Kinna Tasala

YKSILÖN YKSITYISYYS ESINEIDEN INTERNETIN JA ASIAKASDATAN NÄKÖKULMASTA

JYVÄSKYLÄN YLIOPISTO
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA
2018

TIIVISTELMÄ

Tasala, Kinna
Yksilön yksityisyys esineiden internetin ja asiakasdatan näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2018, 30 s.
Tietojärjestelmätiede, kandidaatin tutkielma
Ohjaaja(t): Palonen, Teija

Esineiden internetin luoma heterogeeninen ympäristö voi aiheuttaa ihmisille useita erilaisia yksityisyysuhkia, koska tiedonkeruu esineiden internetissä on erittäin laajaa ja passiivista. Tiedonkeruu kohdistuu usein yksilöiden henkilökohtaisiin tietoihin, mikä voi olla vahingollista heidän yksityisyydellensä. Yritykset voivat hyödyntää näitä tietoja useilla liiketoimintansa osa-alueilla. Yritysten näkökulmasta esineiden internet luo uusia tehokkaita mahdollisuuksia kerätä ja hyödyntää asiakasdataa, mikä voi vaikuttaa vahvasti yksityisyysuhkien realisoitumiseen. Tämä kandidaatin tutkielma käsittelee esineiden internetin ja asiakasdatan luomia uhkia yksityisyydelle yksilön näkökulmasta. Tutkielma toteutetaan kirjallisuuskatsauksena, jonka aineistona käytetään tieteellisiä julkaisuja aiheesta. Esineiden internetin yksityisyysuhkia yksilölle tarkastellaan ensin yleisellä tasolla, minkä jälkeen perehdytään tarkastelemaan näitä uhkia asiakasdatan näkökulmasta. Jotta asiakasdatan näkökulmaa voidaan ymmärtää, yritysten asiakasdatan keruuta ja hyödyntämistä tarkastellaan osana tätä tutkielmaa.

Asiasanat: esineiden internet, yksityisyys, tiedonkeruu, asiakasdata

ABSTRACT

Tasala, Kinna
The individual's privacy in the perspective of the Internet of Things and customer data
Jyväskylä: University of Jyväskylä, 2018, 30 pp.
Information Systems, Bachelor's thesis
Supervisor(s): Palonen, Teija

The heterogeneous environment created by the Internet of Things might cause several different privacy threats for people because its data collection is very extensive and passive. The data collection is often targeted at the personal information of individuals which can be harmful for their privacy. Companies can take advantage of this information in many areas of their business. In the view of companies, the Internet of Things creates new efficient opportunities to collect and utilize customer data, which can strongly affect the realization of privacy threats. This Bachelor's thesis examines the privacy threats created by the Internet of Things and customer data from an individual's perspective. The thesis is executed as a literature review using scientific publications on the subject. The privacy threats created by the Internet of Things to individuals are first considered in general, after which these threats are also examined from the perspective of customer data. To understand the perspective of customer data, the data collection and utilization of companies are considered as a part of this thesis.

Keywords: internet of things, privacy, data collection, customer data

SISÄLLYS

1 JOHDANTO

Esineiden internet (engl. Internet of Things, IoT) muodostuu laitteista ja arjen esineistä, jotka ovat yhteydessä verkkoon ja jotka kykenevät kommunikoimaan toisten laitteiden sekä ihmisten kanssa (Gubbi, Buyya, Marusic & Palaniswami, 2013, s. 1645-1647). Fyysinen maailma ja kyberavaruus muovautuvat erottamattomiksi esineiden internetin seurauksena (Turgut & Boloni, 2017, s. 62), jolloin siitä tulee yhä laajempi osa ihmisten arkea näkyen niin työelämässä kuin myös kotitalouksissa (Atzori, Iera & Morabito, 2010, s. 2787). Esineiden internet luo siis heterogeenisen verkottuneen ympäristön, joka rakentuu näistä tietoa tuottavista älykkäistä laitteista ja esineistä (Miorandi, Sicari, De Pellegrini & Chlamtac, 2012, s. 1498). Esineiden internetin laitteet (IoT-laitteet) keräävät lukuisien sensoreidensa avulla dataa ympäristöstään ja käyttäjistään. Tämä data voi sisältää muun muassa tietoa käyttäjien terveydestä ja fyysisestä sijainnista. (Turgut & Boloni, 2017, s. 63.) Esineiden internetin sensoreita hyödyntävien laitteiden seurauksena ihmisistä tulee tiedonkeruun kohteita huomaamattomammin, koska ihmisellä itsellään ei ole välttämättä aktiivista roolia tietojen jakamisessa (Lopez, Rios, Bao & Wang, 2017, s. 46).

Gartner Inc:n (2017) arvion mukaan 20,4 miljardia IoT-laitetta tulee olemaan yhdistettynä internettiin vuoteen 2020 mennessä. Älylaitteiden määrän kasvaessa tiedonkeruusta tulee vahvempi osa ihmisten jokapäiväistä elämää, minkä seurauksena tunnistettavissa olevia yksityisiä tietoja päätyy massoittain kerätyksi. Esimerkiksi älykkääseen terveydenhuoltoon liittyvät IoT-ratkaisut luovat yksityisyydelle haasteen, koska ne keräävät paljon arkaluontoista informaatiota käyttäjistä (Al-Fuqaha, Guizani, Mohammadi, Aledhari & Ayyash, 2015, s. 2352-2364). IoT-laitteista tulee yhä arkipäiväisempiä ja tiedonkeruu muodostuu passiiviseksi, jolloin ihmiset eivät välttämättä edes tiedosta sitä (Ziegeldorf, Morchon & Wehrle, 2014, s. 2731).

Yritykset hyödyntävät kuluttajista kerättyä dataa, jota kutsutaan asiakasdataksi, liiketoiminnassaan esimerkiksi profiloimiseen. IoT-laitteiden tiedonkeruun avulla yrityksillä on mahdollisuus saada yhä henkilökohtaisempaa tietoa asiakkaistaan, mikä antaa niille mahdollisuuden kohdentaa palveluitaan ja tuotteitaan yhä voimakkaammin. Toisaalta tätä dataa voivat hyödyntää myös

tietoa myyvät yritykset. (Ziegeldorf ym., 2014, s. 2736.) Organisaatioiden esineiden internetistä saadun datan hyödyntäminen voidaan nähdä mahdollisuutena tarjota käyttäjille parempaa palvelua, mutta toisaalta siitä voi seurata uhkia, esimerkiksi henkilökohtaisen datan leviämistä tietovuodon seurauksena.

Esineiden internetin yksityisyyttä uhkaaviin riskeihin tulisi suhtautua vakavasti, ja ymmärtämällä paremmin näitä uhkia niiden tapahtumista voidaan pyrkiä ennaltaehkäisemään tehokkaammin. Esineiden internetin haasteita yksityisyyttä ja muuta tietoturvaa kohtaan tulisi tutkia muun muassa siksi, koska se on yksi tulevaisuuden älykaupunkien hyödyntämistä tekniikoista (Zhang, Ni, Yang, Liang, Ren & Shen, 2017, s. 122). Tällöin älykaupungin turvallisuutta voitaisiin kehittää ja parantaa toimivien ratkaisujen avulla. Yleisesti esineiden internetin uhat turvallisuudelle ja yksityisyydelle on tunnistettu laajalti, koska esimerkiksi Sicarin, Rizzardin, Griecon ja Coen-Porisinin (2015, s. 159) mukaan Euroopan komissiolla on projekteja näiden ongelmien hallintaan liittyen. Euroopan Unioni on esimerkiksi määrännyt Yleisen tietosuoja -asetuksen (engl. General Data Protection Regulation), joka tiukentaa tietojen keräämisen ja hallinnan säännöksiä sakkojen uhalla. Tämä asetus tulee käytäntöön 25.5.2018. (Euroopan komissio, 2018.)

Tämän kandidaatin tutkielman tarkoituksena on tutkia esineiden internetin tiedonkeruun ja asiakasdatan aiheuttamia haasteita yksityisyydelle yksilön näkökulmasta. Tutkielmassa selvitetään yleisimmät uhat yksityisyydelle ja tarkastellaan tarkemmin esineiden internetin tiedonkeruun hyödyntämistä yrityksissä yksilön kannalta. Tutkielma toteutetaan kirjallisuuskatsauksena, jonka lähdemateriaalia etsitään pääosin Google Scholar -hakupalvelun avulla. Lähdemateriaalia valitessa painotetaan mahdollisimman tuoreita tieteellisiä lähteitä 2010-luvulta, koska tutkielman aiheen kannalta tärkeää ovat tuoreet näkemykset ja tutkimustulokset. Kirjallisuuden pohjalta pyrkimyksenä on vastata seuraaviin tutkimuskysymyksiin:

- Mitä uhkia esineiden internet luo yksilön yksityisyydelle?
- Miten asiakasdataa kerätään ja hyödynnetään yrityksissä?
- Miten asiakasdatan käsittely vaikuttaa yksilön yksityisyyteen ja hänen toimiinsa?

IoT-laitteista oleellisia tutkielman kannalta ovat vain yksilön käytössä tai häneen vahvasti vaikuttavat laitteet, koska asioita tarkastellaan yksilön näkökulmasta. Näin ollen esimerkiksi teollisuudessa käytetyt IoT-laitteet rajataan tarkastelun ulkopuolelle eikä niiden vaikutuksia käsitellä. Kyberturvallisuusuhkia tarkastellaan vain yksityisyyden näkökulmasta, joten muihin tekijöihin kohdistuvat uhkia ja niiden vaikutuksia ei tarkastella.

Luvussa 2 määritellään käsitteet esineiden internet ja yksityisyys sekä käydään läpi esineiden internetin uhkia yksityisyydelle. Oleellisinta tässä luvussa on vastata ensimmäiseen tutkimuskysymykseen. Luvussa 3 käsitellään asiakasdatan keräämistä ja hyödyntämistä yrityksissä yksilön näkökulmasta, jolloin saadaan vastaus toiseen tutkimuskysymykseen ja jotta voidaan käsitellä

kolmatta tutkimuskysymystä. Luvussa 4 yhdistetään lukujen 2 ja 3 tuloksia, jotta asiakasdatan käsittelyn ja yksilön oman toiminnan vaikutukset yksityisyyteen voidaan havaita. Toista ja kolmatta tutkimuskysymystä tarkastellaan esineiden internetin näkökulmasta, koska se vaikuttaa asiakasdatan keräämiseen ja hyödyntämiseen enenemissä määrin ja sen odotetaan yleistyvän yhä laajemmaksi tulevaisuudessa.

2 YKSITYISYYS ESINEIDEN INTERNETISSÄ

Esineiden internet kattaa lukuisia älylaitteita, jotka toimivat vuorovaikutteisesti tarjoten palveluita joko niiden välittömässä läheisyydessä tai etäältä (Lopez ym., 2017, s. 46). Esineiden internet luo paljon uusia mahdollisuuksia, mutta varjopuolena on ihmisten yksityisyyden menetys, sillä esineiden internet kerää paljon tietoa käyttäjiensä elämästä. Tiedonkeruun aiheuttamien uhkien tarkastelun avulla esineiden internetin yksityisyysongelmia voidaan paremmin ymmärtää ja ennaltaehkäistä.

Tässä luvussa käsitellään yksityisyyttä esineiden internetissä. Ensin määritellään käsitteet esineiden internet ja yksityisyys. Esineiden internetin määritelmää käsitellään sen toimintaperiaatteiden ja hyödyntämien teknologioiden avulla. Yksityisyyden määritelmää lähestytään esineiden internetin näkökulmasta, jolloin esineiden internetin vaikutukset käsitteeseen voidaan tuoda ilmi. Tämän jälkeen tarkastellaan esineiden internetin uhkia yksityisyydelle yksilön näkökulmasta.

2.1 Esineiden internet

Esineiden internetille ei ole löydettävissä yhtä yksiselitteistä määritelmää, ja eri määritelmissä painotetaan eri asioita ja teknologioita. Havaittavissa on myös se, että esineiden internetin visio ja idea ovat vaihdelleet ajan saatossa. (Atzori, Iera & Morabito, 2017, s. 122-123.) Tämä seikka selittää osaltaan sitä, että selkeä yksi määritelmä ja visio puuttuvat, koska oleellisesti teknologian kehittyessä myös esineiden internet kehittyy sen myötä. Yhteisiä piirteitä määritelmille on toki löydettävissä, ja Li, Da Xu ja Zhao (2015, s. 244) toteavat, että esineiden internet koostuu laitteista, jotka ovat kykeneviä prosessoimaan ja vaihtamaan tietoa keskenään ja joista jokaisella on oma identiteetti. Esineiden internetin käsitettä voidaan lähteä tutkimaan tarkemmin sen toiminnan ja käyttämien teknologioiden kautta. On havaittavissa, että eri lähteissä esineiden internetin eri teknolo-

gioita painotetaan eri tavalla, joten tähän alalukuun on koottu tämän tutkielman kannalta oleellisemmat esineiden internetin mahdollistamat ominaisuudet.

Esineiden internet luo heterogeenisen verkottuneen ympäristön, joka rakentuu tietoa keräävistä ja tuottavista älykkäistä laitteista, joista käytetään myös lyhennettä IoT-laitteet (Miorandi ym., 2012, s. 1498). Nämä laitteet kommunikoivat ja jakavat tietoa keskenään toisille laitteille sekä ihmisille älykkään teknologian avulla (Al-Fuqaha ym., 2015, s. 2347). IoT-laitteilla on oma identiteettinsä, joka mahdollistaa esimerkiksi laitteiden etäkäytön. Identifioimisen mahdollisuutta pidetään esineiden internetin menestyksen mahdollistavana tärkeänä tekijänä. (Gubbi ym., 2013, s. 1649.)

Esineiden internetin eri laitteiden välisen kommunikoinnin teknologioissa hyödynnetään muun muassa radiotaajuustunnistus- (engl. Radio-Frequency Identification, RFID) ja lähikenttäviestintäteknologiaa (engl. Near Field Communication, NFC). RFID-teknologia mahdollistaa laitteiden välisen kommunikaation laitteisiin sijoitettujen RFID-tunnisteiden avulla. NFC-teknologian avulla laitteet voivat kommunikoida ja vaihtaa tietoa lähellä sijaitsevien laitteiden kanssa. (Al-Fuqaha ym., 2015, s. 2350.) Selkeä esimerkki NFC-teknologian hyödyntämisestä on yleisesti käytössä oleva lähimaksaminen mobiililaitteella (Coskun, Ozdenizci & Ok, 2013, s. 2260).

IoT-laitteiden tiedonkeruun ja prosessoinnin mahdollistaa langaton sensoriverkko, jossa erilaiset sensorit keräävät dataa esimerkiksi sijainnista, liikkeestä ja lämpötilasta. Nämä sensorit voivat olla esimerkiksi älysensoreita, aktuaattoreita tai puettavia tunnistuslaitteita. (Al-Fuqaha ym., 2015, s. 2349-2350.) Sensoriverkko on yksi olennaisimmista komponenteista esineiden internetin toiminnan ja luonteen kannalta, koska sen toiminta nojaa hyvin pitkälti siihen (Luong, Hoang, Wang, Niyato, Kim & Han, 2016, s. 2546). Laajan sensoriverkon myötä on huomattavissa, kuinka suuri osa esineiden internetin toiminnasta perustuu tiedonkeruuseen, -käsittelyyn ja -jakamiseen kommunikaatioteknologioiden avulla. Esineiden internetin voidaan siis nähdä olevan laaja kommunikoiva verkosto, jonka osapuolina on niin laitteita kuin ihmisiäkin.

Atzori, Iera ja Morabito (2017, s. 132) tuovat ilmi, että esineiden internet tulee kehittymään kulloinkin vallitsevien teknologian trendien ja ratkaisujen johdattamana. He esimerkiksi mainitsevat tulevaisuuden internetin hyödyntävän pilvilaskentaa enenevissä määrin, mikä tulee näkymään myös siinä, että pilvilaskentaratkaisuja hyödynnetään esineiden internetissä, erityisesti IoT-laitteiden tuottaman massiivisen datamäärän käsittelyssä (Atzori ym., 2017, s. 132-134). Näin ollen esineiden internetin voidaan olettaa kehittyvän tulevaisuudessa kulloistenkin teknologiatrendien suuntaamana, mikä tekee sen muutoksien ennakoimisen haastavaksi.

Ihmisten elämässä esineiden internet näkyy päivittäin käytössä olevissa esineissä ja laitteissa, joissa on paitsi valmiudet identifiointiin, verkottumiseen ja prosessointiin sekä myös mahdollisuus laajaan kommunikointiin ihmisten ja esineiden kesken (Whitmore, Agarwal & Da Xu, 2015, s. 262). Käyttäjät voivat hallita IoT-laitteitaan etäyhteyden kautta (Gubbi ym., 2013, s. 1649), mikä voi helpottaa monia arjen toimintoja huomattavasti. Esimerkiksi esineiden interne-

tin laitteisiin voi kuulua älykkäitä kodinkoneita, terveyden seurantavälineitä ja sähköverkkoja, jotka voivat muun muassa kerätä tietoa käytetystä sähköstä ja mahdollistavat näin tehokkaan toiminnan (Whitmore ym, 2015, s. 262-265). Näin ollen on nähtävissä, että internetin laitteiden kirjo on laajentunut eikä se kata enää vain muun muassa tietokoneita ja mobiililaitteita. On myös tärkeää huomioida IoT-laitteiden tarjoamat älykkäät palvelut, joita voidaan hyödyntää monilla eri osa-alueilla, kuten edellä mainituista laite-esimerkeistä kävi ilmi.

2.2 Yksityisyys

Ziegeldorfin, Morchonin ja Wehrlen (2014, s. 2730) mukaan yksityisyys on tunnustettu perusihmisoikeudeksi vuonna 1948 Ihmisoikeuksien yleismaailmallisessa julistuksessa. Warren ja Brandeis (1890, s. 216) toteavat, että mediassa ei pitäisi sallia sellaisia julkaisuja, jotka koskevat yksityishenkilöiden henkilökohtaista elämää, tapoja, tekoja tai suhteita. Vaikka vuonna 1890 ei ollut vielä kehittynyttä teknologiaa, yksityisyyden ongelmat olivat jo tuolloin tunnistettu muun muassa sanomalehdissä ja valokuvissa Warrenin ja Brandeisin (1890, s. 195) julkaisun mukaan.

Tietosuoja (engl. information privacy) on noussut huolenaiheeksi lisääntyneen sähköisen tiedonkäsittelyn seurauksena (Ziegeldorf ym., 2014, s. 2729), kun henkilökohtaisten tietojen kerääminen, käsittely, jakaminen ja käyttö ovat tulleet osaksi jokapäiväistä tietotekniikkaa (Smith, Dinev & Xu, 2011, s. 990). Esineiden internetin laitteet ovat kehittynyttä tietotekniikkaa, ja niihin kuuluu myös arjen esineitä (Atzori ym., 2017, s. 135), joiden sensoreilla on valmius tiedonkeruuseen ja -käsittelyyn (Al-Fuqaha ym., 2015, s. 2349). Täten tietosuoja on olennainen asia esineiden internetistä puhuttaessa.

Ziegeldorfin, Morchonin ja Wehrlen (2014, s. 2729) mukaan Westin (1968) on määritellyt käsitteen tietosuoja jo vuonna 1968 oikeudeksi valita, mitä henkilökohtaista tietoa itsestä on kenenkin saatavilla. Tämä määritelmä on varsin vanha, mutta se on edelleen pätevä siitä huolimatta, että maailma on muuttunut erityisesti kehittyneen teknologian seurauksena. Yksityisyyden ja tietosuojan määritelmää voidaan laajentaa esineiden internetin kontekstiin Ziegeldorfin ym. (2014, s. 2729) kolmiosaisen määrittelyn avulla. Tämän määritelmän mukaan yksityisyys ja sen hallinta jaetaan kolmeen alueeseen. Näihin alueisiin kuuluvat tietoisuus älylaitteiden- ja palveluiden aiheuttamista riskeistä, henkilökohtainen kontrolli henkilökohtaisen tiedon keruusta ja käsittelystä sekä tietoisuus ja kontrolli näiden tietojen myöhempää käyttöä ja levittämistä kohtaan. (Ziegeldorf ym., 2014, s. 2729.)

2.3 Esineiden internetin uhat yksityisyydelle

Ihmisten yksityisyys kohtaa useita uhkia ja haasteita lukuisten eri IoT-laitteiden kerätessä ja prosessoidessa heistä kerättyä tietoa heterogeenisessa ympäristössä (Al-Fuqaha ym., 2015, s. 2364). Yksityisyyteen kohdistuvat hyökkäykset voidaan jakaa salakuunteluun ja passiiviseen valvontaan, liikenteen analysointiin sekä tiedonlouhintaan (Abomhara & Køien, 2014, s. 4). Yksityisyyden uhkien tarkastelu pelkästään hyökkäyksien kannalta ei kuitenkaan ole kannattavaa, koska monet uhat ovat peräisin tahattomasta tai tietämättömyyteen perustuvasta toiminnasta. Ziegeldorf, Morchon ja Wehrle (2014, s. 2733-2738) jakavat esineiden internetin aiheuttaman yksityisyyden uhat seitsemään kategoriaan, joihin kuuluvat tunnistaminen, paikallistaminen ja seuranta, profilointi, yksityisyyttä loukkaava vuorovaikutus ja esitys, laitteiden elinkaaren siirtymät, inventointihyökkäys sekä linkitys (Ziegeldorf ym., 2014, s. 2733-2738). Aikaisemmin mainitut yksityisyyteen kohdistuvat hyökkäykset voidaan jaotella tämän seitsenkategorisen uhkien luokittelun alle, joten tämä laajempi jaottelu on mielekkäämpi. Hyökkäykset ovat selkeästi suunniteltuja toimia yksityisyyden loukkaamiseksi, mutta esimerkiksi IoT-laitteiden elinkaaren siirtymistä johtuvat uhat voidaan nähdä tahattomasti aiheutetuiksi. Tästä on nähtävissä yksityisyyden uhkien kaksi selkeästi toisistaan eroavaa puolta, tahattomasti ja tahallisesti aiheutetut uhat. Seuraavaksi nämä seitsemän kategoriaa käydään yksitellen läpi.

Tunnistamisessa on kyse siitä, että yksilöön ja hänen tietoihinsa liitetään jokin tunniste, esimerkiksi osoite tai nimi, jolloin yksilön identiteetti voidaan selkeästi tunnistaa. Tämä aiheutuu uhkaksi, jos yksilön identiteettiä käytetään yksityisyyttä loukkaavassa kontekstissa ja siihen on liitettynä paljon muuta henkilökohtaista tietoa. (Ziegeldorf ym., 2014, s. 2734.) Näiden henkilökohtaisesti tunnistettavien tietojen suojeleminen on haastavaa, koska kerättyä dataa jaetaan nopeasti eteenpäin (Terzi, D. S., Terzi, R. & Sagiroglu, 2015, s. 205). Tätä tiedon jakamista tapahtuu paljon esineiden internetin vuorovaikutteisessa verkostossa, kun kaiken kattava tiedonkeruu ja jakaminen voidaan nähdä yhtenä sen kantavista voimista (Lopez ym., 2017, s. 46). Tällöin tunnistettavien tietojen leviäminen aiheutuu suureksi uhkaksi yksityisyydelle. Ziegeldorf ym. (2014, s. 2735) mainitsevat IoT-laitteiden puheentunnistusominaisuudet erääksi tunnistamisen uhkaksi, koska kerättyjen ääninäytteiden avulla voi olla mahdollista tunnistaa tiettyjä yksilöitä heidän äänestään eri palveluissa. Kerättyjen tietojen anonymisointi eli muuttaminen nimettömäksi voisi suojata yksityisyyttä (Terzi, D. S. ym., 2015, s. 205-206), mutta sen toteuttaminen hajautetussa ja heterogeenisessä esineiden internetin ympäristössä on ongelmallista (Ziegeldorf ym., 2014, s. 2735). Tunnistaminen voi edesauttaa muiden yksityisyyttä vaarantavien uhkien syntymistä kuten esimerkiksi yksilön seurantaa ja profilointia (Ziegeldorf ym., 2014, s. 2734), joita käsitellään tarkemmin seuraavissa kappaleissa.

Paikallistaminen ja seuranta voivat koitua uhkaksi yksilölle, kun hänen sijaintinsa voidaan liittää hänen tunnistettuun identiteettiinsä (Ziegeldorf ym., 2014, s. 2734-2735). IoT-laitteet ovat usein tietoisia sijainnistaan tai hyödyntävät

paikallistamiseen GPS-teknologiaa (maailmanlaajuinen paikallistamisjärjestelmä) ja mobiiliverkkoja (Mattern & Floerkemeier, 2010, s. 246), ja paikallistaminen on useiden IoT-laitteiden merkittävä ominaisuus sen toiminnan kannalta (Ziegeldorf ym., 2014, s. 2735). Tämä kuitenkin voi johtaa siihen, että sijainnin seuranta muodostuu uhkaksi yksilön yksityisyydelle, jos hänet voidaan tämän lisäksi myös tunnistaa. Ongelmalliseksi tämä koituu myös sen takia, että seuranta muuttuu passiivisemmaksi eivätkä ihmiset ole tietoisia tästä heihin kohdistuvasta tiedonkeruusta koski se sitten sijaintia tai muita yksilöllisiä tietoja (Ziegeldorf ym., 2014, s. 2735).

Profiloinnissa yksilöön kohdistuvia tietoja yhdistellään eri tietolähteistä, jotta yksilöstä voitaisiin koota henkilökohtainen profiili. Tämän profiilin avulla voidaan saada esimerkiksi tietoa yksilön kiinnostuksen kohteista. Yritykset saattavat myös myydä profiileja eteenpäin, mikä vahvistaa profiloinnin vaikutuksia yksityisyyteen. (Ziegeldorf ym., 2014, s. 2735-2736). Esineiden internet mahdollistaa yhä henkilökohtaisemman ja massiivisemman tiedonkeruun (Turgut & Boloni, 2017, s. 62-63), jolloin se tarjoaa aikaisempaa vahvemmat lähtökohdat yksityisempien profiilien luontiin. Profiloinnin käyttöä yritysten liiketoiminnassa käsitellään tarkemmin luvussa 3.

Yksityisyyttä loukkaava vuorovaikutus ja esitys ilmenevät, kun henkilökohtaisia tietoja paljastuu ei-halutulle yleisölle henkilön ja IoT-laitteiden vuorovaikutuksen seurauksena. IoT-laitteen ja sen käyttäjän vuorovaikutus voi olla erittäin näkyvää, koska monia laitteita voidaan kontrolloida koskemalla tai puhumalla, jolloin tämä voi näkyä myös ulkopuolisille henkilöille. Toisaalta myös kauppojen suosittelujärjestelmät voivat paljastaa tietoa kuluttajien henkilökohtaisista asioista ulkopuolisille. (Ziegeldorf ym., 2014, s. 2736.) Tämä koituu siis uhkaksi erityisesti sosiaalisissa ympäristöissä, jolloin ihminen on muiden nähtävillä.

Laitteiden elinkaaren siirtymät voivat muodostua uhkaksi silloin, kun IoT-laitteeseen jää edellisen käyttäjän henkilökohtaisia tietoja, esimerkiksi kuvia tai lokitietoja. Kun yhä useammat arkipäiväiset laitteet, kuten televisiot tai autot, keräävät massiivisen määrän dataa, laitteen omistajan muutokset koituvat yhä suuremmiksi uhiksi. Mahdollista on myös IoT-laitteiden vuokraus tai lainaus, mikä lisää samankaltaisia uhkia yksityisten tietojen leviämisestä. (Ziegeldorf ym., 2014, s. 2736-2737.) Laitteiden edelliset käyttäjät voivat luulla, että kaikki heidän tuottamansa tieto on hävitetty, mutta IoT-laitteiden tiedonkeruun ja säilömisen laajuutta on vaikea ymmärtää ja ottaa huomioon laitteen käyttöä lopettaessa (Aleisa & Renaud, 2016, s. 2). Näin ollen on mahdollista, että tallennettuja tietoja ei havaita laitteessa, jotta ne voitaisiin poistaa ennen laitteen seuraavaa omistajaa.

Inventointihyökkäyksessä on kyse luvattomasta henkilön henkilökohtaisten asioiden tietokokoelman ylläpitämisestä, ja tämä kokoelma voi sisältää tietoa henkilön tuntomerkeistä tai muista ominaisuuksista (Ziegeldorf ym., 2014, s. 2737). Esimerkiksi murtovarkaat ovat voineet hyödyntää tällaisia tietokokoelmia jo ilman varsinaisia IoT-laitteita selvittäessään, mikä olisi kannattavin ajankohta suorittaa murto (Bloxham, 2011). IoT-laitteet mahdollistavat tietokokoel-

mat, jotka voivat sisältää tietoa vielä tarkemmin esimerkiksi elämäntavasta ja siitä, milloin henkilö on poissa kotoa. Esineiden internetin tiedonkeruu voi siis helpottaa tällaisten luvattomien tietokokoelmien hyödyntämistä rikollisuudessa. Tämä kategoria on ainoa selvästi vain laittomaan toimintaan perustuva uhka.

Linkitetyn datan käyttö mahdollistaa erilaisista tietolähteistä ja -rakenteista peräisin olevien tietojen hyödyntämisen yhdessä (Malik, Ahmad, Farhan, Aslam, Jabbar, Khalid, Kim, 2016, s. 12729). Esineiden internetissä data on peräisin heterogeenisesta laitteiden, järjestelmien ja palveluntarjoajien joukosta, jolloin datan linkityksestä tulee kannattavaa ja tarpeellista. Tätä voidaan kuitenkin pitää uhkaavana asiana yksityisyyden kannalta, koska linkitetty data voi paljastaa sellaista informaatiota, jota henkilö ei ole halunnut tuoda esille (Ziegeldorf ym., 2014, s. 2738) sekä henkilön on vaikea enää kontrolloida tätä dataa (Serrano-Alvarado & Desmontils, 2013, s. 1). Uhkana on myös yksityisyyden suojausmenetelmien ohittaminen, koska data voi olla peräisin useiden eri yhtiöiden järjestelmistä. Tämä tapahtuu siksi, koska eri laitteilla ja yhtiöillä voi olla erilaiset suojausmenetelmät käytössään, jolloin niiden yhteishallinta dataa linkittäessä voi olla haastavaa. Tämä voi aiheuttaa esimerkiksi tietovuotojen tapahtumisen herkemmin, kun suojaus ei ole kunnossa. (Ziegeldorf ym., 2014, s. 2738.)

Ihmiset eivät usein ole tietoisia esineiden internetin tiedonkeruun aiheuttamista yksityisyysuhista (Weber, 2015). Tämä tietämättömyys voi aiheuttaa sen, että tässä luvussa luetelluista uhkista tulee yhä vaarallisempia ja yleisempiä, kun niihin ei osata varautua ja ottaa huomioon omassa henkilökohtaisessa toiminnassaan. Tällöin myös yksityisyyteen kohdistuvat hyökkäykset voivat yleistyä, kun ne ovat helpompia toteuttaa huomaamattomammin. Yksityisyyttä ja henkilökohtaisia tietoja on vaikea saada takaisin sen jälkeen, kun ne on kerran menetetty, joten näiden uhkien ennaltaehkäisy on tärkeää.

3 ASIAKASDATAN KERÄÄMINEN JA HYÖDYNTÄMINEN YRITYKSISSÄ

Yritykset keräävät ja hyödyntävät kuluttajista kerättyä dataa, asiakasdataa (engl. customer data), koska sen avulla ne voivat parantaa toimintaansa ja saavuttaa menestystä liiketoiminnassaan. Kuluttajien tarpeiden ja käyttäytymisen ymmärtäminen on erittäin tärkeää yritysten toiminnan kehittämisen ja ylläpitämisen vuoksi, koska kuluttajilla on suuri vaikutus yrityksen liiketoiminnan kannattavuuden ylläpitämiseen ja kilpailu markkinoilla on kovaa. (Karwatzki, Trenz, Tuunainen & Veit, 2017, s. 688.) Jo ilman esineiden internetin mahdollistamaa laajaa tiedonkeruuta kuluttajista kerättyä dataa on hyödynnetty oleellisena osana liiketoimintaa. Esimerkiksi Google ja Facebook ovat suurimmaksi osaksi rahoitettu käyttäjätietojen hyödyntämisen avulla. (Karwatzki, ym., 2017, s. 688.) Google ja Facebook ovat esimerkkejä yrityksistä, joiden toiminta on vahvasti riippuvaista asiakasdatan keruusta ja sen hyödyntämisestä. Asiakasdatasta voidaan siis nähdä tulleen myös itsessään liiketoimintaa joidenkin yrityksien kohdalla, vaikka usein sitä käytetään toimintaa tukevana välttämättömänä tekijänä.

Karwatzki, Trenz, Tuunainen ja Veit (2017, s. 688) kertovat internetin tuleen osaksi yksityistä sekä ammatillista elämää, ja että ihmiset aktiivisesti jakavat tietoa itsestään esimerkiksi verkkokaupoissa. Esineiden internet muuttaa tätä skenaariota siten, että kuluttajista kerätty data ei ole vain heidän aktiivisen toiminnan seurauksena tuotettua, vaan iso osa siitä on peräisin passiivisesta tiedonkeruusta ilman kuluttajan omaa aktiivista panosta (Turgut & Boloni, 2017, s. 62-63). Kerätyn datan ja näin ollen asiakasdatan määrä kasvaa siis huomattavasti, mikä tarjoaa yrityksille entistä laajemmat mahdollisuudet asiakasdatan hyödyntämiseen ja tämän avulla mahdollisuuteen saavuttaa kilpailuetua ja menestystä liiketoiminnalle.

Seuraavissa alaluvuissa käsitellään tarkemmin sitä, miten asiakasdataa kerätään ja miten sitä hyödynnetään yrityksen toiminnassa. Asiakasdatan keräämistä tarkastellessa otetaan huomioon niin sanotut perinteiset väylät ja pohditaan esineiden internetin mahdollistamia uusia tiedonkeruun väyliä. Näitä tekijöitä tarkastellaan painottaen kuluttajan eli yksilön näkökulmaa. Tämän jälkeen

käsitellään tarkemmin, miten tätä asiakasdataa hyödynnetään yrityksissä. Tässäkin tarkastelussa esineiden internet otetaan huomioon.

3.1 Asiakasdatan kerääminen

Yritykset pyrkivät keräämään mahdollisimman paljon dataa kuluttajista eri tietolähteistä, jotta voisivat tuottaa mahdollisimman paljon arvoa yritykselle tämän datan hyödyntämisen avulla (Rehman, Chang, Batool & Wah, 2016, s. 918-919). Massiivista data-aineistoa, joka on kerättyä, varastoitua, käsiteltyä tai analysoitua, kutsutaan big dataksi (Manyika, Chui, Brown, Bughin, Dobbs, Roxburgh, 2011, s. 1), johon yritysten tapauksessa voi sisältyä paljon kiinnostavaa tietoa niiden asiakkaista. Yritysten keräämää dataa asiakkaista kutsutaan asiakasdataksi, joka voi sisältää esimerkiksi asiakasta ja hänen käytöstään kuvailevaa dataa tai muun muassa asiakkaiden suoria vastauksia kyselyihin (Rygielski, Wang, Yen, 2002, s. 492). Edellä oleva tieto on peräisin varsin vanhasta lähteestä, mutta asiakasdata sisältää edelleen samankaltaista tietoa. Kuitenkin asiakasdatan voidaan nähdä laajentuneen kattamaan nykypäivänä suurempaa määrää tietoa asiakkaiden elämästä, mikä on seurausta kehittyneen teknologian mahdollistamista uudenlaisista tiedonkeruumenetelmistä. Muun muassa Plangger ja Watson (2015, s. 631) toteavat, että mahdollisuudet kuluttajan seurannassa tulevat kasvamaan entisestään seuraavan vuosikymmenen aikana, koska esineiden internet ja sen hyödyntämät teknologiat, kuten sensoriteknologia ja puettavat laitteet, kehittyvät jatkuvasti.

Ihmiset jakavat aktiivisesti itsestään tietoa käyttäessään internetpalveluita, esimerkiksi verkkokauppoja ja sosiaalista mediaa, jolloin he paljastavat itsestään paljon henkilökohtaista tietoa, joka sisältää informaatiota muun muassa heidän persoonallisuudestaan, käyttäytymisestään ja mieltymyksistään (Karwatzki ym., 2017, s. 688-689). Esimerkkeinä mainittujen verkkokaupan ja sosiaalisen median tapauksessa tiedonkeruu tapahtuu sekä aktiivisesti kuluttajan syöttäessä tietoa itsestään että passiivisemmin asiakkaan toimintaa tarkkailevien seurantavälineiden avulla. Esimerkiksi kuluttajasta voidaan kerätä paljon yksityiskohtaista dataa IP-osoitekohtaisesti evästeiden ja palvelulokien avulla. (Chen, Chiang & Storey, 2012, s. 1167.)

Yritykset itse voivat kerätä asiakasdataa suorasti asiakkaistaan esimerkiksi palautteen tai kyselyiden avulla (Rehman ym., 2016, s. 917-918). Tällöin asiakas on itse selkeästi aktiivisena jakamassa tietojaan yritykselle suorassa interaktiossa. Tässä tiedonkeruun tavassa asiakkaiden oma aktiivisuus on avainasemassa, mikä voi osaltaan vähentää sen tehokkuutta määrällisesti, kun kaikki asiakkaat eivät ole halukkaita jakamaan tietoa avoimesti tai näkemään vaivaa siihen. Toisaalta näin kerätty data voi olla arvokkaampaa yritykselle, koska tällöin asiakkaiden henkilökohtaiset mielipiteet tulevat selkeämmin esille.

Suora interaktio yrityksen ja kuluttajien välillä ei ole ainoa tapa kerätä dataa asiakkaista, vaan yritykset hyödyntävät myös passiivisempaa tiedonkeruuta ja tiedonhankintaa sekundaarisista ulkoisista tietolähteistä (Karwatzki ym.,

2017, s. 688-689). Ulkoiset tiedonlähteet voivat olla kolmansia osapuolia, joihin voi kuulua esimerkiksi tietokantamarkkinoijia tai markkina-analyysiyrityksiä. Epäsuorasti passiivisemmin asiakasdataa on mahdollista kerätä myös esimerkiksi asiakkaan klikkaustiedoista internetsivustoilla tai geo-sijaintitiedoista. (Rehman, ym., 2016, s. 918.) Esimerkiksi sijaintitietoja asiakkaista voidaan saada RFID-teknologian, Bluetoothin tai GPS:n avulla arkipäiväisistä laitteista ja esineistä (Plangger & Watson, 2015, s. 628). Esineiden internetissä monet IoT-laitteet ovat tietoisia sijainnistaan ja hyödyntävät juuri edellä mainittuja teknologioita. Tämän avulla yritykset voivat saada tietoon asiakkaidensa tietoja reaaliajassa sijaintikohtaisesti. (Mattern & Floerkemeier, 2010, s. 246.) Esineiden internet siis tehostaa passiivista tiedonkeruuta reaaliajassa.

Esineiden internetin myötä dataa on mahdollista kerätä ja siirtää jatkoprosessointiin langattoman sensoriverkon avulla. Sensoriverkot ovat älykästä teknologiaa, jonka on mahdollista optimoida toimintaansa ilman ihmisen vahvaa osallistumista tähän optimointiin. (Luong ym., 2016, s. 2546.) Sensoriverkonmahdollistama automaattinen tiedonkeruu lyhentää huomattavasti datan prosessointiaikaa (Atzori ym., 2010, s. 2795), mikä voi tehdä sen yrityksille kannattavaksi tiedonkeruun väyläksi. Esineiden internetin voidaan siis nähdä helpottavan ja automatisoivan datan keruuta, ja tämän johdosta yritykset voivat saada suuremman määrän merkityksellisestä asiakasdataa asiakastietokantoihinsa jatkohyödyntämistä varten IoT-laitteiden avulla.

Yritysten täytyy säilyttää kerättyä asiakasdataa kuten muutakin tietoa jollain tavalla myöhempää hyödyntämistä varten. Datan varastointi voidaan toteuttaa joko itse tai käyttää toisen yrityksen tarjoamaa datan varastointipalvelua. Usein päädytään pilvipalvelun käyttöön, koska silloin yrityksen ei tarvitse ylläpitää omaa paikallista infrastruktuuria datan varastoinnille. Pilvipalveluiden käytössä on useita hyötyjä, koska sen avulla voidaan vähentää varastoinnista aiheutuneita kustannuksia ja saavuttaa hyvä datan saatavuus riippumatta sen hetkisestä sijainnista. (Wang, Ren, Lou & Li, 2010, s. 20.) Esineiden internetin myötä datan ja sen lähteiden heterogeenisuus luo datan varastoinnille haasteita, jotka tulee ottaa huomioon varastointi infrastruktuurin toteutuksessa (Jiang Da Xu, Cai, Jiang, Bu, & Xu, 2014, s. 1443-1444). Myös tämän takia yritysten voi olla helpompi ulkoistaa datan varastointi ja sen vaatiman infrastruktuurin ylläpito.

3.2 Asiakasdatan hyödyntäminen yrityksissä

Asiakkuudenhallinnan (engl. customer relationship management) avulla yritykset voivat ymmärtää paremmin asiakkaitaan ja parantaa sen avulla kilpailukykyään markkinoilla (Chen & Popovich, 2003, s. 672-673; Bahrami, Ghorbani & Arabzad, 2012, s. 60). Huolimatta asiakkuudenhallintaan liittyvien artikkelien välisestä pitkästä julkaisuvälistä asiakkuudenhallinta nähdään molemmissa erittäin tärkeänä, jopa välttämättömänä, toimintana yrityksissä. Informaatioteknologiaa käytetään paljon yritysten asiakassuhteiden hallinnassa. Tässä hal-

linnassa oleellista on myös asiakasdatan tehokas hyödyntäminen (Bahrami ym., 2012, s. 61.) Informaatioteknologian kehittyminen näkyy siis myös asiakkuudenhallinnassa, jolloin myös esineiden internetin tuo omat vaikutuksensa siihen.

Yleisimmin yritykset käyttävät asiakasdataa kehittääkseen joko tuotteitaan ja palveluitaan tai löytääkseen tuottoisimmat asiakkaat (Saarijärvi, Grönroos & Kuusela, 2014, s. 529), mutta on olemassa myös yrityksiä, joiden liiketoiminta on itsessään rahoitettu täysin asiakasdatan hyödyntämisen, esimerkiksi datan myymisen mainostajille, kautta (Karwatzki, ym., 2017, s. 688). Toisaalta on myös olemassa yrityksiä, joiden toiminta perustuu täysin tiedonkeruuseen, kun yrityksen liiketoimintana on esimerkiksi vain myydä kerättyä dataa (Ziegeldorf ym., 2014, s. 2736). Näin ollen on nähtävissä monenlaisia eri tavoin asiakasdataa hyödyntäviä yrityksiä, joista toisissa liiketoiminnan pääkohtana on nimenomaan asiakasdata, ja toisaalta toisissa pääkohtana on tukea liiketoimintaansa asiakasdatan avulla joko käyttäen sitä toimintansa kehittämiseen ja/tai vahvemmin rahoituksen hankkimiseen.

Yritykset keräävät suuria määriä asiakasdataa monista eri lähteistä, kuten yleisesti big dataa on tapana kerätä, mikä tekee hyödyllisen tietämyksen löytämisen haastavaksi (Wu, Zhu, Wu & Ding, 2014, s. 98). Suuresta datamäärästä voidaan havaita piiloutunutta informaatiota asiakkaista tiedonlouhinnan avulla, mikä helpottaa yrityksen asiakasymmärryksen muodostamista. Tiedonlouhinnassa on kyse suuren datamäärän tutkimisesta ja mallintamisesta, jonka prosessissa käytetään monia eri laskentamenetelmiä, jotta voidaan löytää ymmärrettävää ja hyödyllistä tietoa. (Shaw, Subramaniam, Tan & Welge, 2001, s. 128.) Tiedonlouhinnan laskentamenetelmien voidaan olettaa kehittyneen huomattavasti tehokkaammiksi teknologian kehittyessä, mutta toisaalta myös tiedonkeruun määrä ja näin ollen asiakasdatan määrä ovat kasvaneet. Esineiden internet tekee tiedonlouhinnasta vielä haastavampaa, koska data on lähtöisin yhä heterogeenisimmistä lähteistä ja se on hyvin vaihtelevissa muodoissa (Chen, Deng, Wan, Zhang, Vasilakos & Rong, 2015, s. 7).

Chen ym. (2015, s. 6) mainitsevat sähköisen kaupankäynnin olevan yksi yleisimmistä tiedonlouhinnan tarkoituksista. Tiedonlouhinnan avulla voidaan löytää asiakkaiden käytöksen ja palveluiden käyttämisen malleja, ja niiden avulla voidaan parantaa asiakastuntemusta ja luoda arvokasta tietämystä asiakkaista (Padhy, Mishra, Panigrahi, 2012, s. 43-53). Asiakkaan toimia voidaan analysoida, jolloin esimerkiksi palveluita tai tuotesuosituksia voidaan personalisoida vahvemmin tietylle yksilöidylle asiakkaalle (Chen ym., 2015, s. 6). Tämän avulla yritykset voivat tarjota yhä henkilökohtaisempaa palvelua asiakaskohtaisesti yksilöille.

Luvussa 2 esineiden internetin uhkien käsittelyssä mainittu profilointi on yleinen tapa hyödyntää kuluttajista kerättyä ja koottua dataa liiketoiminnassa, erityisesti sähköisessä kaupankäynnissä. Useat liiketoimintamallit nimenomaan nojaavat vahvasti profilointiin ja ovat saavuttaneet huomattavaa menestystä sen avulla. Kuluttajien profiilien avulla yritykset voivat kohdentaa palveluitaan henkilökohtaisemmin yksilöille, kun tiedossa on hänen perustietonsa sekä esimerkiksi hänen käytökseensä liittyvää tietoa. (Ziegeldorf ym., 2014, s. 2736-

2738.) Asiakkaan profiilin luonti vaatii asiakasdatan systemaattista tallentamista ja keräämistä eri tietolähteistä (Wiedmann, Buxel & Walsh, 2001, s. 171), mutta sen voidaan nähdä olevan kannattavaa, koska asiakasprofiilien hyödyntäminen voi tehostaa liiketoimintaa huomattavasti. Yritykset voivat esimerkiksi tunnistaa eri asiakkaiden profiilien samankaltaisuutta vertailun avulla ja kohdistaa personolisoituja palveluja tai tuotteita toisen samankaltaisen asiakasprofiilin omaavan henkilön toimien perusteella (Chen ym., 2015, s. 6).

Esineiden internet vaikuttaa paljon sähköiseen ja erityisesti mobiiliseen kaupankäyntiin, koska IoT-teknologioiden keräämien tietojen avulla markkinointia voidaan tehdä liittyen kuluttajan sen hetkisen tilanteen sijaintiin, aikaan tai kontekstiin (Tsai, Wang, Yan & Chang, 2017, s. 1). Datan linkityksen avulla esimerkiksi kuluttajan profiiliin voidaan liittää tieto hänen sen hetkisestä sijainnista, mikä tekee näistä tiedoista merkityksellisempiä yrityksille, koska tätä tietoa voidaan hyödyntää esimerkiksi reaaliaikaisena mainontana perustuen sen hetkisen sijainnin lähellä oleviin palveluihin (Malik ym., 2016, s. 12729; Tsai ym., 2017, s. 1-2).

4 YKSITYISYYDEN HUOMIOIMINEN ASIAKASDATAN HYÖDYNTÄMISESSÄ

Asiakasdataa vahvasti hyödyntävät yritykset ovat saavuttaneet yleisesti menestystä, joten suurten tietomäärien, big datan, kerääminen on edelleen suosittua. Tiedonkeruu ja -käsittely kohdistuu eniten yrityksen asiakaskuntaan. Esineiden internet edesauttaa ja vahvistaa tätä asiakasdatan suurta hyödyntämistä, koska keskeistä esineiden internetissä on kaikkialla läsnä oleva tiedonkeruu. (Ziegeldorf ym., 2014, s. 2738.) Yritykset hyötyvät huomattavasti liiketoiminnallisesti tästä tiedonkeruusta, mutta asiakkaiden yksityisyyden huomioiminen voi jäädä näiden hyötyjen varjoon. Tällöin asiakkaan olisi hyvä olla itse tietoinen tämän ilmiön haasteista kuten myös mahdollisuuksista, jotta hän voi toimia turvallisesti ja kannattavasti ympäristössä, jossa tiedonkeruu on vahvasti läsnä.

Tässä luvussa yhdistetään lukujen 2 ja 3 havaintoja tarkastelemalla yritysten asiakasdatan hyödyntämisen vaikutuksia yksilöön erityisesti esineiden internetin näkökulmasta. Tämän luvun tarkasteluissa keskiössä on siis yksilön näkökulma tähän aiheeseen. Alaluvussa 4.1 käsitellään sitä, miten asiakasdatan keruu ja hyödyntäminen vaikuttavat yksilöön ja hänen yksityisyyteensä. Toisin sanoen siis luvussa 2 esiteltyjä esineiden internetin yksityisyysuhkia ja luvun 3 havaintoja asiakasdatasta hyödynnetään yhtenäisen kuvan luomiseksi. Alaluku 4.2 keskittyy tarkastelemaan lyhyesti yksilön omia toimia suojatakseen yksityisyyttään. Alaluvussa ei tarkastella yritysten toimia asiakkaidensa yksityisyyden suojaamiseen vaan painopiste on yksilössä itsessään.

4.1 Asiakasdatan haasteet ja mahdollisuudet

Camenisch (2012, s. 3834) toteaa henkilökohtaisten tietojen olevan nykyään niin sanottu uusi valuutta internetissä rahan sijasta. Kun henkilökohtaisesta tiedosta tulee näin tärkeä osa liiketoimintaa, on pohdittava sitä, kuinka henkilökohtaisia tietoja ihmiset ovat valmiita jakamaan yrityksille ja onko arkaluonteisen henkilökohtaisen datan käyttö oikein esimerkiksi personolisoitujen palveluiden tuot-

tamisessa. Esimerkiksi puettavien IoT-laitteiden sensorien, muun muassa sykemittarien ja muiden erilaisten seurantavälineiden, avulla voidaan kerätä yksilöstä erittäin henkilökohtaista dataa, joka sisältää paljon tietoa esimerkiksi hänen terveydentilastaan (Turgut & Boloni, 2017, s. 63). Toisaalta tällaista yksityiskohtaista ja henkilökohtaista dataa hyödyntämällä voidaan tarjota kohdistettuja palveluita, jotka luovat arvoa yksilölle ja hän voi hyötyä niistä huomattavasti. Varjopuolena on kuitenkin yksityisyyden ja yksilön oman hallinnan menetys henkilökohtaista dataa kohtaan, mikä kuuluu aikaisemmin tässä tutkielmassa mainittuun Ziegeldorfin ym. (2014, s. 2729) yksityisyyden määritelmään.

Asiakasdatan aiheuttamia yksityisyyden uhkia, kuten myös mahdollisuuksia, yksilölle aiheuttavat monet tekijät, jotka mainittiin luvussa 2. Uhkia yksityisyydelle asiakasdatan keruun ja hyödyntämisen näkökulmasta voidaan nähdä samoissa tekijöissä kuin Ziegeldorfin ym. (2014, s. 2733-2738) seitsenkategorisessa esineiden internetin yksityisyysuhkien listassa. Näistä tunnistaminen, paikallistaminen ja seuranta, profilointi ja linkitys ovat merkittäviä uhkien aiheuttamia tekijöitä myös asiakasdatan hyödyntämisessä, koska sen keruussa ja näin ollen myös hyödyntämisessä käytetään samoja teknologioita enenevissä määrin tulevaisuudessa, kuten Plangger ja Watson (2015, s. 631) toteavat artikkelissaan. Toisaalta näiden kategorioiden sisältämät asiat tarjoavat uhkien lisäksi myös paljon mahdollisuuksia hyvän kohdistetun älykkään palvelun saannille.

Esimerkiksi sähkön kulutusta ja hintaa seurantaa tarjoava IoT-laite, voi ajastaa pesukoneen päälle kytkemisen ajankohtana, jolloin sähkö on halvinta ja toiminta tehokkainta (Weber, 2015, s. 618). Jotta tämänkaltaista palvelua voidaan tarjota kuluttajille, palveluntarjoajan tulee tietää oleellisesti monia yksityisiä tunnistettavia tietoja, kuten esimerkiksi osoite ja sähkön hinta tai sähkösopimus. Kuten Weber (2015, s. 618) mainitsee, IoT-laitteet luovat arvoa yksilöille, kuten myös liiketoiminnalle, mutta aiheuttavat myös riskejä nimenomaan yksityisyydelle. Tämä luo ristiriitaisen tilanteen, kun yksilön on punnittava haittojen ja hyötyjen välillä, jotta voi päättää, onko hyöty haittojen arvoista.

Asiakasdata voi päätyä myös helposti kolmansille osapuolille, jolloin yksilön yksityisyyden hallitseminen ja suojaaminen vaikeutuvat huomattavasti varsinkin, kun tällöin data voi kulkeutua monen välikäden kautta (Rehman ym., 2016, s. 918; Ziegeldorf ym., 2014, s. 2736-2738). Yksityisyyden kannalta haastavia ovat tietokantamarkkinoijat ja markkina-analyysiyritykset, joiden toiminta perustuu yksilön profiilien tai muun yksilöllisen datan myyntiin (Rehman, ym., 2016, s. 918). Muut yritykset voivat siis ostaa tämänkaltaisilta yrityksiltä heille arvokasta tietoa kuluttajista, mutta yksilön on itse vaikea hallita tätä tiedon kulkua ja jakamista yritysten välillä. Tämä voi tapahtua hyvin huomaamattomasti yksilön näkökulmasta (Turgut & Boloni, 2017, s. 62-63).

Yritykset varastoivat asiakasdataa omissa tai ulkoistetuissa palveluissa, minkä seurauksena syntyy erittäin laaja ja alati kasvava tietokanta heidän asiakaskunnastaan (Wang ym., 2010, s. 20). Asiakasdata voi olla myös hajautettua, jolloin data sijaitsee useassa eri tietokannassa. Tällainen tietokanta voi altistaa

asiakkaat monille uhille, koska tietokannan datan joutuminen vääriin käsiin voi aiheuttaa ongelmia yksityisyydelle. Tätä uhkaa lisää erityisesti tietokannan datan jakaminen eteenpäin yrityksen toimesta, koska se lisää huomattavasti riskiä tietovuodoille tai datan väärinkäytölle, kun suojausmenetelmiä saatetaan ohittaa epähuomiossa. (Ziegeldorf ym., 2014, s. 2728-2738.) Tietovuodossa asiakasdata paljastuu yleiseen tai rikollisten tietoon, jolloin henkilökohtaisen datan vuotaessa yksityisyys joutuu vaikeaan asemaan, koska tietoon voi tulla esimerkiksi tunnistetun yksilön osoite, työpaikka tai terveystietoja (Lopez ym., 2017, s. 50-54). Toisaalta ulkoistettu ja/tai hajautettu pilvipalveluna toteutettu tietokanta voi tarjota nopeita ja kustannustehokkaita datan säilytysratkaisuja (Wang ym., 2010, s. 20), mikä voi osaltaan hyödyttää myös asiakkaan yritykseltä saatujen palveluiden tehokkuutta.

4.2 Yksilön oma toiminta

Fyysisessä maailmassa ihmisen on paljon helpompi arvioida omaa turvallisuuttaan ja yksityisyyttään esimerkiksi lähtiessään ulos, mutta kyberavaruudessa tämä arviointi on paljon haastavampaa (Turgut & Boloni, 2017, s. 62). Tämä tekee oman yksityisyytensä suojelemisesta monimutkaista ja vaikeaa hallita. Uhkia yksityisyyden menetykselle ei välttämättä tiedosteta samalla tavalla, koska esimerkiksi Turgutin ja Bolonin (2017, s. 62) mukaan ihmiset paljastavat henkilökohtaista tietoa useammin kyberavaruudessa kuin fyysisessä kommunikoinnissa. Tämä tuo esiin sen seikan, että fyysisessä kommunikoinnissa osataan ottaa yksityisyys yleisesti paremmin huomioon kuin kyberavaruudessa. Esineiden internet yhdistää nämä kaksi maailmaa erottamattomiksi toisistaan ulottuen yksilön elämän monille osa-alueille, mikä tästä kokonaisuudesta ja näin ollen yksityisyyden hallinnasta entistä monimutkaisempaa (Turgut & Boloni, 2017, s. 62; Atzori ym., 2010, s. 2787).

Luvussa 2 esitellyssä Ziegeldorfin ym. (2014, s. 2729) yksityisyyden määritelmän mukaan oleellista yksilön yksityisyydelle on hänen tietoisuutensa älylaitteiden- ja palveluiden uhkista, kontrollista henkilökohtaisen datan keruuta ja käsittelyä kohtaan sekä tietoisuudesta ja kontrollista datan myöhempää käyttöä kohtaan. Tämän pohjalta yksilön omia toimia yksityisyyttään kohtaan voidaan tarkastella.

Suurimpia uhkia yksilön yksityisyydelle asiakasdatan keruussa ja hyödyntämisessä, ovat yksilön oma vähäinen ymmärrys ja tietämys tiedonkeruusta. Kun asiakasdatan kerääminen tapahtuu yhä passiivisemmin ilman yksilön omaa panosta, ihmisten voi olla vaikeaa tiedostaa sen aiheuttamia uhkia (Turgut & Boloni, 2017, s. 62-63). Erityisesti IoT-laitteiden sensoriverkon tapauksessa tiedonkeruu voi tapahtua hyvin huomaamattomasti arkipäiväisissä tilanteissa, jolloin tiedonkeruun laajuutta ja vaikutuksia voi olla vaikea sisäistää (Ziegeldorf ym., 2014, s. 2731). Muista poikkeavasti Karwatzki ym. (2017, s. 688) tuo kuitenkin ilmi, että monet ihmiset nykypäivänä ovat tietoisempia ja huolestuneempia tiedonkeruun vaaroista kuin ennen olivat, mikä antaa sellaisen ku-

van, että tietoisuus olisi ainakin jollain tasolla lisääntynyt nykypäivänä. Toisaalta tiedonkeruun määrä on kasvanut jatkuvasti, ja esineiden internet sekä datan leviäminen useille osapuolille tekevät kokonaisuudesta monimutkaisemman ja vaikeammin hallittavan. Tämä johtuu tiedonkeruun ja jakamisen tapahtumisesta nopeasti ja passiivisesti. (Terzi, D. S. ym., 2015, s. 205.) Tällöin erityisesti datan leviämistä ja mahdollista myöhempää käyttöä voi olla vaikeaa hallita yksilön omasta toimesta, vaikka olisi tietoinen tapahtuvasta tiedonkeruusta. Yleensä kaikista tietoa keräävien laitteiden ja palveluiden käytöstä ei kuitenkaan haluta luopua.

Yksilö voi pyrkiä suojaamaan yksityisyyttään käyttämällä vain sellaisten yritysten palveluja, joiden asiakasdatan käsittelyyn he voivat luottaa (Atzori ym., 2017, s. 125-131). Toinen tärkeä asia yksityisyytensä suojaamiseen yksilön kannalta on se, että hänen tulisi ymmärtää ja mahdollisuuksien mukaan rajoittaa liian henkilökohtaisen datan jakamista käyttäessään verkko- tai IoT-toteutuksia. Tärkeää olisi ymmärtää, mitä tietoja on valmis luovuttamaan palveluntarjoajille. IoT-laitteiden langaton tiedonsiirto ja kommunikointi sekä datan nopea leviäminen tekevät kaikkien osapuolien tunnistamisesta hankalaa (Ziegeldorf ym., 2014, s. 2728-2733), jolloin on vaikeampia tulla tietoiseksi epäluotettavista toimijoista. Tähän auttaa yksilön tietoisuus hänen ja yrityksen välisestä sopimuksesta tiedonkeruun ja -käsittelyn suhteen, jolloin hän voi olla käyttämättä palveluita sellaisilta tahoilta, joiden toimintaperiaatteista hän ei ole varma (Terzi, D. S. ym., 2015, s. 205). Näin ollen on tärkeää myös tietää yrityksen tietosuojakäytännöt ja omat oikeutensa itseensä kohdistuvaa tiedonkeruuta kohtaan yksityisyyden turvaamiseen. Täyttä kontrollia henkilökohtaisesti identifioitavasta datasta on kuitenkin vaikea enää saavuttaa, koska esimerkiksi Terzi, D. S. ym. (2015, s. 206) ovat todenneet, että järjestelmien ja sovellusten kehittyminen on johtanut tilanteeseen, että yksilö on menettänyt tiedonkeruun ja tiedon hyödyntämisen hallinnan. Varovainen toiminta voi kuitenkin pienentää riskiä yksityisyyden vaarantamisessa, vaikka kaikissa yllä mainituissa lähteissä täyttä hallintaa pidetään mahdottomana. Yksilön on kuitenkin tiedostettava se tosiasia, että kyberavaruuteen on paljon helpompi luoda epämääräisiä palveluita kuin fyysiseen maailmaan (Turgut & Boloni, 2017, s. 62), jolloin varovaisuuden avulla voidaan välttää niiden käyttö.

Lowry, Dinev ja Willison (2017, s. 556) uskovat, että esineiden internetin tullessa tutummaksi, ihmiset alkavat kiinnittää enemmän huomiota datan kontrollointiin ja verkottuneisiin laitteisiin. Hyödyllistä voisi olla tietämyksen lisääminen ihmisten keskuuteen esimerkiksi jonkin kansallisen tahon puolesta. Tällöin yksityisyyteen vaikuttavat tekijät asiakasdatan ja esineiden internetin suhteen nousevan suurempaan tietoisuuteen koko väestön keskuudessa varsinkin, kun termi esineiden internet sen ominaisuuksineen tulee tutummaksi. Jotta yksilö voisi saavuttaa haluamalla tasolla yksityisyyden, hänen tulisi olla tietoinen uhkista sekä punnita hyötyjen ja haittojen välillä. Ainakin liiketoiminnan näkökulmasta huomioitavaa on se, että täydellinen asiakkaiden yksityisyys ei voi olla enää saavutettavissa, koska tällöin yritys joutuisi luopumaan voitoistaan ja myös asiakkaille tarjotut palvelut kärsisivät tästä (Turgut & Boloni, 2017,

s. 63). Yksilön on siis hyväksyttävä täydellisen yksityisyyden menettäminen käyttäessään nykypäivän palveluita. Turgut ja Boloni (2017, s. 63) toteavat, että esineiden internetissä tulisi päämääränä täydellisen yksityisyyden sijasta olla reilu kauppa.

5 YHTEENVETO

Tässä tutkielmassa tarkasteltiin esineiden internetin ja asiakasdatan keruun luomia uhkia yksityisyydelle yksilön näkökulmasta. Tämän tarkastelun avulla voidaan havaita ongelmakohtia ja pohtia, miten tämä vaikuttaa yksilöön. Tutkimus toteutettiin kirjallisuuskatsauksena kandidaatin tutkielman tavoin. Lähdemateriaalin valinnassa painotettiin mahdollisimman tuoreita lähteitä, koska erityisesti esineiden internet on varsin tuore käsite, joka kehittyy edelleen jatkuvasti. Tutkielmaa varten lähteitä etsittiin kattava määrä, jotta aiheesta saatiin hyvä kokonaiskuva ja laajasti tietoa aiheen eri puolista. Kaikkiin tutkielman aiheisiin ei löytynyt suoraa lähdemateriaalia, mutta aihetta sivuavista artikkeleista saatiin kuitenkin koottua selkeä ja informatiivinen katsaus.

Tutkielman rakenne luvuittain koostuu johdannosta, kolmesta sisältöluvusta ja yhteenvedosta. Johdannon jälkeen luvussa 2 käsiteltiin yleisesti esineiden internetin aiheuttamia uhkia yksilön yksityisyydelle Ziegeldorfin ym. (2014, s. 2733-2738) laatiman seitsenkategorisen uhkaluokittelun mukaan. Tarkastelun kannalta tärkeät käsitteet ”esineiden internet” ja ”yksityisyys” määriteltiin kattavasti tutkimuksen aiheelle sopivalla tavalla ennen varsinaista keskittymistä ensimmäiseen tutkimuskysymykseen. Luvun päätarkoituksena oli siis käsitteiden määrittelyn lisäksi vastata ensimmäiseen tutkimuskysymykseen. Seitsenkategorinen uhkaluokittelu osoittautui toimivaksi, koska se sisälsi kattavasti sekä tahallisesti että tahattomasti aiheutetut uhat. Monet muut aihetta käsittelevät artikkelit myös käyttivät Ziegeldorfin ym. (2014) luokittelun sisältävää artikkelia lähteenään, joten sen voi päätellä olevan vakuuttava ja järkevä kategorisointi luokitteluun. Uhkia tarkastellessa huomattiin se seikka, että suurin osa yksityisyysuhkista aiheutuu tai voimistuu yksilön omasta huolimattomasta toiminnasta tietämättömyyden vuoksi. Näin ollen uhkien ennaltaehkäisyssä tulisi kiinnittää huomiota yleisen tietämyksen lisäämiseen. Tarkemmat jatkotutkimukset tästä havainnosta olisivat kannattavia varsinkin, kun aiheesta ei ole kovinkaan tarkkoja tutkimuksia vielä olemassa ja tästä tutkielmasta keinot uhkien ennaltaehkäisemiseen ovat rajattu ulos tarkemmasta käsittelystä.

Luvussa 3 tarkasteltiin tarkemmin asiakasdatan keräämistä ja hyödyntämistä yrityksissä, eli vastattiin toiseen tutkimuskysymykseen. Tarkastelussa

otettiin vahvasti huomioon esineiden internetin tarjoamat mahdollisuudet ja vaikutukset asiakasdataan. Tutkimuksia, jotka käsittelevät asiakasdatan ja esineiden internetin yhteyttä, on vielä varsin vähän saatavilla. Lähdemateriaalia suoraan edellä mainittuun asiaan liittyen oli haastavaa löytää, ja yleensä asiakasdataa käsitellessä kantaa otettiin vain hyvin lyhyesti esineiden internetin näkökulmasta. Kuitenkin tutkielmassa onnistuttiin kuvaamaan selkeästi asiakasdatan keräämistä ja hyödyntämistä yrityksissä yksilön, eli kuluttajan, näkökulmasta niin, että myös esineiden internetin vaikutus voitiin ottaa huomioon yhdistelemällä useiden tieteellisten julkaisujen sisältöä lähdemateriaalina. Lähteissä tuli ilmi asiakkaiden valvonnan lisääntyvän huomattavasti tulevaisuudessa esineiden internetin myötä. Tällöin jopa yrityksillä voi olla vaikeuksia osata hyödyntää kaikkea esineiden internetin tarjoamaa monipuolista heterogeenista dataa asiakkaista (Plangger & Watson, 2015, s. 631), koska esimerkiksi tämän johdosta tiedonlouhinnasta tulee vaikeampaa, kun piilotettua tietoa tulisi löytää massiivisesta aineistosta (Chen ym., 2015, s. 7). Asiakasdatan tyypillisimpinä tapoina havaittiin olevan tiedonlouhinnan kautta profilointi ja personolisoidut palvelut sekä toisaalta myös liiketoiminnan rahoittaminen erityisesti tietoja myymällä.

Luku 4 yhdistää lukujen 2 ja 3 havaintoja, jotta asiakasdatan yksityisyysuhat voitaisiin huomioida tehokkaasti esineiden internetissä. Luvussa tarkasteltiin sekä asiakasdatan haasteita, että myös mahdollisuuksia yksilölle, minkä lisäksi pohdittiin yksilön oman toiminnan vaikutusta yksityisyyteensä hallintaan tässä kontekstissa. Tämä tarkastelu vastasi kolmanteen tutkimuskysymykseen. Tässä tarkastelussa ei otettu huomioon yrityksen toimia kuluttajien yksityisyyden turvaamiseen, mikä on myös oleellinen osa kokonaisuutta yksityisyyden suojelemisessa heterogeenisessa ympäristössä. Toisaalta ongelmalliseksi osoittautui, että monet tieteelliset artikkelit käsittelivät juuri näitä yrityksen toimia eikä yksilön omia toimia, minkä takia lähteitä oli paikoin vaikea löytää. Yksilön omia toimia yksityisyytensä suojelemiseen oli myös vaikeaa tarkastella laajasti kandidaatin tutkielman rajallisen laajuuden vuoksi, koska kattava tarkastelu vaatisi erikseen perinteisempien ja uudempien asiakasdatan keruun väylien pohdintaa. Esineiden internet on laajentanut asiakasdatan keruuta viime vuosina niin paljon, että asiaa käsitteleviä artikkeleita ei vielä ole kovinkaan paljon julkaistu. Kuitenkin asiaa kyettiin tarkastelemaan kirjallisuuskatsauksen tavoin, mutta yksilön omien toimien tarkastelu jäi varsin suppeaksi. Asiakasdatan haasteita ja mahdollisuuksia yksilölle ja hänen yksityisyydelleen havaittiin olevan hyvin monissa samoissa tekijöissä kuin luvun 2 esineiden internetin yksityisyysuhkien tarkastelussa.

Tämän tutkielman rajallisen laajuuden vuoksi kaikkia esineiden internetissä yksityisyyteen vaikuttavia tekijöitä ei pystytty käsittelemään. Esimerkiksi eri näkökulmat yksilön näkökulman lisäksi rajattiin suurimmaksi osaksi pois. Tutkielmassa onnistuttiin kuitenkin sisällyttämään hyvin liiketoiminnan vaikutus yksilön yksityisyyteen, jotta yksityisyyden vaikuttavaa kokonaisuutta voidaan tarkemmin ymmärtää. Jatkotutkimuksissa yrityksen toimia kuluttajiensa yksityisyyteen olisi syytä tutkia tarkemmin, jolloin yksilön omia toimia yksityi-

syytensä suojelemiseksi esineiden internetissä voidaan paremmin tarkastella. Esineiden internetiä voidaan hyödyntää monilla alueilla, ja esimerkiksi terveydenhuolto on eräs näistä alueista, joissa tiedonkeruu esimerkiksi potilaiden osalta on suurta (Whitmore ym, 2015, s. 265). Tämän seikan yksityisyyteen kohdistuvien uhkien tarkastelu vaatisi laajan käsittelyn, joten sitä ei voitu sisällyttää tähän tutkielmaan. Tarkastelu päätettiin kohdistaa vain kaupallisiin yrityksiin, ja muut organisaatiot jätettiin tarkastelun ulkopuolelle.

Tutkielman havainnoista huomioitavaa oli yksilön tietämättömyyden vaikuttaminen yksityisyysuhkiin. Esineiden internet toimii passiivisesti normaalissa arjessa kuten myös työpaikoilla, jolloin seurannasta ja tiedonkeruusta tulee huomaamattomampaa. Tietämättömyyden vuoksi yksilö voi toimia varomattomasti ja huolimattomasti käyttäessään IoT-laitteita, jolloin paljon henkilökohtaista tietoa voi päätyä eri yritysten tietokantoihin, joista se voi nopeasti edetä edelleen eteenpäin muille toimijoille. Tämän vuoksi yksilön olisi tärkeää tunnistaa riskit ja toisaalta myös mahdollisuudet, joita esineiden internetin tiedonkeruu ja prosessointi aiheuttavat, jotta hän voisi itse tietoisemmin hallita ja päättää, mihin on valmis saadakseen esineiden internetin mahdollistamia edistyksellisiä ja personolisoituja palveluita. Tärkeää on myös tietää omat oikeutensa ja tietosuojalait yrityksien tiedonkeruuta ja -käsittelyä kohtaan. Uhkien ennaltaehkäisemiseksi voisi olla perusteltua järjestää koulutusta tai yritysten puolesta ilmoittaa selkeästi tiedonkeruun väylät, jotta ihmisten tietämystään voitaisiin lisätä.

LÄHTEET

Abomhara, M., & Køien, G. M. (2014, May). Security and privacy in the Internet of Things: Current status and open issues. In *Privacy and Security in Mobile Systems (PRISMS), 2014 International Conference on* (pp. 1-8). IEEE.

Aleisa, N., & Renaud, K. (2016). Privacy of the Internet of Things: A Systematic Literature Review (Extended Discussion). *arXiv preprint arXiv:1611.03340.*

Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M. & Ayyash, M. (2015). Internet of things: A survey on enabling technologies, protocols, and applications. *IEEE Communications Surveys & Tutorials, 17*(4), 2347-2376.

Atzori, L., Iera, A. & Morabito, G. (2010). The internet of things: A survey. *Computer networks, 54*(15), 2787-2805.

Atzori, L., Iera, A. & Morabito, G. (2017). Understanding the internet of things: Definition, potentials, and societal role of a fast evolving paradigm. *Ad Hoc Networks, 56*, 122-140.

Bahrami, M., Ghorbani, M. & Arabzad, S. M. (2012). Information technology (IT) as an improvement tool for customer relationship management (CRM). *Procedia-Social and Behavioral Sciences, 41*, 59-64.

Bloxham, A. (2011). Most burglars using facebook and twitter to target victims, survey suggests. *The Telegraph (26 September 2011), 21*. Viitattu 3.3.2018 https://www.telegraph.co.uk/technology/news/8789538/Most-burglars-using-Facebook-and-Twitter-to-target-victims-survey-suggests.html

Camenisch, J. (2012). Information privacy?!. *Computer networks, 56*(18), 3834-3848.

Chen, F., Deng, P., Wan, J., Zhang, D., Vasilakos, A. V. & Rong, X. (2015). Data mining for the internet of things: Literature review and challenges. *International Journal of Distributed Sensor Networks, 11*(8), 431047.

Chen, H., Chiang, R. H. & Storey, V. C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, 1165-1188.

Chen, I. J., & Popovich, K. (2003). Understanding customer relationship management (CRM) People, process and technology. *Business process management journal, 9*(5), 672-688.

Coskun, V., Ozdenizci, B. & Ok, K. (2013). A survey on near field communication (NFC) technology. *Wireless Personal Communications, 71*(3), 2259-2294.

Euroopan komissio. (2018). Data protection in the EU. Viitattu 24.2.2014 https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en

Gartner, Inc. (2017). Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016. Viitattu 1.2.2018 https://www.gartner.com/newsroom/id/3598917

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013). Internet of things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems, 29*(7), 1645-1660.

Jiang, L., Da Xu, L., Cai, H., Jiang, Z., Bu, F. & Xu, B. (2014). An IoT-oriented data storage framework in cloud computing platform. *IEEE Transactions on Industrial Informatics, 10*(2), 1443-1451.

Karwatzki, S., Trenz, M., Tuunainen, V. K. & Veit, D. (2017). Adverse consequences of access to individuals' information: An analysis of perceptions and the scope of organisational influence. *European Journal of Information Systems, 26*(6), 688-715.

Li, S., Da Xu, L. & Zhao, S. (2015). The internet of things: A survey. *Information Systems Frontiers, 17*(2), 243-259.

Lopez, J., Rios, R., Bao, F. & Wang, G. (2017). Evolving privacy: From sensors to the internet of things. *Future Generation Computer Systems, 75*, 46-57.

Lowry, P. B., Dinev, T. & Willison, R. (2017). Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems, 26*(6), 546-563.

Luong, N. C., Hoang, D. T., Wang, P., Niyato, D., Kim, D. I. & Han, Z. (2016). Data collection and wireless communication in internet of things (IoT) using economic analysis and pricing models: A survey. *IEEE Communications Surveys & Tutorials, 18*(4), 2546-2590.

Malik, K. R., Ahmad, T., Farhan, M., Aslam, M., Jabbar, S., Khalid, S. & Kim, M. (2016). Big-data: Transformation from heterogeneous data to semantically-enriched simplified data. *Multimedia Tools and Applications, 75*(20), 12727-12747.

Manyika, J., Chui, M., Brown, B., Bughin, J., Dobbs, R., Roxburgh, C., & Byers, A. H. (2011). Big data: The next frontier for innovation, competition, and productivity.

Mattern, F. & Floerkemeier, C. (2010). From the internet of computers to the internet of things. *From active data management to event-based systems and more* (s. 242-259) Springer.

Miorandi, D., Sicari, S., De Pellegrini, F. & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad hoc networks, 10*(7), 1497-1516.

Padhy, N., Mishra, D., & Panigrahi, R. (2012). The survey of data mining applications and feature scope. *arXiv preprint arXiv:1211.5723.*

Plangger, K. & Watson, R. T. (2015). Balancing customer privacy, secrets, and surveillance: Insights and management. *Business Horizons, 58*(6), 625-633.

Rehman, M. H., Chang, V., Batool, A. & Wah, T. Y. (2016). Big data reduction framework for value creation in sustainable enterprises. *International Journal of Information Management, 36*(6), 917-928.

Rygielski, C., Wang, J. C., & Yen, D. C. (2002). Data mining techniques for customer relationship management. *Technology in society, 24*(4), 483-502.

Saarijärvi, H., Grönroos, C. & Kuusela, H. (2014). Reverse use of customer data: Implications for service-based business models. *Journal of Services Marketing, 28*(7), 529-537.

Serrano-Alvarado, P., & Desmontils, E. (2013, June). Personal linked data: a solution to manage user's privacy on the web. In *Atelier sur la Protection de la Vie Privée (APVP).*

Shaw, M. J., Subramaniam, C., Tan, G. W. & Welge, M. E. (2001). Knowledge management and data mining for marketing. *Decision Support Systems, 31*(1), 127-137.

Sicari, S., Rizzardi, A., Grieco, L. A. & Coen-Porisini, A. (2015). Security, privacy and trust in internet of things: The road ahead. *Computer networks, 76*, 146-164.

Smith, H. J., Dinev, T. & Xu, H. (2011). Information privacy research: An interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Terzi, D. S., Terzi, R. & Sagiroglu, S. (2015, December). A survey on security and privacy issues in big data. In *Internet Technology and Secured Transactions (ICITST), 2015 10th International Conference for* (s. 202-207). IEEE.

Tsai, Y., Wang, S., Yan, K. & Chang, C. (2017). Precise positioning of marketing and behavior intentions of location-based mobile commerce in the internet of things. *Symmetry, 9*(8), 139.

Turgut, D. & Boloni, L. (2017). Value of information and cost of privacy in the internet of things. *IEEE Communications Magazine, 55*(9), 62-66.

Wang, C., Ren, K., Lou, W. & Li, J. (2010). Toward publicly auditable secure cloud data storage services. *IEEE Network, 24*(4)

Warren, S. D. & Brandeis, L. D. (1890). The right to privacy. *Harvard Law Review,* 193-220.

Weber, R. H. (2015). Internet of things: Privacy issues revisited. *Computer Law & Security Review, 31*(5), 618-627.

Whitmore, A., Agarwal, A. & Da Xu, L. (2015). The internet of Things—A survey of topics and trends. *Information Systems Frontiers, 17*(2), 261-274.

Wiedmann, K. P., Buxel, H., & Walsh, G. (2002). Customer profiling in e-commerce: Methodological aspects and challenges. *Journal of Database Marketing & Customer Strategy Management, 9*(2), 170-184.

Wu, X., Zhu, X., Wu, G. & Ding, W. (2014). Data mining with big data. *IEEE Transactions on Knowledge and Data Engineering, 26*(1), 97-107.

Zhang, K., Ni, J., Yang, K., Liang, X., Ren, J. & Shen, X. S. (2017). Security and privacy in smart city applications: Challenges and solutions. *IEEE Communications Magazine, 55*(1), 122-129.

Ziegeldorf, J. H., Morchon, O. G. & Wehrle, K. (2014). Privacy in the internet of things: Threats and challenges. *Security and Communication Networks, 7*(12), 2728-2742.