of Customer Knowledge Process. *Journal of the Academy of Marketing Science*, Vol. 32 (3), 219–233.

Joinson, A. N. – Paine, C. – Reips, U.-D. – Buchanan T. (2006) Privacy and Trust: the role of situational and dispositional variables in online disclosure. *Workshop on Privacy in the Electronic Society 2006*.

Karwatzki, S. – Dytynko, O. – Trenz, M. – Veit, D. (2017) Beyond the Personalization–Privacy Paradox: Privacy Valuation, Transparency Features, and Service Personalization. *Journal of Management Information Systems*, Vol. 34 (2), 369–400.

Kehr, F. – Kowatch, T. – Wentzel, D. – Fleisch, E. (2015) Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal*, Vol. 25 (6), 607–635.

Keith, M. J. – Thompson, S. C. – Hale, J. – Lowry, P. B. – Greer, C. (2013) Information disclosure on mobile devices: Re-examining privacy calculus with actual user behaviour. *International Journal of Human-Computer Studies*, Vol. 71 (12), 1163–1173.

Kim, S. H. (2015) Carrie James: Disconnected: Youth, New Media, and the Ethics Gap. *Journal of Youth and Adolescence*, Vol. 44, 1168–1170.

Kokolakis, S. (2015) Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. *Computers & Security*, Vol. 64, 122–134.

Koppa.jyu.fi, käsiteanalyysi <<https://koppa.jyu.fi/avoimet/kirjasto/kirjastotuutori/aihehaku-tutkimusprosessissa/kasiteanalyysi>>, haettu 2.4.2020.

Koskinen, J. – Knaappi-Junnila, S. – Rantanen, M. M. (2019) What if we had fair, people-centred data economy ecosystems? *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation*, 329–334.

Laufer, R. S. – Wolfe, M. (1977) Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory. *Journal of Social Issues*, Vol. 33 (3), 22–42.

Lee, D.-J. – Ahn, J.-H. – Bang, Y. (2011) Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection. *MIS Quarterly*, Vol. 35 (2), 423–444.

Lee, M. K. O. – Cheung, C. M. K. – Lim, K. H. – Ling Sia, C. (2006) Understanding customer knowledge sharing in web-based discussion boards. An exploratory study. *Internet Research*, Vol. 16 (3), 289–303.

Lesser, E. – Mundel, D. – Wiecha, C. (2000) Managing Customer Knowledge. *Journal of Business Strategy*, Vol. 21 (6), 34–37.

Li, H. – Sarathy, R. – Xu, H. (2010) Understanding Situational Online Information Disclosure as a Privacy Calculus. *Journal of Computer Information Systems*, Vol. 51 (1), 62–71.

Li, H. – Luo, X. R. – Zhang, J. – Xu, H. (2017) Resolving the privacy paradox: Toward a cognitive appraisal and emotion approach to online privacy behaviors. *Information & Management*, Vol. 54, 1012–1022.

Li, T. – Unger, T. (2012) Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems*, Vol. 21, 621–642.

Liang, T.-P., – Chen, H.-Y. – Du, T. – Turban, E. – Li, Yuwen (2012) Effect of personalization on the perceived usefulness of online customer services: a dual-core theory. *Journal of Electronic Commerce Research*, Vol. 13 (4), 275–288.

Liew, A. (2007) Understanding Data, Information, Knowledge and Their Inter-Relationships. *Journal of Knowledge Management Practice*, Vol. 8 (2).

Liu, J. – Li, J. – Li, W. – Wu, J. (2016) Rethinking big data: A review on the data quality and usage issues. *ISPRS Journal of Photogrammetry and Remote Sensing*, 134–142.

Liu, Z. – Bonazzi, R. – Shan, J. – Pigneur, Y. (2014) Privacy as a Tradeoff: Introducing the Notion of Privacy Calculus for Context-Aware Mobile Applications. *2014 47th Hawaii International Conference on System Sciences*, 1063–1072.

Lutz, C. – Strathoff, P. (2011) Privacy Concerns and Online Behavior – Not so Paradoxical After All? Viewing the Privacy Paradox through different theoretical lenses. <<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2425132>>, haettu 28.4.2020.

Lämsä, A.-M. – Takala, T. (2004) Tulkitseva käsitetutkimus <<https://metodix.fi/2014/05/19/lamsa-tulkitseva-kasitetutkimus/>>, haettu 31.3.2020.

Malhotra, N. K. – Kim, S. S. – Agarwal, J. (2004) Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, Vol. 15 (4), 336–355.

Malgieri, G. – Custers, B. (2018) Pricing privacy – the right to know the value of your personal data. *Computer Law & Security Review*, Vol. 34, 289–303.

Matney, S. – Brewster, P. J. – Sward, K. A. – Cloyes, K. G. – Staggers, N. (2011) Philosophical Approaches to the Nursing Informatics Data-Information-Knowledge-Wisdom Framework. *Advances in Nursing Science*, 6–18.

Marwick, A. – Hargittai, E. (2019) Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society*, Vol. 22 (12), 1697–1713.

Mavlanova, T. – Benbunan-Fich, R. – Koufaris, M. (2012) Signaling theory and information asymmetry in online commerce. *Information & Management*, Vol. 49, 240–247.

Michota, A. – Katsikas, S. (2015) Designing a Seamless Privacy Policy for Social Networks. *PCI '15: Proceedings of the 19th Panhellenic Conference on Informatics*, 139–143.

Narayanan, A. – Shmatikov, V. (2010) Myths and fallacies of “Personally Identifiable Information”. *Communications of the ACM*, Vol. 53 (6), 24–26.

Norberg, P. – Horne, D. R. – Horne, D. A. (2007) The Privacy Paradox: Personal Information Disclosure Intentions versus Behaviors. *The Journal of Consumer Affairs*, Vol. 41 (1), 100–126.

Pötzsch, S. (2009) Privacy Awareness: A Means to Solve the Privacy Paradox? Teoksessa: *The Future of Identity in the Information Society. Privacy and Identity 2008. IFIP Advances in Information and Communication Technology*, Vol. 298, toim. Vashek Matyáš – Simone Fischer-Hübner – Daniel Cvrček, 226–236. Springer, Berlin, Heidelberg.

Rantanen, M. M. (2019) Towards Ethical Guidelines for Fair Data Economy – Thematic Analysis of Values of Europeans. *Third Annual Seminar on Technology Ethics, At Turku, Finland*, 27–38.

Raynes-Goldie, K. (2010) Aliases, creeping, and wall cleaning: Understanding privacy in the age of Facebook. *First Monday*, Vol. 15 (1).

Schrammel, J. – Köffel, C. – Tscheligi, M. (2009) How Much do You Tell? Information Disclosure Behaviour in Different Types of Online Communities. *C&T '09: Proceedings of the fourth international conference on Communities and technologies*, 275–284.

Schomakers, E.-M. – Lidynia, C. – Ziefle, M. (2019) A Typology of Online Privacy Personalities. Exploring and Segmenting Users’ Diverse Privacy Attitudes and Behaviors. *Journal of Grid Computing*, Vol. 17 (4), 727–747.

Schwartz, P. M. – Solove, D. J. (2011) The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *New York University Law Review*, Vol. 86, 1814–1894.

Smith, H. J. – Dinev, T. – Xu, H. (2011) Information Privacy Research: An Interdisciplinary Review. *MIS Quarterly*, Vol. 35 (4), 989–1015.

Spiekermann, S. – Grossklags, J. – Berendt, B. (2001) E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus actual Behavior. *EC '01: Proceedings of the 3rd ACM conference on Electronic Commerce*, 38–47.

Stanton, J. – Nemati, H. – Chun, S. – Chen, J. (2007) Privacy in the YouTube Era: Evolving Concepts in the Protection of Personal Information. *Association for Information Systems - 13th Americas Conference on Information Systems, AMCIS 2007: Reaching New Heights, AMCIS 2007 Proceedings*, 1–6.

Stutzman, F. – Capra, R. – Thompson, J. (2011) Factors mediating disclosure in social network sites. *Computers in Human Behavior*, Vol. 27, 590–598.

Sunikka, A. – Bragge, J. (2012) Applying text-mining to personalization and customization research literature – Who, what and where? *Expert Systems with Applications*, Vol. 39, 10049–10058.

Tietosuoja.fi/pseudonymisointi-anonymisointi, Pseudonymisoidut ja anonymisoidut tiedot <<https://tietosuoja.fi/pseudonymisointi-anonymisointi>>, haettu 10.2.2020.

Tietosuoja.fi/tietosuoja, Tietosuoja <<https://tietosuoja.fi/tietosuoja>>, haettu 28.5.2020.

Tilastokeskus 2020, Tutkimus- ja kehittämistoiminta <<https://www.stat.fi/meta/kas/t_ktoiminta.html>>, haettu 23.5.2020.

Trepte, S. – Dienlin, T. – Reinecke, L. (2014) Risky Behaviors – How Online Experiences Influence Privacy Behaviors. <<https://www.researchgate.net/profile/Tobias_Dienlin2/publication/266078957_Risky_behaviors_How_online_experiences_influence_privacy_behaviors/links/546a9c3f0cf20dedafd38af8/Risky-behaviors-How-online-experiences-influence-privacy-behaviors.pdf>>, haettu 3.4.2020.

Tsai, J. Y. – Egelman, S. – Cranor, A. – Acquisti, A. (2011) The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study. *Information Systems Research*, Vol. 22 (2), 254–268.

Tsk.fi, jäljite <<http://www.tsk.fi/tsk/termitalkoot/haku-266.html?page=get_id&id=ID0174&vocabulary_code=TSKTT>>, haettu 19.5.2020.

United Nations 2020, Universal Declaration of Human Rights. <<https://www.un.org/en/universal-declaration-human-rights/>>, haettu 17.5.2020.

Wang, L. – Hu, H.-H. – Yan, J. – Mei, M. Q. (2020) Privacy calculus or heuristic cues? The dual process of privacy decision making on Chinese social media. *Journal of Enterprise Information Management*, Vol. 33 (2), 353–380.

Warren, S. D. – Brandeis, L. D. (1890) The Right to Privacy. *Harvard Law Review*. Vol. 4 (5), 193–220.

Weinberger, M. – Bouhnik, D. – Zhitomirsky-Geffet, M. (2017) Factors Affecting Students' Privacy Paradox and Privacy Protection Behavior. *Open Information Science*, 3–20.

Westin, A. F. (2003) Social and Political Dimensions of Privacy. *Journal of Social Issues*, Vol. 59 (2), 431–453.

Wiedmann, K.-P. – Buxel, H. – Walsh, G. (2001) Customer profiling in e-commerce: Methodological aspects and challenges. *Journal of Database Marketing*, Vol. 9 (2), 170–184.

Williams, M. – Nurse, J. R. C. – Creese, S. (2019a) (Smart)Watch Out! encouraging privacy-protective behavior through interactive games. *International Journal of Human-Computer Studies*, Vol. 132, 121–137.

Williams, M. – Nurse, J. R. C. – Creese, S. (2019b) Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior*, Vol. 99, 38–54.

Wilson, D. W. – Valacich, J. S. (2012) Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. *Thirty Third International Conference on Information Systems*, 1–11.

Wu, D. – Im, I. – Tremaine, M. – Instone, K. – Turoff, M. (2003) A framework for classifying personalization scheme used on e-commerce Websites. System Sciences, 2003. *Proceedings of the 36th Annual Hawaii International Conference on 36th Annual Hawaii International Conference on System Sciences*.

Wu, P. F. (2019) The Privacy Paradox in the Context of Online Social Networking: A Self-Identity Perspective. *Journal of the Association for Information Science and Technology*, Vol. 70 (3), 207–219.

Xie, W. – Fowler-Dawson, A. – Tvauri, A. (2019) Revealing the relationship between rational fatalism and the online privacy paradox. *Behaviour & Information Technology*, Vol. 38 (7), 742–759.

Young, A. L. – Quan-Haase, A. (2013) Privacy protection strategies on Facebook. The Internet privacy paradox revisited. *Information, Communication & Society*, Vol. 16 (4), 479–500.

Zaiferopoulou, A. M. – Millard, D. E. – Webber, C. – Hara, K. O' (2013) Unpicking the Privacy Paradox: Can Structuration Theory Help to Explain Location-Based Privacy Decisions? *WebSci '13: Proceedings of the 5th Annual ACM Web Science Conference*, 463–472.

Zhang, Y. – Wang, T. – Hsu, C. (2019) The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure and trust. *Journal of Intellectual Capital*, Vol. 21 (2), 145–163.

Zillner, S. – Becker, T. – Munné, R. – Hussain, K. – Rusitschka, S. – Lippell, H. – Curry, E. – Ojo, A. (2016) Big Data-Driven Innovation in Industrial Sectors. Teoksessa: *New Horizons for a Data-Driven Economy*, toim. José María Cavanillas – Edward Curry – Wolfgang Wahlster, 169–178. Springer International Publishing.

Zins, C. (2007) Conceptual approaches for defining data, information, and knowledge. *Journal of the Association for Information Science and Technology*, Vol. 58 (4), 479–493.

Zorotheos, A. – Kafeza, E. (2009) Users' perceptions on privacy and their intention to transact online: a study on Greek internet users. *Direct Marketing: An International Journal*, Vol. 3 (2), 139–153.

LIITTEET

Liite 1. Yksityisyyden paradoksin teoreettisen viitekehyksen vaikuttavat tekijät

Taulukossa 2 esitetään taulukkomuodossa tämän tutkielman lopputuloksena syntyneen viitekehyksen yksilöiden aikeisiin ja käytökseen vaikuttavat tekijät. Viitekehys on esitetty kuviona tämän tutkielman luvussa 4.2.

Taulukko 2. Yksityisyyden paradoksin yksilön aikeita ja käytöstä selittävän viitekehyksen vaikuttavat tekijät

Taulukon ensimmäisessä sarakkeessa nimetään viitekehyksessä esiintyvä vaikuttava tekijä. Toisessa sarakkeessa annetaan vaikuttavan tekijän määritelmä. Kolmannessa sarakkeessa kerrotaan, vaikuttaako tekijä aikeisiin, käytökseen vai molempiin. Kolmannessa sarakkeessa **tekstin lihavoinnilla** viitataan kirjallisuudessa esiintyneisiin erimielisyyksiin tekijän vaikutuksesta aikeisiin tai käytökseen. Neljännessä sarakkeessa esitetään vaikuttavan tekijän muodostamiseen ja määrittelyyn hyödynnetyt tieteelliset artikkelit. Mikäli vaikuttavassa tekijässä esiintyi valtaosasta tutkimuksia eroavia tuloksia, on ristiriitaisia tuloksia esittänyt lähdeviite **lihavoitu**.

Yksityisyyden paradoksin yksilön aikeita ja käytöstä selittävät tekijät			
Vaikuttava tekijä	Määritelmä	Vaikuttaa	Lähdeviitteet
Verkkoon liittyvä kiinnostus	Yksilön henkilökohtainen kiinnostus tai mieltymys käyttää internetiä, verkkosivustoa tai sähköistä palvelua.	Aikeet	Dinev & Hart (2006) Zorotheos & Kafeza (2009) Li ym. (2017)
Tilanteeseen liittyvät yksilölliset tekijät	Tilanteeseen ja kontekstiin sidonnaiset yksilöön liittyvät tekijät, kuten mieliala tai flow-tunne päätöksentekotilanteessa.	Aikeet	Alashoor ym. (2018) Wang ym. (2020)
Läpinäkyvyyden arvostus	Yksilön arvostus organisaation avoimuutta ja läpinäkyvyyttä kohtaan liittyen tietojen sekä datan keräämiseen, analysoimiseen ja käyttöön.	Aikeet	Awad & Krishnan (2006)
Tietosuojaselosteiden konkreettisuus	Organisaation tietosuojaselosteisiin liittyvä selkeys, yksityiskohtaisuus ja ymmärrettävyys.	Aikeet	Zhang ym. (2019)
GDPR:n soveltaminen	Euroopan yleisten tietosuojakäytänteiden (GDPR) hyödyntäminen organisaatiossa, joissa soveltaminen ei olisi pakollista.	Aikeet	Zhang ym. (2019)

Yksityisyyden paradoksin yksilön aikeita ja käytöstä selittävät tekijät			
Vaikuttava tekijä	Määritelmä	Vaikuttaa	Lähdeviitteet
Kysyttävät tiedot	Yksilöltä pyydettävien tietojen määrä sekä tietojen arkaluontoisuus ja tarkkuus.	**Käytös**	**Hui ym. (2007)** Schrammel ym. (2009) Marwick & Hargittai (2019) Williams ym. (2019a; 2019b)
Tilanteeseen liittyvät ulkoiset tekijät	Yksilöstä riippumattomat verkon päätöksentekotilanteissa vaikuttavat tekijät. Esimerkiksi käyttöliittymä, verkkoyhteisön tyyppi, yksityisyyden suojan selosteiden olemassaolo ja niiden sisältö sekä päätöksentekotilanteen konteksti.	Käytös	Hui ym. (2007) Schrammel ym. (2009) Zaiferopoulou ym. (2013) Hughes-Roberts & Kani-Zahibi (2014) Benson ym. (2015)
Yksilön tottumukset	Ihmisen yksilölliset tottumukset toimia yksityisyyteen liittyvissä asioissa, kuten yksilön tapa jakaa tietoja tai tutustua yksityisyyden suojaan liittyviin selosteisiin.	Käytös	Stutzman ym. (2011) Beldad & Koehorst (2015)
Sosiaaliset tarpeet	Yksilön kokema tarve suosiolle, kommunikoinnille tai sosiaalisille yhteyksille.	Käytös	Chen ym. (2015) Wu (2019)
Itsetunto	Yksilön tietoisuus ja tuntemus itseensä sekä hänen omaan identiteettiinsä liittyen.	Käytös	Chen ym. (2015) Wu (2019)
Motorinen impulsiivisuus	Yksilön persoonallinen piirre, johon liittyy tarve ja taipumus toimia sekä tehdä päätöksiä spontaanisti ilman seurausten ajattelua.	Käytös	Aivazpour & Rao (2020)
Yksityisyys-asenteet	Yksilön suhtautumistavat ja ajatusmallit yksityisyyteen liittyvään toimintaan sekä käytökseen liittyvät arviot ja arvostukset.	Käytös	Stutzman ym. (2011) Zaiferopoulou ym. (2013) Hughes-Roberts & Kani-Zahibi (2014) Büchi ym. (2016)
Käsitys tiedonjaon pakollisuudesta	Yksilön kokemus vaihtoehtojen puutteesta ja henkilökohtaisten tietojen luovuttamisen välttämättömyydestä.	Käytös	Marwick & Hargittai (2019)
Hyödyt	Yksilölle tiedonjaosta (oletetut) realisoituvat hyödyt. Esimerkiksi hinnanalennukset ja käyttömukavuus. Osana privacy calculus -teorian mukaista kustannus-hyötyanalyysia.	Aikeet ja käytös	Hui ym. (2007) Li ym. (2010) Keith ym. (2013) Beldad & Koehorst (2015) Hallam & Zanella (2017) Karwatzki ym. (2017) Li ym. (2017) Alashoor ym. (2018) Marwick & Hargittai (2019) Williams ym. (2019a; 2019b) Wang ym. (2020)

Yksityisyyden paradoksin yksilön aikeita ja käytöstä selittävät tekijät			
Vaikuttava tekijä	Määritelmä	Vaikuttaa	Lähdeviitteet
Yksityisyysriskit	Yksilön tiedonjaosta (oletetut) aiheutuvat riskit ja psykologiset kustannukset, esimerkiksi vaiva, yksityisyyden häirintä, tai identiteettivarkaus. Osana privacy calculus -teorian mukaista kustannus-hyötyanalyysia.	Aikeet ja käytös	Dinev & Hart (2006) Norberg ym. (2007) Li ym. (2010) Keith ym. (2013) Alashoor ym. (2018) Booth & Ho (2019) Marwick & Hargittai (2019)
Yksityisyyshuolet	Yksilöiden oma, subjektiivinen käsitys omien henkilökohtaisten tietojen kontrollista ja koetut pelot, epävarmuudet sekä huolet tiedonjakoon liittyen. Osana privacy calculus -teorian mukaista kustannus-hyötyanalyysia.	Aikeet ja **käytös**	Awad & Krishnan (2006) Dinev & Hart (2006) Joinson ym. (2006) Zorotheos & Kafeza (2009) **Keith ym. (2013)** Hoffman ym. (2016) Dincelli & Goel (2017) **Hallam & Zanella (2017)** Li ym. (2017) Weinberger ym. (2017) Alashoor ym. (2018) Choi ym. (2018) Aivazpour & Rao (2020) Wang ym. (2020)
Subjektiiviset normit	Yksilön henkilökohtainen näkemys ympäröivien ihmisten odotuksista ja mielipiteistä jotakin tiettyä asiaa tai toimintaa kohtaan.	**Aikeet** ja käytös	Hughes-Roberts & Kani-Zahibi (2014) **Dincelli & Goel (2017)** Wang ym. (2020)
Verkkoon ja yksityisyyteen liittyvät taidot	Yksilön verkkoon ja yksityisyyteen liittyvät taidot, tietämys ja tietoisuus. Esimerkiksi ymmärrys organisaation datankeruuseen liittyviin prosesseihin tai henkilökohtaisten tietojen käsittelyyn liittyvä osaaminen.	**Aikeet** ja käytös	Benson ym. (2015) Büchi ym. (2016) **Dincelli & Goel (2017)** Weinberger ym. (2017) Williams ym. (2019a; 2019b) Wang ym. (2020)
Luottamus organisaatioon	Yksilön itse muodostettu arvio organisaation luotettavuudesta ja siitä, ettei vastapuoli toimi opportunistisesti.	Aikeet ja **käytös**	Dinev & Hart (2006) Joinson ym. (2006) **Norberg ym. (2007)** Zorotheos & Kafeza (2009) **Beldad ja Koehorst (2015)** Booth & Ho (2019) Marwick & Hargittai (2019)
Oletettu yksityisyyden kontrolli	Yksilön yksityisyyteen ja käytökseen liittyvät oletukset omasta kontrollista henkilökohtaisiin tietoihin liittyen sekä uskomukset ja koettu luottamus omiin yksityisyyteen liittyviin kykyihin.	Aikeet ja **käytös**	Zorotheos & Kafeza (2009) Hughes-Roberts & Kani-Zahibi (2014) Beldad & Koehorst (2015) Benson ym. (2015) Li ym. (2017) Weinberger ym. (2017) Booth & Ho (2019) **Wu (2019)** Xie ym. (2019)

Yksityisyyden paradoksin yksilön aikeita ja käytöstä selittävät tekijät			
Vaikuttava tekijä	Määritelmä	Vaikuttaa	Lähdeviitteet
Yksilön arvot	Yksilön omat henkilökohtaiset arvokäsitykset. Esimerkiksi painotus individualismin ja kollektivismin välillä sekä kontrollin arvostus.	Aikeet ja käytös	Zaiferopoulou ym. (2013) Dincelli & Goel (2017)
Aikaisemmat kokemukset yksityisyyden häirinnästä	Yksilön omat kokemukset itseensä kohdistuneista yksityisyyden suojan häirinnästä tai rikkomuksista.	Aikeet ja käytös	Awad & Krishnan (2006) Büchi ym. (2016)
Yksityisyys-persoonallisuus	Yksilöiden persoonallinen ominaisuus ja piirre. Yksityisyyspersoonallisuus perustuu yksilöiden keskuudessa esiintyviin yhtäläisyyksiin ja eroavaisuuksiin, joiden avulla voidaan jakaa yksilöitä erilaisiin ryhmiin yksityisyyden suojaan liittyvien käsitysten ja yksityisyyden arvostukseen liittyen.	Aikeet ja käytös	Hann ym. (2007) James (2014, Kimin 2015 mukaan) Karwatzki ym. (2017) Adorjan & Ricciardelli (2019) Marwick & Hargittai (2019) Schomakers ym. (2019)
Yksityisyys-uupumus	Yksilön tunne ja ajattelutapa yksityisyyteen liittyvän päätöksenteon haastavuudesta sekä halukkuus ja taipumus päätyä yksinkertaisiin ratkaisuihin vaivan minimoiseksi.	Aikeet ja käytös	Choi ym. (2018)