TURUN YLIOPISTO
Kauppakorkeakoulu

Datankeräys verkossa kuluttajan yksityisyyden näkökulmasta

Markkinoinnin
kandidaatintutkielma

Laatija:
Jasmin Blomstedt

Ohjaaja:
KTT Joachim Ramström
KTT Helena Rusanen

3.5.2023
Pori

Kandidaatintutkielma

Oppiaine: Markkinointi
Tekijä: Jasmin Blomstedt
Otsikko: Datankeräys verkossa kuluttajan yksityisyyden näkökulmasta
Ohjaajat: KTT Joachim Ramström, KTT Helena Rusanen
Sivumäärä: 41 sivua
Päivämäärä: 3.5.2024

Tutkielman aiheena on kuluttajadatan keräys verkossa ja organisaatioiden keinot suojata kuluttajadataa. Kuluttajilla on huolia dataturvallisuudestaan verkossa, eivätkä he ole aina tietoisia datankeräyksestä ja sen tavoista. Tutkimusongelma on kuluttajan yksityisyyden suojaus verkkoympäristössä kerätyssä datassa.

Metodina tutkielmassa käytetään kuvailevaa kirjallisuuskatsausta. Tärkeimmät löydökset ovat kuluttajadatan suojausmenetelmät, joita ovat EU:n yleisen tietosuoja-asetuksen seuraaminen, yksityisyyskäytäntöjen esittäminen verkkosivuilla, opt-outmahdollisuuden tarjoaminen kuluttajalle, itsesääntely ja kryptografiset salauskeinot.

Johtopäätöksistä ilmeni, että läpinäkyvyyden tuominen osaksi organisaatiokulttuuria on keino ylläpitää kuluttajien luottamusta. Suostumuksen saaminen kuluttajalta datankeräykseen on yksi keskeisimpiä tutkielman oppeja. Tämän vuoksi organisaatioiden tulisi esittää selkeät yksityisyyskäytännöt sivuillaan ja tarjota opt-outmahdollisuus. Organisaatiossa tulee kyetä salaamaan kuluttajadata riittävällä tavalla estääkseen sen joutuminen yksityisyysrikkomuksen kohteeksi.

Avainsanat: yksityisyydensuoja, kuluttajansuojalaki, yksityisyyshuolet, verkkodatankeräys, kuluttajien yksityisyys

Sisällysluettelo

Kuvioluettelo

1 JOHDANTO

1.1 Johdatus aiheeseen

Tässä tutkielmassa selvitetään verkosta kerätyn kuluttajadatan suojaustapoja. Tietoturvaongelmat ovat tietoyhteiskunnassa jatkuvasti esillä (Gerlick & Liozu 2019, 9). Acquistin (2016, ks. Gerlick & Liozu 2019, 9) mukaan yksityisyys on nousemassa yhdeksi keskeisimmistä yhteiskuntapolitiikan ongelmista. Tämä aihe valikoitui kandidaatintutkielman teemaksi, koska kuluttajilla on aiempien tutkimusten mukaan huolia siitä, että yritykset keräävät paljon henkilökohtaista tietoa kuluttajista. (Alatalo & Siponen 2001; Lee & Cranage 2011)

Kuluttajista kerätään ja välitetään tietoa muille toimijoille heidän tietämättään ja ilman lupaa. Kuluttajia ei tyypillisesti osallisteta datankeräysprosessiin eivätkä he tiedä, mitä tietoa heistä kerätään, mihin sitä käytetään, kenelle se välitetään ja kuinka se suojataan. (Solove 2003, 1256–1258.) Kuluttajadatan keräämisestä ja hyväksikäytöstä on tullut yksi tärkeimmistä kilpailutekijöistä, jolla yritykset saavat kokonaisvaltaisen kuvan asiakkaistaan (Blasco-Arcas 2022, 436). Koska datan keräyksestä ja prosessoinnista on tullut yleinen toimintatapa markkinointialalla, sääntelyllä on pyritty tarjoamaan kuluttajalle hallintaa omasta datastaan. (Strycharz ym. 2019, 1)

1.2 Tutkimusaukko

Kuluttajadataa on tutkittu monesta näkökulmasta, kuten datapohjaisen markkinoinnin, data-analytiikan ja yksityisyyden, massadatan ja jäsentelemättömän datan näkökulmista. (Blasco-Arcas 2022, 437). Aiempi tutkimus on lisäksi käsitellyt kuluttajan datan keräämistä ilman suostumusta (Alatalo & Siponen 2001, 6–8; Geneiatakis ym. 16). Datankeräys ei aina tapahdu kuluttajan ehdoilla. (Alatalo & Siponen 2001, 7.) Kuluttajat paljastavat verkossa tekemiensä toimintojen kautta tietojaan sekä tiedostamatta että tietoisesti (Acquisti 2015, 509). Kuluttajadatan kerääminen mahdollistaa osuvat hakutulokset, mutta aiheuttaa huolta siitä, onko kuluttajadata turvassa ja leviääkö se kolmansille osapuolille (Alatalo & Siponen 2001, 7). Moni tutkimus on myös käsitellyt kuluttajien reaktioita datankeräykseen (mm. Gerlick & Liozu, 2019; Anderson ym. 2023).

Informaation aikakautena yksityisyys on tärkeä ongelma. Aktiviteetit, jotka aiemmin olivat yksityisiä tai jaettiin vain muutaman kanssa jättävät nyt datajäljen, joka paljastaa persoonallisuuspiirteemme, mielenkiinnon kohteemme, uskomuksemme ja aikomuksemme. (Acquisti 2015, 509.)

Teknologian kehitys on mahdollistanut kuluttajadatan digitalisoitumisen ja avannut uusia mahdollisuuksia datankeräykselle (Blasco-Arcas 2022, 437). Markkinointiviestintä ja myynti nojaavat yhä enemmän teknologiaan (Skiera 2022, 11). Yritykset keräävät kuluttajista dataa, jotta ne saavat tietoa siitä, mikä tuote kiinnostaa yksittäistä asiakasta, ja voivat siten kohdistaa tuotteita ja palveluita paremmin. Esimerkiksi kuluttajan maksuhalukkuutta voidaan tutkia sitä paremmin, mitä enemmän kuluttajadataa on saatavilla ja mitä kehittyneemmät algoritmit ovat käytössä. (Anderson ym. 2023, 2086.)

Kuluttajien yksityisyydensuojan tutkimus on ajankohtaista, koska verkkorikollisuus on nousussa ja markkinat ovat digitalisoituneet (Kyberturvallisuuskeskus, 2020). Lisäksi kuluttajien voimaannuttamisesta ja yritysten läpinäkyvyydestä on tullut yhä tärkeämpi aihe markkinoinnissa (Strycharz ym. 2019, 1), minkä vuoksi tutkielma keskittyy kuluttajadatan suojaamiseen.

1.3 Tutkimuksen tarkoitus ja rajaukset

Tutkimusten mukaan kuluttajien odotukset kuluttajadatan käyttökohteesta eroavat todellisesta tavasta, jolla datankerääjät ja kolmannet osapuolet hyödyntävät dataa. Tämä osoittaa, että kuluttajat eivät pysty hallitsemaan omia tietojaan, elleivät kieltäydy käyttämästä digitaalista alustaa kokonaisuudessaan. (Chapdelaine 2020, 11.) Haasteena ovat siten kuluttajadatan keräämisen aiheuttamat yksityisyysongelmat verkossa. Tämä ongelma nousee esille kuluttajien yksityisyyshuolista: mihin dataa käytetään, käytetäänkö sitä luvatta, pidetäänkö se turvassa ja saako kuluttaja siitä hyötyä. Tiedämme jo paljon kuluttajien näkemyksistä datankeräyksestä (Lee & Cranage 2011; Gerlick & Liozu 2019), mutta emme tiedä riittävästi organisaatioiden toimista henkilötietojen suojaamiseksi eivätkä kuluttajadatan suojaustavat ole kaikkien yritysten käytössä (Strycharz ym. 2019, 2). Tutkimuksen myötä organisaatiot saavat tietoa yksityisyyslainsäädännöstä ja mahdollisista kuluttajadatan suojauskeinoista.

Tutkimuskysymys, johon aion vastata, on *miten organisaatiot voivat suojata kuluttajien yksityisyyttä verkosta kerätyssä kuluttajadatassa*? Osaongelmat ovat: 1) Minkälaista

dataa kuluttajista kerätään verkosta? 2) Mitä keinoja organisaatioilla on suojata kuluttajien yksityisyyttä verkkodatassa?

Ensimmäistä osaongelmaa avataan kertomalla, millä tavoilla organisaatiot keräävät kuluttajien dataa verkossa ja mihin tarkoitukseen dataa käytetään. Koska organisaatiot ovat dataa kerätessään vastuussa sen suojaamisesta, tutkielmassa selvitetään, minkälaisia keinoja datan turvaamiseksi käytetään. Tämä vastaa toiseen osaongelmaan.

Datankeräys rajataan käsittelemään verkossa tapahtuvaa datankeräystä, jossa yritykset keräävät kuluttajadataa markkinointitarkoitukseen. Kuluttajan yksityisyys on laaja käsite, joten ilmiötä tarkastellaan tietosuojan kautta. Siihen sisältyy sekä lainsäädäntö että huolet ja riskit koskien datan leviämistä ja suojaamista sekä luvatonta keräämistä ja käyttöä. Rajaan lainsäädännön käsittelyn EU:n tasolle, ja lainsäädännön tasolla käsitellään EU:n yleistä tietosuoja-asetusta.

1.4 Tutkimusmetodi

Tutkimusmetodina on kuvaileva kirjallisuuskatsaus. Kirjallisuuskatsaukset ovat joukko erityyppisiä tutkimusmenetelmiä joko empiirisen tutkimuksen osana tai itsenäisenä tutkimusmenetelmänä (Kangasniemi ym. 2013, 291–293). Kuvaileva kirjallisuuskatsaus on yksi yleisimmin käytetyistä kirjallisuuskatsauksen perustyypeistä. Sitä voidaan luonnehtia yleiskatsaukseksi ilman tiukkoja rajoituksia ja sääntöjä. Kirjallisuuskatsaus tehdään käyttämällä lähteenä aiempaa tutkimusta, joka on perustana uusille tutkimustuloksille. Kuvaileva kirjallisuuskatsaus keskittyy rakentamaan kokonaiskuvaa tietystä asiakokonaisuudesta. (Salminen 2011, 6–9.) Tutkimusmetodin vahvuuksia ovat sen argumentoitavuus ja mahdollisuus ohjata tutkimusta kysymysten avulla (Kangasniemi ym. 2013, 291–293).

Kuvailevan kirjallisuuskatsauksen tutkimusongelma on usein kysymyksen muodossa. Tällä tutkimusmetodilla saadaan yleiskuva aiheesta aiemman tutkimuksen pohjalta, mutta sen avulla kehitetään samalla laajempia päätelmiä aiheesta. (Kangasniemi ym. 2013, 294–296.)

Kuvaileva kirjallisuuskatsaus valikoitui tämän tutkielman tutkimusmetodiksi, koska sillä voidaan tarkentaa laajan aiheen käsittelyä tiettyyn painopisteeseen (Efron & Ravid 2018, 1–2) ja sillä saadaan selville ilmiöiden suhde (Kangasniemi ym. 2013, 294–296), jotka tässä tutkielmassa ovat kuluttajien yksityisyys ja markkinoinnin datankeräys. Tutkielmaa varten on luettu aihetta koskevaa tutkimusta ja teorioita. Kirjallisuuden tarkastelussa

tarkoituksena on esittää kattava, kriittinen ja todenmukainen ymmärrys aiheen tämänhetkisestä tutkimuksesta, vertailla eri teorioita ja paljastaa tutkimusaukkoja tämänhetkisestä tutkimuksesta. (Efron & Ravid 2018, 1–2.) Tutkimus lähti liikkeelle tutkimusprosessia ohjaavan tutkimuskysymyksen ja osaongelmien muodostamisesta. Sen jälkeen siirryttiin aineiston valintaan. Aineiston tarkastelun avulla on hankittu syvempi ymmärrys aiheesta kuvailun rakentamisella siitä, mitä aiheesta jo tiedetään, ja tutkielman lopuksi tarkastellaan tuotettua tulosta. Tutkielmassa pyritään esittämään aiheen tutkimuksen nykytila tuoreesta näkökulmasta (Efron & Ravid 2018, 4).

Tutkielmassa hyödynnetään vertaisarvioituja markkinoinnin datankeräykseen ja kuluttajan yksityisyydensuojaan liittyviä tieteellisiä journaaliartikkeleita. Tutkielmassa on myös käytetty joitakin kirjalähteitä sekä Suomen lainsäädäntöä, kuten tietosuoja- ja kuluttajansuojalakia, niiltä osin, kun se on tutkimuksen sisällön kannalta välttämätöntä. Käytän tutkielmassani tiedonhakuun EBSCO- (Business Source Complete), ABI/INFORM- ja EconLit -tietokantoja. Lisäksi tutkielmassa on hyödynnetty Suomen lainsäädäntöä verkossa. Hakusanoina tutkielman tiedonhaussa käytettiin termeinä muun muassa ”consumer data”, ”consumer privacy”, ”privacy policy” ja ”consumer privacy concerns”, sekä näistä hakusanoista luotuja erilaisia yhdistelmiä.

1.5 Keskeiset käsitteet

Kuluttajadata viittaa yleisesti kaikkeen henkilökohtaiseen, käytöspohjaiseen, psykografiseen ja demografiseen dataan, jota yritykset keräävät tietokannoistaan. Kuluttajadata koostuu datayksiköistä, jotka kerätään vuorovaikutuksessa asiakkaan kanssa sekä potentiaalisilta että nykyisiltä asiakkailta. (Blasco-Arcas ym. 2022, 436–438.) Kuluttajadatan prosessointi tarjoaa yrityksille arvokasta tietoa kuluttajista, jota voidaan markkinoinnissa hyödyntää oikean tuotteen identifioinnissa oikeille markkinoille, kommunikaatiokanavien, myyntiajankohdan ja hinnan asettamisessa sekä myyntitavan ja -viestin valinnassa. (Elia ym. 2020, 619.)

Yksityisyyslait asettavat toiminnallisia, organisatorisia ja teknisiä vaatimuksia kuluttajadatan keräämiselle, säilyttämiselle ja prosessoinnille. Nämä vaatimukset suojelevat dataa sekä datan kohteita. Vaatimuksiin kuuluu esimerkiksi laillisen tiedonhankinnan edellytykset sekä ilmoittaminen datankeräyksestä, sen tarkoituksesta, datan prosessoinnista ja datan siirrosta datankeräyksen kohteelle. Lainsäädännöllä voidaan myös varmistaa tarvittavat turvamekanismit, kuten pääsynhallinta ja valvonta. (Kobsa 2007, 647–648.)

Yksityisyyskäytäntö (engl. privacy policy) on yksi tutkielman keskeisimpiä käsitteitä, sillä kuluttajan yksityisyyttä tarkastellaan tässä tutkielmassa organisaatioiden yksityisyyskäytäntöjen ja tietosuoja-asetusten kautta. Yksityisyyskäytäntö tarkoittaa kirjallista lausuntoa, usein organisaation verkkosivuilla, joka kertoo toimista informaation käyttöön ja keräykseen liittyen. (Awad & Krishnan 2006, 19–25.) Organisaatioiden yksityisyyskäytännöt ovat yksityisyyskeskustelussa keskeisiä, sillä ne vaikuttavat kuluttajan yksityisyyshuoliin, yksityisyyden hallintaan, näkemykseen riskeistä, luottamukseen ja opt-outvaihtoehdon valintaan. (Mutimukwe ym. 2020, 1–3)

1.6 Tutkielman rakenne

Tutkielma koostuu kuudesta pääluvusta. Luvussa 2 ja 3 käsitellään tutkielman viitekehystä: kuluttajadatan keräystä ja kuluttajan yksityisyyttä. Neljännessä luvussa yhdistetään viitekehykset kuvaamalla ratkaisuja kuluttajadatan turvaamiseen.

Luku 2 käsittelee kuluttajadatan keräystä. Sen alaluvuissa käsitellään kuluttajadataa käsitteenä sekä sen keräystapoja ja hyödyntämistä. Luku 3 käsittelee kuluttajan yksityisyyttä organisaation datankeräyksen kontekstissa. Sen alaluvuissa käsitellään kuluttajan yksityisyyttä käsitteenä sekä sen aiheuttamia ongelmia. Luvussa 4 käsitellään keinoja kuluttajadatan turvaamiseen organisaatioissa. Keinot on jaettu viiteen alalukuun: EU:n yleinen tietosuoja-asetus, yksityisyyskäytännöt, opt-outmahdollisuus, hallinnollinen ja itsehallinnollinen sääntely, ja kryptografiset salauskeinot. Luvussa 5 esitetään tulokset ja johtopäätökset. Luvussa 6 on tutkielman yhteenveto.

2 KULUTTAJADATAN KERÄÄMINEN VERKOSSA MARKKINOINTITARKOITUKSIIN

2.1 Verkosta kerättävä kuluttajadata

Kuluttajadata viittaa kaikkeen henkilökohtaiseen, käytöspohjaiseen, psykografiseen ja demografiseen dataan, jota yritykset keräävät asiakastietokannoistaan. Se voi olla kuluttajan luovuttamaa tai seurannan avulla kerättyä dataa. Seurannan avulla kerätty data voi sisältää jäsenneltyä dataa, kuten dataa liiketoimista, tai jäsentämätöntä dataa, kuten verkkosivuston liikennetietoja tai kuluttajan sijaintidataa. Jäsennelty data on yleensä kuluttajan luovuttamaa, ja yritykset keräävät sitä perinteisin markkinatutkimuksen keinoin. Jäsentämätön data on seurannan avulla kerättyä, joten asiakas ei ole luovuttanut sitä tietoisesti. Sitä kerätään esimerkiksi kokeellisten tiedonkeruun menetelmien avulla sekä liiketoimintaraporteista. (Blasco-Arcas ym. 2022, 437–438)

Kuluttajadatan tallennusmahdollisuudet tekevät aiemmin luovutetusta datasta lähes mahdotonta poistaa (Acquisti 2015, 509). Chapdelainen (2020, 10) mukaan OECD on selvittänyt, että luovutettua dataa ovat muun muassa nimi, ikä, osoite, puhelinnumero, syntymäpäivä, ammatti, koulutus ja vastaukset kyselyihin. Havainnoitua dataa ovat IP-osoite, kuluttajan käyttämä tietokonejärjestelmä, haku- ja ostohistoria, klikkauksen nopeus, kuluttajan sijainti, verkkovierailut ja tykkäykset sosiaalisessa mediassa. Lisäksi voidaan päätellä kuluttajista tietoja, kuten tulot, terveydentila, reaktio mainoksiin, poliittinen suuntautuminen, asiakasuskollisuus ja harrastukset. (Chapdelaine 2020, 10.) Data ei ole kuitenkaan aina todenmukaista. Tämä tarkoittaa, että vaikka yritykset pyrkivät varmistamaan datan täsmällisyyden, nämä prosessit eivät aina ole tehokkaita. (Rao ym. 2015, 7–9)

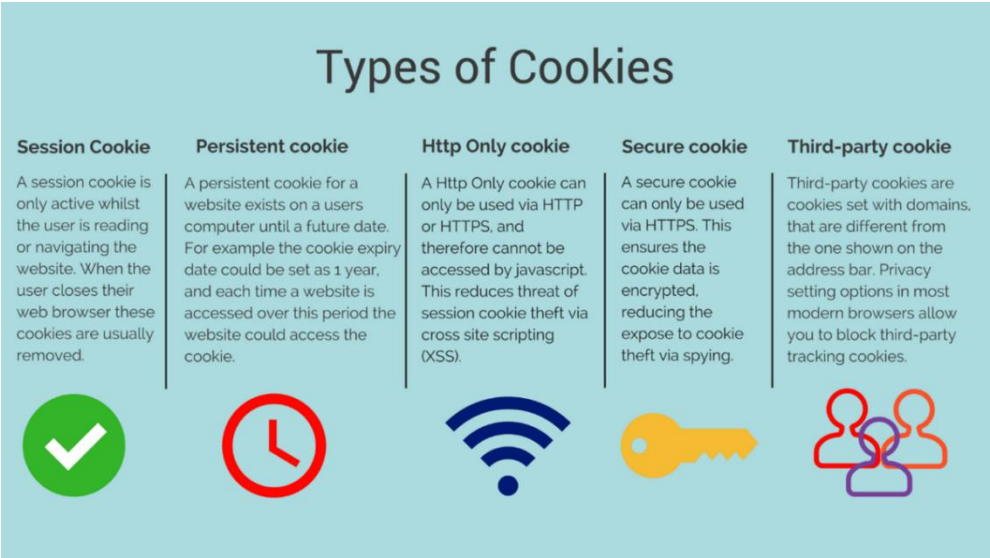
Massadata on monimutkainen ja jatkuvasti kasvava yritysten saatavilla oleva valtava datamäärä (Fyall, 2019, 66). Kuluttajadatan puhdistamisen massadatasta voi mahdollistaa massadata-analytiikka, joka tarkoittaa raakadatan puhdistusta, järjestelyä ja analysointia (Gerlick & Liozu, 2020, 86). Massadata-analytiikalla yritykset voivat muuntaa kuluttajien verkkokäyttäytymisen, kuten hakuhistorian ja ostokäyttäytymisen, arvokkaaksi dataksi, jolla voidaan parantaa kuluttajan asiakaskokemusta ja kasvattaa konversiota eli verkkosivuilla kävijän toivottua käytöstä (Zeng ym. 2022, 781). Kaikesta saatavilla olevasta datamäärästä kuluttajadata on yrityksille erityisen arvokasta, sillä tämä tarjoaa ymmärrystä kuluttajien käytöksestä ja preferensseistä asiakaskosketuspinnoissa sekä digitaalisessa että fyysisessä ympäristössä asiakaspolun varrella. (Blasco-Arcas 2022, 436)

2.2 Keinoja kuluttajadatan keräämiseen verkosta

Tässä luvussa käsitellään keinoja, joilla yritykset voivat kerätä kuluttajadataa verkosta. Keinoina käsitellään evästeitä, kolmannen osapuolen dataa ja mobiilisovelluksia, sillä nämä kolme keinoa tulevat organisaatioiden verkkodatakeräyksestä tehdyssä tutkimuksessa laajasti ilmi. Näiden keinojen avaaminen selkeyttää sitä, mistä kanavista ja millä keinoin organisaatiot saavat kuluttajadataa, jota ne hyödyntävät markkinointitarkoituksiin.

2.2.1 Evästeet

Sähköinen kaupankäynti on yksi keskeisimmistä aloista nykypäivänä, ja verkkokauppojen määrä on kasvanut etenkin koronaviruspandemian aikana (Adak ym. 2022, 70–81). Evästeitä käytetään verkkokaupoissa datankeräykseen, mikä mahdollistaa asiakkaan tunnistamisen ja asiakkaan ostohistorian tarkkailun. Evästeet säilyttävät yksilöllisiä tunnisteita tai tietoja asiakastapahtumista, jotka säilyvät sivustolla seuraavaa vierailukertaa varten. Evästeillä voidaan tarjota yksilökohtaisia hintoja ja tarjouksia tai yksilöityjä ehdotuksia. HTTP-protokolla mahdollistaa evästeiden asettamisen ja niiden lukemisen palvelimella. Evästeiden avulla datan kerääminen ja säilyttäminen verkossa on suhteellisen helppoa. (Acquisti & Varian 2005, 367.) Evästeet voivat olla esimerkiksi selainevästeitä tai flash-evästeitä, jotka liittyvät Adobe Flash -ohjelmaan (Rao ym. 2015, 1–2).



Kuva 1 Kuvaus evästetyypeistä (Let's tech IT easy 2020)

Esimerkiksi verkkokauppa Amazon on erottanut olemassa olevat asiakkaat uusista asiakkaista evästeiden avulla ja muuttanut hintoja yksittäisille asiakkaille aiemman ostokäyttäytymisen perusteella (Huang ym. 2005, 343–346). Amazon tarjoaa evästeiden avulla nopeampaa ostoa vanhoille asiakkaille, säästäen heiltä aikaa, kun heidän ei tarvitse syöttää tilaustietojaan uudelleen. Lisäksi Amazon tarjoaa suosituksia asiakkailleen ostohistorian perusteella. (Acquisti & Varian 2005, 367–371.)

Yritys voi kerätä tietoa verkossa evästeiden avulla, esimerkiksi kun asiakas on laittanut tuotteen verkkokaupassa ostoskoriin, mutta ei ole ostanut sitä. Tämän jälkeen ihmisten suunnittelema, mutta teknologian automaattisesti toteuttama prosessi lähtee käyntiin. Evästeiden avulla yritys voi asettaa kuluttajille näkyviä mainoksia ostoskoriin jääneestä tuotteesta hänen vierailemilleen verkkosivuille. Vaihtoehtoisesti asiakas voi vastaanottaa verkkokauppiaalta viestin sähköpostitse tuotteesta, joka on jäänyt ostoskoriin. Mikäli kuluttaja avaa viestin, se osoittaa yritykselle kiinnostusta tuotteesta. Jos kuluttaja edelleen jättää tuotteen ostamatta, voidaan lähettää uusi viesti alennuksen kera. (Skiera 2022, 11–12.) Evästeeseen tallentuu, onko asiakas ostanut tarjotulla hinnalla, mikä mahdollistaa hinnan säätämisen seuraavalla verkkokaupan vierailukerralla (Acquisti & Varian 2005, 371). Seuraavan kerran kun kuluttaja jättää tuotteen ostoskoriin, voidaan käyttää samaa prosessia. Sitä ei kuitenkaan käytetä enää kolmannella kerralla, koska ei haluta asiakkaan oppivan, että ostamatta jättäminen johtaa hinnan alenemiseen. (Skiera 2022, 11–12)

EU:n yleisen tietosuoja-asetuksen (GDPR) astuttua voimaan Euroopan Unionissa, verkkosivujen tulee informoida kuluttajaa siitä, mitä tietoa ne keräävät kuluttajasta evästeiden avulla ja pyytää lupaa muiden kuin toiminnallisten evästeiden käyttöön. Degelingin ym. (2019, 345–346) tutkimuksessa selvitettiin, kuinka yksityisyyskäytännöt muuttuivat EU:n yleisen tietosuoja-asetuksen astuttua voimaan toukokuussa 2018. Vaikka usealla verkkosivuilla oli jo yksityisyyskäytäntöjä, joissakin maissa jopa 15,7 % verkkosivuista lisäsi uusia yksityisyyskäytäntöjä tietosuoja-asetuksen astuttua voimaan. Yleisen tietosuoja-asetuksen astuttua voimaan 62,1 % Euroopan alueella toimivista verkkosivuista esittivät evästeiden suostumusilmoituksen, joka oli 16 % enemmän kuin tammikuussa 2018 ennen asetuksen voimaantuloa. Nämä ilmoitukset kertovat käyttäjälle evästeiden käytöstä ja käyttäjän seurannasta.

Kuluttajilla on useita keinoja välttyä seurannalta ja personoidulta hinnoittelulta, kuten evästeiden hylkääminen tai poistaminen verkkovierailun jälkeen. Yritysten tulee siis tarjota joitakin etuja asiakkaalle, jotta hän paljastaisi ostohistoriansa tai identiteettinsä.

Evästeet voivat esimerkiksi mahdollistaa nopeamman ostoprosessin, koska evästeet tallentavat toimitus- ja pankkitiedot, jolloin asiakkaan ei tarvitse kirjata niitä uudelleen. (Acquisti & Varian, 2005, 367–368.)

Acquisti ja Varian (2005, 371–376) erottelevat asiakkaita heidän tuottamansa arvon mukaan ja korkean arvon omaavat asiakkaat erotellaan vielä sen mukaan, kykenevätkö he suojautumaan personoidulta hinnoittelulta. Näille kolmelle segmentille voidaan tarjota erilaiset hinnat evästeiden avulla. Evästeet mahdollistavat, että yritys voi muuttaa hintaa, jos evästeeseen on tallentunut, että asiakas ei ole ostanut tuotetta aiemmin tarjotulla hinnalla ensimmäisellä vierailukerralla sivustolla.

2.2.2 Datan hankkiminen kolmannelta osapuolelta

Kolmannen osapuolen data tarjoaa useita uusia mahdollisuuksia markkinoijille, mutta useista lähteistä, kuten johtavilta kuluttajadatan myyjiltä ja verkostoilta, kerätty data on usein hyvin heterogeenistä. (Neumann ym. 2023, 520.) Dataa voidaan saada kolmansilta osapuolilta, kuten markkinointitutkimusta tekeviltä yrityksiltä, luottopisteytyslaitoksilta ja sosiaalisen median kanavista (Buttle & Maklan, 2015, 290). Esimerkiksi datamarkkinayritykset, kuten Acxiom, ChoicePoint ja LexisNexis ostavat ja myyvät kuluttajadataa. Nämä yritykset keräävät, kokoavat kuluttajadataa useista julkisista ja yksityisistä lähteistä. (Li & Raghunathan 2014, 63.)

Yrityksille on kallista kerätä dataa siitä, ketkä kuluttajista voisivat olla kiinnostuneita heidän tuotteistaan ja luoda tarjous sen perusteella. Kustannus voi muodostua yrityksen sisäisestä dataselvityksestä tai ulkoisen datanvälittäjän palveluista, kuten kolmannen osapuolen datan tapauksessa. (Anderson ym. 2022, 2086–2087.) Kustannukset kolmannen osapuolen datan hankinnasta eivät yleensä ole vaivan arvoisia, jos dataa kerätään yleisimmistä kuluttajatyypeistä, koska hyödyt ja kustannukset eivät siis ole sopivassa suhteessa (Neumann ym. 2023, 520).

Eri toimijoiden, kuten alustojen ja verkkosivujen omistajien sekä sovelluskehittäjien, tulee tehdä yhteistyötä, jotta saadaan luotua dataprofiileita kuluttajista. Nämä toimijat työskentelevät yhdessä kerätäkseen kuluttajadataa ja seuratakseen kuluttajien käytöstä. Yhteistyö on välttämätöntä, jotta saadaan luotua katkeamaton sarja dataa, joka kertoo mistä asiakas tulee ja mihin hän menee seuraavaksi verkkoympäristössä. Tällä mainostajat välttävät sen, että heidän tulisi neuvotella jokaisen sivuston kanssa erikseen kuluttajadatan vastaanottamisesta. Tämä toiminta johtaa epäsymmetriseen tiedonkulkuun,

jossa vain yritykset tietävät datavirrasta ja kontrolloivat sitä, mikä vähentää kuluttajan kykyä ylläpitää yksityisyyttään. (Ezrachi & Stucke 2017, 159–160.)

Kuluttajat ovat huolissaan, että heidän dataansa myydään kolmansille osapuolille (Strychartz & Duivenvoorde 2021, 6). Kuluttajille on hyväksyttävämpää, jos yritys suoraan hyödyntää dataa asiakassuhteessa eikä se mene kolmansille osapuolille (Spiekermann ym. 2015, 165). Yrityksille ongelmaksi on kuluttajien yksityisyyshuolien lisäksi noussut vaikeus luottaa kolmannen osapuolen dataan markkinoinnissa, sillä se ei ole aina todenmukaista tai ajantasaista, joten niiden tulisi pääasiassa tukeutua omiin tietokantoihinsa parhaan asiakaskokemuksen luomiseksi (Skiera 2022, 7).

2.2.3 Mobiilisovellukset

Nykyään verkkosivujen ja järjestelmien lisäksi yritykset keräävät dataa kuluttajista houkuttelemalla heitä ilmaisilla mobiilisovelluksilla. Yritykset tavoittelevat kilpailuetua niistä kerätyllä ajankohtaisella datalla. (Ezrachi & Stucke 2017, 159–160.) Personointi mobiilisovelluksissa on uusi ilmiö, jota ei ole laajasti tutkittu kuluttajien näkökulmasta. Mobiilisovellusten järjestelmät ovat haavoittuvaisia yksityisyysrikkomuksille, jonka vuoksi niitä on tutkittu yksityisyyden kontekstissa. Personointi mobiilisovellusten sisällössä ja käyttökokemuksessa on kuitenkin saanut kuluttajilta positiivisia reaktioita kasvattaen luottamusta ja uskollisuutta esimerkiksi hotellisovelluksissa, mutta on nostanut myös esille yksityisyyshuolia. Mobiililaitteen ponnahdusilmoitusten personointi on nostanut esiin enemmän yksityisyyshuolia ja vastareaktioita kuin personoitu mobiilisovellusten käyttökokemus, joka on kuluttajille hyväksyttävämpää. (Strycharz ym. 2018, 645.)

Mobiililaitteiden käytön lisääntyessä ja pilvipalveluiden lisääntyessä mobiilipilvi terminä tuli käyttöön. Mobiililaitteet ovat pääsyväline pilvipalveluihin, jossa data usein säilytetään. Mobiililaitteet voivat luoda yhteyksiä keskenään, jakaa tietoa keskenään ja olla samanaikaisesti yhteydessä pilvipalveluihin. Mobiilisovellukset usein säästävät kehityskustannuksissa, jotta ne saavat pidettyä matalat hinnat sovellusmarkkinoilla. Tämä johtaa siihen, että niiden dataturva on puutteellista, koska koodaus on tehty kiireellä. Mobiilisovelluksiin liittyviä riskejä ovat vakoilu, toisena henkilönä esiintyminen, sijainnin seuranta, palvelunesto sekä datan vioittuminen tai muokkaaminen. Nämä haitat esiintyvät myös tietokoneen käytössä, mutta niiden riski on korkea mobiilikäytössä hyökkäyksen helppouden vuoksi, mikä johtuu fyysisten suojausjärjestelmien puutteesta. (Geneiatakis ym. 16–22)

Koska mobiililaitteissa on jatkuvasti mikrofoni päällä, uusi markkinointikeino nimeltä *watermarking* (vesileimaus) on kehitetty yhdistämään markkinointi viestintävälineiden välillä. Televisiosta tai mainoksesta tuleva ääni lähettää signaalin mobiililaitteeseen, joka avaa mainoksen mobiililaitteella ponnahdusilmoituksena. Tämä on keino kerätä dataa kuluttajan ympäristöstä valvonnan avulla. Tämän markkinointikeinon uskotaan kuitenkin herättävän enemmän yksityisyyshuolia kuluttajassa kuin yksilöidyt mainokset, jotka on luotu verkkoseurannan perusteella. (Strycharz & Segijn 2024, 2.)

Sovelluskaupat, kuten Google Play Store ja iTunes, mahdollistavat käyttäjälle sovellusten lataamisen ilman muiden osapuolien väliintuloa ja tutkivat sovellukset mahdollisen haitallisen toiminnan varalta ennen julkaisua sovelluskaupassa. Ne eivät kuitenkaan kykene täysin estämään haittaohjelmia. Mobiilisovellukset hallitsevat kuluttajadataa, mikä tekee niistä mielenkiintoisen kohteen hyökkääjille. Esimerkiksi vakoilusovellukset voivat varastaa kuluttajien tietoja ja myydä niitä markkinointiyrityksille. Mobiilisovellukset voivat käyttää kuluttajadataa ominaisuuksien ja etujen tarjoamiseen kuluttajille, mutta on ollut tapauksia, kun tietoja on välitetty eteenpäin kuluttajan tietämättä. Esimerkiksi Twitter-sovellus (nykyään X) on lähettänyt tietoja kolmansille osapuolille. (Geneiatakis ym. 16–22.) Myös Uberia on syytetty siitä, että kuskit pääsevät näkemään akun tason potentiaalisilta asiakkailta, jolloin he tunnistavat asiakkaan tarpeen heidän palveluilleen (Strycharz & Duivenvoorde 2021, 8).

Yksityisyyshuolet nousevat mobiilisovellusten käytössä esiin, kun sovelluskehittäjä ei ole selkeästi ilmaissut kuluttajadatan käyttökohdetta. Yksityisyyshuolien syntyminen kuitenkin vaatii kuluttajalta digitaalista lukutaitoa. Tämän vuoksi henkilö, joka ei omaa teknisiä taitoja, ei luultavasti huolestu digitaalisista yksityisyysongelmista. (Silvestru ym. 2021, 665.)

Turvausmekanismit on luotu loppukäyttäjää varten, mutta usein loppukäyttäjä on heikoin lenkki turvallisuutta ajatellen, sillä käyttäjät eivät ymmärrä mobiilisovellusten turvallisuusriskejä tai tiedä, miten hallita yksityisyysasetuksiaan. Lisäksi ylimääräisten yksityisyysominaisuuksien nähdään häiritsevän käyttökokemusta. (Geneiatakis ym. 16–22.)

Kuva 2 Mobiilisovellukset jakavat tietoa kolmansille osapuolille (vpnMentor 2024)

2.3 Verkosta kerättävän kuluttajadatan hyödyntäminen markkinoinnissa

Kuluttajadatan käyttökohteet tuntuvat olevan rajattomat (Rao ym. 2015, 9). Dataa organisoimalla voidaan ennustaa kysyntää, tukea välitöntä päätöksentekoa ja parantaa teknologisia palveluita. Se myös mahdollistaa syvemmät asiakasyhteydet, asiakkaan elinkaaren pidentämisen, tuotekehityksen ja uusien strategioiden kehittymisen. Datamäärä verkossa on valtava, joten oikeanlaisen informaation tunnistaminen voi olla hankalaa. (Fyall, 2019, 460.) Tähän kaikkeen tarvitaan oikeanlaisia henkilöitä, jonka vuoksi dataanalyytikoiden palkkauksen uskottiin vuonna 2018 kasvavan 50 % seuraavan 3 vuoden aikana (Gerlick & Liozu 2020, 86–87).

Evästetietoihin ja verkkokäyttäytymiseen liittyviä tietoja käytetään psykografisen, käyttäytymiseen liittyvän ja ennustavan tiedon keräämiseen. Psykografisia tietoja ovat esimerkiksi asenteet, mielenkiinnon kohteet, arvot ja elämäntyyli. Sen selvittäminen, mitä asiakas pitää arvossa, auttaa ennustamaan ostokäyttäytymistä. Ennustava data yhdistää tietoja useista lähteistä, usein asiakkaan ostosuunnitelmien ennustamiseen lähitulevaisuudessa. (Rao ym. 2015, 5.) Ennustavan analytiikan laatu paranee koneoppimisen ja datamäärän kasvun myötä, mikä vaikuttaa datan hyödyntämiseen (Chapdelaine, 2020, 15).

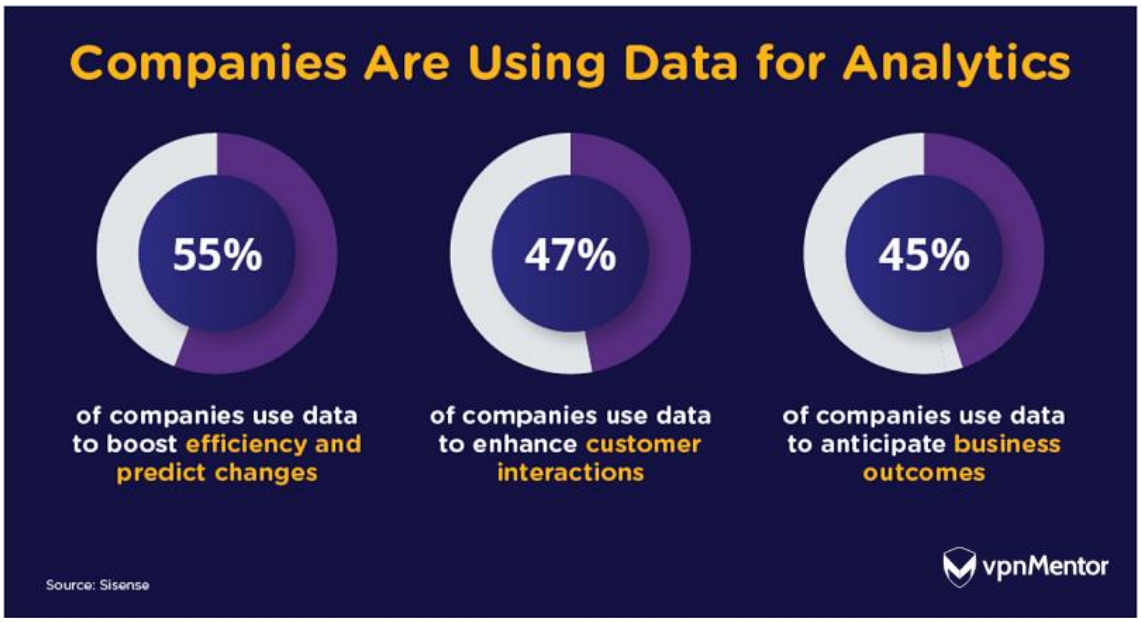
Datatalous mahdollistaa, että kuluttajille tarjotaan parempia tuotteita ja palveluita, kuten personalisointia, riskientunnistusta, kohdennettua markkinointia ja henkilön paikantamista, esimerkiksi hakukoneilla. Datatalous tarkoittaa, että kuluttajat tarjoavat henkilötietojansa yksityisen ja julkisen sektorin palveluntarjoajille vastaanottaessaan tuotteita tai palveluita niiltä. Yksityisen sektorin palveluntarjoajiin lukeutuvat muun muassa kivijalkaliikkeet, markkinoijat ja verkkosivut. Julkisen sektorin palveluntarjoajiin lukeutuvat muun muassa väestörekisterit, äänestäjien rekisteröintitietokannat, konkurssitietokannat ja keltaisten sivujen hakemistot. Yksityisiä tietokantoja ovat kyselyt, liiketoimet verkossa ja kivijalkaliikkeissä sekä toimet verkkosivuilla ja sosiaalisissa verkostoissa. (Rao ym. 2015, 1–2) Monilla toimialoilla, kuten supermarketeilla, lentoyhtiöillä ja luottokorttiyhtiöillä, on suuret tietokannat yksittäisten kuluttajien liiketoimista, ja ne ovat hyödyntäneet tietoja ostokäyttäytymisen seurantaan ja yksilöityjen tarjouksien lähettämiseen suoramarkkinoinnin keinoilla. (Acquisti & Varian 2005)

Datan avulla luodaan yksilöllisiä profiileja, joilla tutkitaan kuluttajien käytöstä ja pyritään vaikuttamaan siihen. Muun muassa mainosten kohdennus kuluttajille helpottuu. Lisäksi mainostajat tuottavat rahaa alustojen ylläpitäjille, kun kuluttajat klikkaavat mainoksia. Yritykset haluavat selvittää, mitä kuluttajat haluavat ostaa, millä hinnalla, milloin ja millä mainoksella tämä saadaan tapahtumaan. Datan kerääminen yksilöiltä myös auttaa kehittämään algoritmeja tunnistamaan käytösmalleja entistäkin paremmin. (Ezrachi & Stucke, 2016, 159–161.) Kuluttajan henkilötietojen avulla voidaan luoda profiili esimerkiksi ostovoimasta ja ostokäyttäytymisestä. Seurantaa tehdään esimerkiksi IP-osoitteen tai evästeiden avulla. (Chapdelaine 2020, 11.) Kuluttajien data nähdään hyödykkeenä, jonka takia on syntynyt ns. ekosysteemi, joka kerää, analysoi ja jakaa dataa. Syy miksi data nähdään arvokkaana, on sen mahdollisuus hyödyttää yrityksiä ja asiakkaita. Lisäksi data vähentää tarvetta tuotetutkimukselle, mahdollistaa personoinnin ja kohdistetun markkinoinnin, kuluttajien riskianalyysin ja matalammat transaktio- ja tutkimuskustannukset. (Acquisti ym. 2015, 1–2.)

Datan kerääminen kuluttajista vaikuttaa kasvavissa määrin markkinointiin. Yritykset käyttävät kuluttajadataa yhä enemmän tuotteiden ja palveluiden personointiin, myös hinnoittelussa. Personointi on yksilöllisten tuotteiden, palveluiden tai informaation tarjoamista. Se on laaja käsite, johon sisältyy esimerkiksi suosittelu, yksilöinti ja mukautuvat verkkosivut. Sitä käytetään verkossa pääosin verkkokaupassa. (Mulvenna ym. 2000, 122–125.) Kuluttajien asiakaskokemus verkkosivuilla paranee, kun heille suositellaan heitä kiinnostavia tuotteita verkossa heidän datansa perusteella (Adak ym. 2022, 70–81).

Yritykset kilpailevat keskenään datasta ja eniten dataa kerännyt yritys kasvattaa yrityksen valtaa markkinoilla (Ezrachi & Stucke, 2016, 171). Organisaatiot, jotka kykenevät auttamaan kuluttajia tiedonhaun ja päätöksenteon prosesseissa saavat varmemmin ostoja ja siten tuottavuus kasvaa (Ho & Kwok 2003). Totuudenmukainen informaatio kuluttajista on strategisesti tärkeää yrityksen toiminnalle. Se mahdollistaa esimerkiksi suoramarkkinoinnin ja asiakassuhteiden hallinnan. (Xie ym. 2006, 61.) Asiakkaan tunteminen mahdollistaa laadukkaammat palvelut, syvemmät suhteet asiakkaiden kanssa ja markkinointistrategian kehittämisen (Talón-Ballestero ym. 2018, 187–188).

Google on yksi suurimmista toimijoista, joka kerää kuluttajadataa yksilöityjen hakukonetulosten luomiseksi. Matkailualalla personoituja hakutuloksia luovat Booking.com, Expedia, Travelocity ja Trivago. Expedia ja Travelocity esimerkiksi ehdottavat asiakkaan aiempien verkkohakujen ja lempikohteiden perusteella matkapaketteja, hintavertailuja sekä nopean ja helpon tavan matkan suunnitteluun. (Lee & Cranage 2011, 988.)



Kuva 3 Yritykset käyttävät kuluttajadataa erilaisiin tarkoituksiin (vpnMentor 2024)

3 KULUTTAJAN YKSITYISYYS VERKKODATANKERÄYKSEN NÄKÖKULMASTA

3.1 Kuluttajan yksityisyys

Yksityisyys tarkoittaa vuorovaikutuksen hallintaa henkilön ja ulkopuolisen entiteetin välillä, jonka tarkoituksena on lisätä yksilön autonomiaa ja vähentää haavoittuvaisuutta (Mutimukwe ym. 2020, 2). Datankeräys koskettaa useaa yksityisyyteen liittyvää lakia ja asetusta, kuten kilpailuoikeutta, kilpailulainsäädäntöä, yksityisyyslakia, sopimuslakia, kuluttajansuojalakia ja syrjinnänvastaisia asetuksia. Näiden tarkoitus olisi suojella kuluttajan yksityisyyttä datankeräyksen vaaroilta. (Chapdelaine 2020, 3.) Kuluttajat luovuttavat dataa, jos näkevät hyödyn ylittävän koetun riskin datan luovuttamisessa. Yritysten tulee siis luoda ilmapiiri, jossa kuluttajilla on halukkuus luovuttaa tietojaan. (Culnan & Bies 2003, 327.) Usein verkkokäyttäjät pyrkivät pysymään anonyyminä (Gerlick & Liozu 2019, 9), vaikka 80 % suostuu luovuttamaan dataa anonyyminä tutkimustarkoituksiin (Gerlick & Liozu 2020, 92).

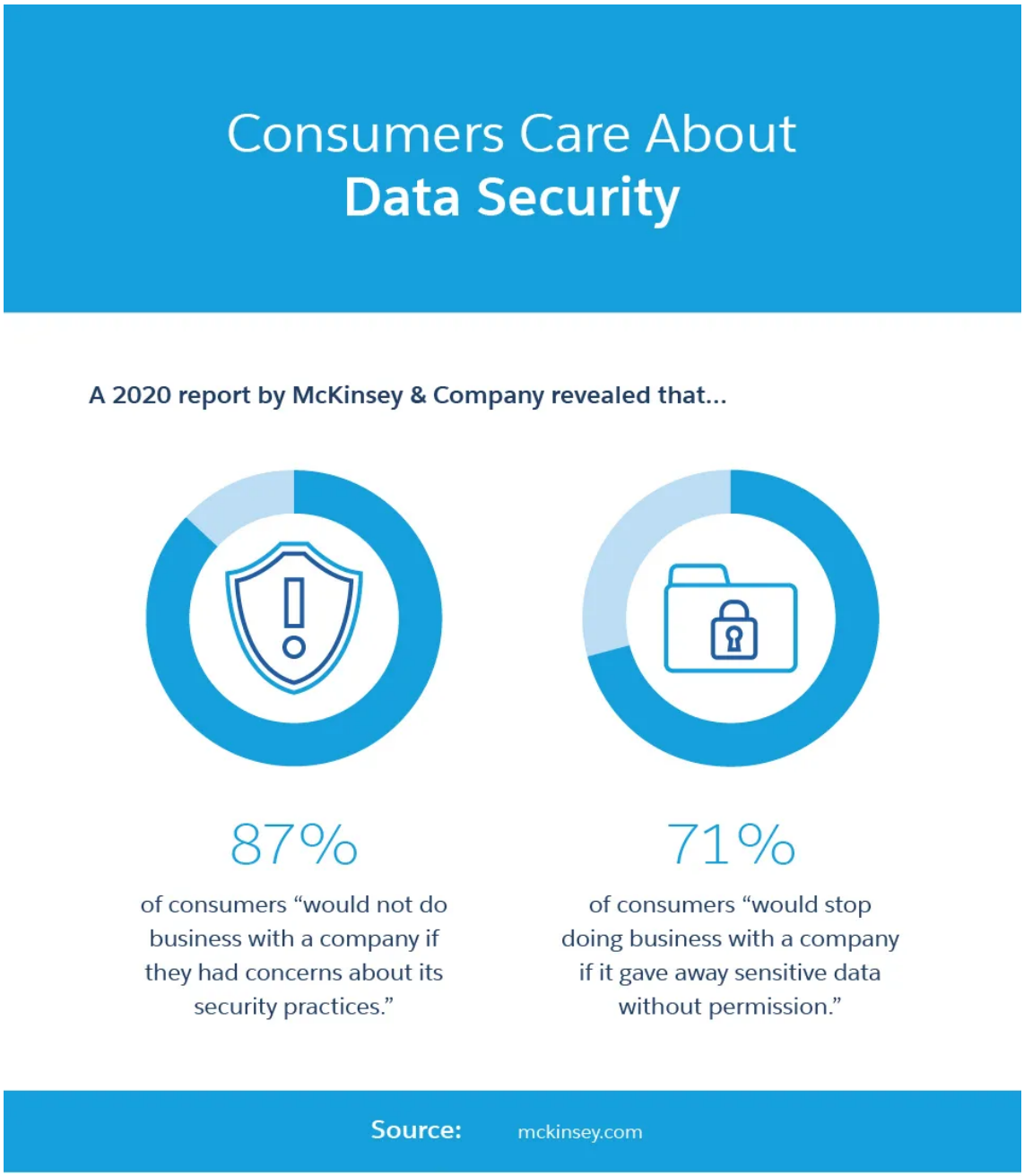
Datan jakaminen ei aina johda edistykseen, tehokkuuteen tai tasa-arvoon. Datan väärinkäytölle on paljon uhkia, joita ovat esimerkiksi taloudellinen ja sosiaalinen syrjintä, vaikutusvalta ja manipulointi, kiristäminen ja sensurointi. Kuitenkin sekä yritykset että kuluttajat voivat hyötyä datasta, analytiikkatyökaluista ja integroiduista datatietokannoista. Myös yhteiskunta laajemmin voi hyötyä niistä, esimerkiksi terveysalalla. (Acquisti 2015, 509.) Kuluttajille se on usein helpotus, ettei heistä tiedetä kaikkea ja että data ei ole aina todenmukaista (Rao ym. 2015, 7–9).

Mikäli yksityisyyden ympäristössä tapahtuu muutoksia, kuten valvontakameroiden asennus kuluttajan ympäristöön, yksityisyyshuolet nousevat usein pintaan. Muutoksiin kuitenkin sopeudutaan, joten ajan kanssa yksityisyyshuolet lievittyvät ja muuttumattomiin yksityisyyden puutteisiin totutaan. Yksityisyys on siis kontekstiriippuvaista: ihmisten käytös ja henkilökohtaiset rajat muuttuvat sen mukaan, kun teknologia kehittyy. (Acquisti 2015, 511–512.)

Culnan ja Bies (2003, 323–325) esittävät kolme näkökulmaa kuluttajan yksityisyyteen: yritysnäkökulman (engl. the corporate perspective), aktivistinäkökulman (engl. the activist perspective) ja keskustanäkökulman (engl. the centrist perspective). Ensimmäisen näkemyksen mukaan pääsyä kuluttajien tietoihin ei tule rajoittaa, koska se mahdollistaa yritysten toiminnan. Yritykset taas mahdollistavat yhteiskunnan kehityksen ja kasvun.

Toinen näkemys on, että vapaat markkinat ja teknologinen kehitys mahdollistaa, että tiedot voivat levitä kenen tahansa käyttöön, mikä vaarantaa oikeuden yksityisyydensuojaan ja aiheuttaa haittaa yhteiskunnalle.

Kolmas näkökulma on näiden välimaastossa. Sen mukaan kuluttajalla tulee olla mahdollisuus valita luovuttaako hän dataa, ja jos yrityksellä on vain kohtuullinen pääsy kuluttajan dataan, kuluttajalla on paremmat mahdollisuudet suojautua. Oikeudenmukaiset tietoturvakäytännöt tarjoavat kuluttajalle kontrollin tietojen keräämisestä ja käyttökohteesta. Ne luovat tasapainon yrityksen ja kuluttajan tarpeiden välillä. Kuitenkin eri maissa käytännöt vaihtelevat paikallisten normien ja lainsäädännön mukaan. (Culnan & Bies 2003, 323–330.)



Kuva 4 Kuluttajien yksityisyyshuolet (McKinsey 2021)

3.2 Kuluttajan yksityisyyshuolet

Yksityisyyshuolilla tarkoitetaan kuluttajan huolia datankeräyksen riskeistä (Gerlick & Liozu 2019, 3). Yksityisyyshuolet ovat yksilön huolia yksityisyyden menettämisestä, joka syntyy seurauksena tietojen luovuttamisesta toiselle osapuolelle, kuten organisaatiolle (Mutimukwe ym. 2020, 2). Huolia syntyy verkossa tapahtuvien yksityisyyden suojan loukkausten seurauksena. Niitä voivat olla esimerkiksi pyytämättömien sähköpostien

vastaanottaminen tai identiteettivarkaudet. (Awad & Krishnan 2006, 19.) Kuluttajia huolestuttaa, että heidän dataansa kerätään ilman lupaa ja ilman heidän tietoisuuttaan asiasta (Ho & Kwok 2003). Lisäksi kuluttajat eivät pidä datankeräyksestä, koska menettävät hallinnan seurauksista, mikä haittaa personoitua hinnoittelua organisaatioiden näkökulmasta (Buhalis & Amaranggana, 2015, 384). Yksityiskäytännöt usein lupaavat, että data pidetään turvassa, mutta usein niin pinnallisesti, etteivät ne lievitä kuluttajien yksityisyyshuolia (Solove 2003, 1258).

Datankeräys aiheuttaa huolia dataturvallisuudesta, datankeräyksen läpinäkyvyydestä ja profiilien todenmukaisuudesta. Läpinäkyvyyden lisäämiseksi jotkut yritykset antavat asiakkaille pääsyn dataprofiileihinsa. Kuluttajien nähtävillä olevissa yksilökohtaisissa dataprofiileissa on vain osa yrityksen keräämästä datasta. Joskus kuluttajalla on myös pääsy muokkaamaan tietoja. Yritykset voivat tarjota pääsyn tunnistautumisella kuluttajapuolelta tai palvelimen puolelta. Esimerkiksi Google, Yahoo ja BlueKai antavat kuluttajille pääsyn omiin tietoihinsa evästeiden avulla. (Rao ym. 2015, 1–2.)

3.3 Datankeräys ja sen potentiaaliset haitat kuluttajan näkökulmasta

Syitä, miksi datankeräys pelottaa kuluttajia ovat esimerkiksi maksutietojen varastaminen ja kyberrikollisuus (Victor ym. 2018, 5–9). Ongelma on, etteivät kuluttajat ole osallisia datansa käsittelyyn ja se kulkee huolettomasti ja suojaamatta. Se on haavoittuvainen virheille, väärinkäytölle ja vaaroille. (Solove 2003, 1258.)

Algoritmit eivät ole turvassa puolueellisilta, vääristyneiltä tai syrjiviltä ennusteilta, kolmansien osapuolien puuttumiselta ja vapaita markkinoita rikkovilta ja kilpailunvastaisilta sopimuksilta (Gerlick & Liozu 2019, 16). Järjestelmät hyödyntävät puutteellista dataa, jolloin on hankalaa saada oikeanlaisia hakutuloksia. Se siis pakottaa kuluttajia antamaan lisää dataa, jolloin kuluttaja saa parempia tuloksia ja käyttö on helpompaa. (Alatalo & Siponen 2001, 7–9.)

Kuluttaja ei halua luopua henkilökohtaisista tiedoistaan ja organisaatiot eivät halua huonoa imagoa tai negatiivista Word of Mouthia sosiaalisessa mediassa datankeräämisen ja hintasyrjinnän seurauksena. Yksityisyydensuojaa pidetään tärkeänä, mutta se ei tuo varmuutta siitä, pitävätkö organisaatiot kuluttajien tietoja turvassa. Kuluttajien tietoon on

tullut tapauksia, kun kuluttajadata on levinnyt vääriin käsiin. (Alatalo & Siponen 2001, 7–9.)

Esimerkiksi Vastaamon tietomurto vuonna 2020 on tuonut esiin, ettei henkilötietoja ole suojattu tarpeeksi hyvin yritysten toimesta. Tapauksessa pyydettiin lunnaita vuotaneista potilastiedoista. (Kortesoja 2022, 10.) Kortesoja (2022, 11–12) ehdottaa tietosuojaongelmiin yritysten ja virastojen tietoteknisen osaamisen parantamista, tietosuojasta huolehtimista, tehokkaampia resursseja kyberuhkien torjumiseen sekä tiukempaa lainsäädäntöä ja auditointia. Suomessa yritysten on laitonta kerätä dataa luvatta asiakkailta, sillä asiakas ei silloin pysty hallitsemaan henkilötietojaan. Tällainen yritystoiminta rikkoo oikeutta yksityisyydensuojaan. (Alatalo & Siponen 2001, 7.)

Yksityisyysrikkomukset aiheuttavat uhreille haittaa, joita voivat olla häpeä, henkinen kärsimys tai haitta yksilön maineelle. Perinteinen tapa ymmärtää yksityisyysrikkomuksia on, että vain edellä mainittujen haittojen esiintyessä rikkomus on tapahtunut. Tämä ajatus on ollut voimassa 1890-luvusta lähtien. Kuitenkin nykypäivän informaatioyhteiskunnassa kyseinen ajatus on vanhentunut. (Solove 2003, 1228.)

FBI:n mukaan identiteettivarkaus on nopeimmin kasvava talousrikos. (Solove 2003, 1244). Identiteettivarkaat hyödyntävät arkkitehtuuria, joka ei suojaa kuluttajadataa. Yritysten luomat digitaaliset asiakirjat kuluttajista ovat varkaiden käytettävissä, manipuloitavissa ja saastutettavissa. Sosiaaliturvatunnukset ovat arvokasta informaatiota identiteettivarkaille, koska ne mahdollistavat pääsyn muuhun tietoon. Informaatiovirtojen arkkitehtuuri tulee suunnitella uudestaan identiteettivarkauksien estämiseksi. Yksi ehdotus on tunnistautumistavan uudistaminen sosiaaliturvatunnuksesta esimerkiksi fyysisiin ominaisuuksiin, kuten sormenjälkeen tai silmään, jolloin varkaan on hankalampi varastaa. (Solove 2003, 1251–1262.)

4 RATKAISUJA KULUTTAJAN YKSITYISYYDEN TURVAAMISEEN DATANKERÄYKSESSÄ

4.1 EU:n yleinen tietosuoja-asetus

Lainsäädännöllä on suuri rooli kuluttajadatan turvaamisessa. (Solove 2003, 1228) EU:n yleistä tietosuoja-asetusta kutsutaan myös nimellä GDPR, joka tulee sanoista *General Data Protection Regulation*. Se on EU:n vuonna 2018 voimaan astunut yleinen tietosuoja-asetus, joka käsittelee henkilötietojen suojausta. (Tietosuojavaltuutetun toimisto.) Yleinen tietosuoja-asetus mahdollistaa, että yksityishenkilöllä on helpommin pääsy tarkastelemaan ja hallitsemaan omaa dataansa ja estää datankäyttö luvatta esimerkiksi profilointiin tai yksilöintiin. Se myös mahdollistaa datan siirtämisen palvelusta toiseen. (Consilium 2022.) Yleiseen tietosuoja-asetukseen, kuten moniin muihinkin tietosuojalakeihin, sisältyy oikeus tulla unohdetuksi eli saada tietonsa poistetuksi verkkosivuilta (Skiera 2022, 17).

Yleisen tietosuoja-asetuksen tarkoituksena on asettaa korkeat standardit EU:n alueella kuluttajadatan keräykselle ja prosessoinnille. Sen tavoitteena on vahvistaa yksilön hallintaa verkkodatan keräyksessä. Sen vaikutukset yltävät datan keräystapoihin, kerätyn datan sisältöön ja siihen, kuinka kuluttajille kerrotaan keräystavoista. (Strycharz & Segijn 2024, 2–3.) EU:n tietosuojalakia on kuitenkin kritisoitu siitä, että se jättää paljon tilaa datan käsittelylle personoitua markkinointiviestintää varten, varsinkin jos kuluttaja on hyväksynyt datankäsittelyn (Strycharz & Duivenvoorde 2021, 9).

Yleinen tietosuoja-asetus pyrkii tietoturvan ja yksityisyyden yhtenäistämiseen EU:n alueella, ja jokaisen yrityksen tulee seurata lainsäädäntöä tarjoamalla vaadittavat oikeudet, käyttöehdot tai varotoimet jokaiselle heidän palveluitaan käyttävälle eurooppalaiselle tai lopettaa toimintansa EU:n alueella. Mikäli lainsäädäntöä ei noudateta, se voi johtaa suuriin sakkoihin. (Müller ym. 2019, 151–159.) EU:n yleisen tietosuoja-asetuksen rikkominen voi johtaa sakkoihin suuruudeltaan 4 % yrityksen liikevoitosta tai 20 miljoonaa euroa, riippuen kumpi summa on suurempi. (Skiera 2022, 17.)

Osoittaakseen tarpeen datan prosessoinnille yrityksen tulee osoittaa, että heillä on siihen todellinen tarve, joka ei vaaranna kuluttajan vapauksia tai oikeuksia. Koska EU:n yleinen tietosuoja-asetus ja uusi ePrivacy-asetus rajoittavat datankeräystä, yrityksen tulee osoittaa oikeusperuste, jossa tarve datanprosessointiin ylittää kuluttajan tarpeen estää hänen datansa prosessointi. Kuluttajan lailliseen suostumukseen tarvitaan kuluttajan

vapaaehtoinen, tietoinen ja yksiselitteinen hyväksyntä yhteen tai useampaan selkeästi ilmaistuun datan prosessointitarkoitukseen. (Skiera 2022, 16.)

4.2 Yksityisyyskäytännöt

Yksityisyyskäytäntöjä on Zengin ym. (2022) mukaan kahta tyyppiä. Yksityisyyskäytännöt voivat korostaa yksityisyydensuojaa, jolloin kuluttajien näkökulmasta riskit kuluttajadatan luovuttamisesta korostuvat. Tämänlaisessa yksityisyyskäytännössä kerrotaan, miltä riskeiltä kuluttajadataa suojataan. Tämä vaikuttaa negatiivisesti kuluttajan ostohalukkuuteen. Yksityisyyskäytännöt voivat myös korostaa personointia, jolloin kuluttajille esitetään hyödyt kuluttajadatan luovuttamisesta kertomalla mihin heidän dataansa käytetään. Tämänlainen yksityisyyskäytäntö nostaa kuluttajan ostohalukkuutta. (Zeng ym. 2022, 781–782.) Kuluttajat ovat haavoittuvaisia ja epätietoisia yksityisyyskäytännöistä, joten käytäntöjen tulisi suojella kuluttajia. Tällä hetkellä yrityksillä on valta-asema kuluttajadatan ja kuluttajan yksityisyyden hallinnassa. (Acquisti 2015, 514.)

Yksityisyyskäytäntöjä liitetään usein personoituihin markkinointikampanjoihin, jotta organisaatiot välttyvät ongelmilta hyödyntäessään kuluttajien dataa. Yksityisyyskäytäntöjen avulla voidaan välttää kuluttajan tietojen leviämistä. Yksityisyyskäytäntöjen tärkeys nousee esille siinä, että ne voivat kasvattaa asiakkaiden brändiuskollisuutta ja niiden puutteellisuus voi johtaa asiakkaiden menettämiseen. (Zeng ym. 2022, 782–783.)

Dataa analysoivat yritykset vastaanottavat dataa, kun yksityishenkilöt hyväksyvät käyttöehtoja sivustoilla (Chapdelaine 2020, 11). Kuluttajat kuitenkin harvemmin lukevat sivustojen yksityisyyskäytäntöjä (Awad & Krishnan 2006, 19–25), joten luvallisuus on kyseenalaista. Etenkin Facebookia on kritisoitu tästä, sillä sen yksityisyyskäytäntöjä on pidetty harhaanjohtavana. (Chapdelaine 2020, 11) Sellaisia yksityisyyskäytäntöjä tulisi asettaa, joissa kuluttajien tietoista päätöksentekoa ei tarvita. Käytäntöjen tulisi olla sisäänrakennettuna oikeudenmukaisissa tietokäytännöissä. (Acquisti 2015, 514.)

Yksityisyyskäytännöistä välittävät kuluttajat vaativat usein personoitujen tuotteiden ja palveluiden datantarpeen ilmoittamista läpinäkyvällä tavalla. He haluavat tietää, mitä dataa heiltä kerätään ja mihin tarkoitukseen. (Awad & Krishnan 2006, 19.) Yksityisyyskäytännöt verkkosivuilla ovat usein pakollisia, myös alueilla, joissa Omnibus-lainsäädäntöä ei ole käytössä (Kobsa 2007, 649).

Organisaatioiden yksityisyyskäytäntöjen toimivuus vaikuttaa kuluttajien halukkuuteen luovuttaa tietoa, kuluttajan kokemukseen yksityisyytensä hallinnasta ja uskomukseen,

että organisaatioiden itsesääntely on toimiva keino yksityisyyden suojaamiseen verkkoympäristössä. Kuluttajan informoiminen käytännöistä lisää kuluttajien kokemaa hallinnan tunnetta omasta datastaan ja luottamusta organisaatioiden tietosuojakäytäntöihin. (Mutimukwe ym. 2020, 10–11)

4.3 Opt-outmahdollisuus

Yksityisyyden lainsäädäntöön voi sisältyä opt-in ja opt-outvaihtoehdot. Opt-in tarkoittaa luvan saamista kuluttajalta ennen datankeräystä ja opt-out kieltäytymistä esimerkiksi datan keräyksestä ja prosessoinnista. (Kobsa 2007, 647–648.) Dataa keräävien yritysten tulee olla läpinäkyviä ja tarjota kuluttajalle tietoa datankeräysprosessista. Yritykset ovat tämän lisäksi mahdollistaneet kuluttajille datankeräyksen suostumuksesta vetäytymisen opt-outmahdollisuudella. (Strycharz ym. 2019, 1.)

Anderson ym. (2022, 2086–2087) ehdottavat ratkaisuksi yksityisyyshuoliin, että kuluttajille tulee tarjota mahdollisuus valita, haluavatko he yksilöllisiä tarjouksia sekä milloin heidän dataansa hyödynnetään ja mihin. Tämä tukee EU:n yksityisyyslainsäädäntöä ja hyödyttää kuluttajaa, koska hinnat putoavat, kun osa kuluttajista ei hyväksy yksilöityjä tarjouksia. (Anderson ym. 2022, 2086–2087) Myös Eurooppa-neuvoston tietosuojalainsäädäntö tukee tätä ajatusta (Eurooppa-neuvosto 2023).

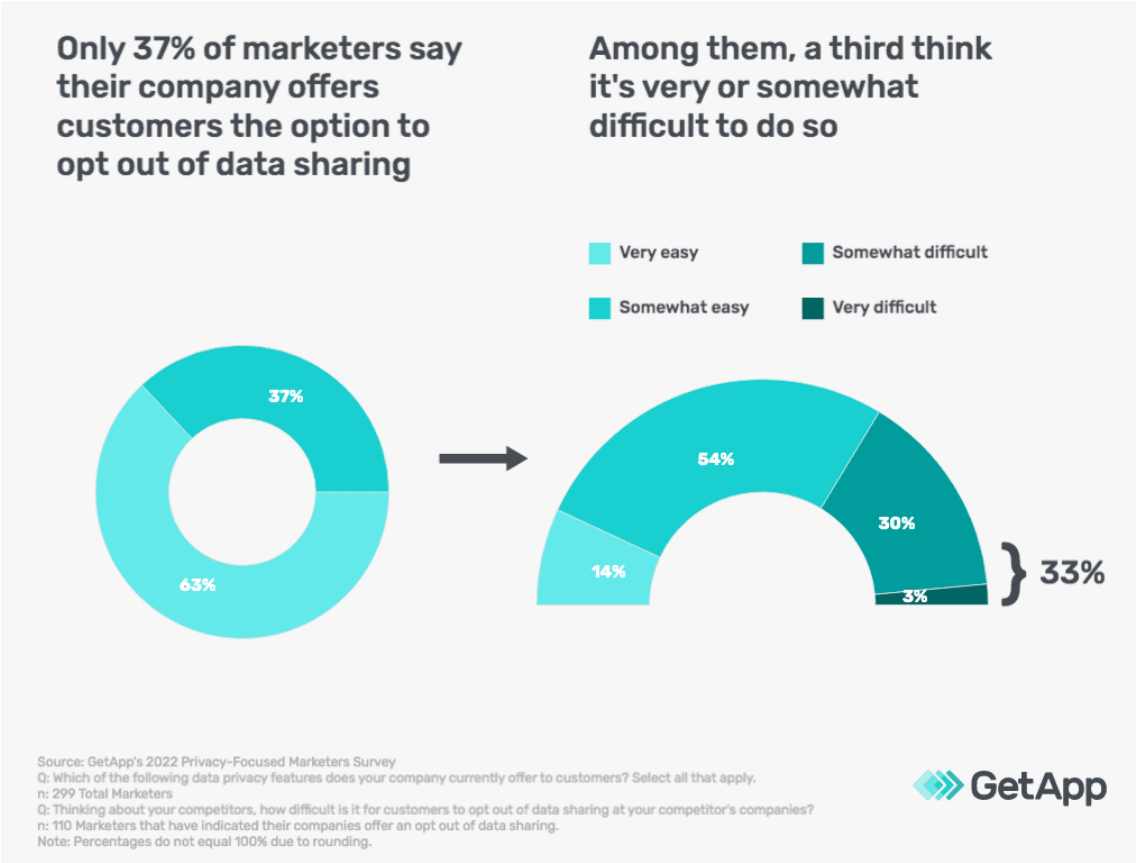
Nykypäivänä kuluttajat kohtaavat jatkuvasti personoitua digitaalista mainontaa heidän datansa perusteella. EU:n yleisen tietosuoja-asetuksen yhtenä tarkoituksena on kuluttajien voimaannuttaminen, jota varten organisaatioiden tulee tarjota kuluttajille teknistä informaatiota datankeräyksestä ja sen prosessoinnista sekä tietoja kuluttajan oikeuksista. Kuluttajan voimaannuttaminen siis pyrkii antamaan kuluttajalle työkalut kuluttajadatansa hallintaan lainsäädännön ja säädösten lisäksi. Opt-outmahdollisuus jää kuluttajalta kuitenkin usein käyttämättä. (Strycharz ym. 2019, 1–2.)

Personointi on nähty yhtenä kyseenalaisimmista markkinoinnin keinoina, koska se tekee kuluttajat epämukavaksi. Kuitenkin personoinnin antama sisältö voidaan nähdä relevanttina ja hyödyllisenä, mutta se herättää yksityisyyshuolia kuluttajassa. (Strycharz ym. 2019, 2.) Yritysten pyrkimyksessä toimia läpinäkyvällä tavalla monilla verkkosivuilla personoidussa mainoksessa voi klikata pientä mainosten valintanappia, josta pääsee sivulle, joka avaa datankeräys- ja opt-outvaihtoehdot. Tämä on tehokasta, mutta monimutkaista ja vaativaa kuluttajalle. Googlen käyttämä yksinkertaisempi vaihtoehto läpinäkyvyyteen on sivusto, jossa on selkeä kuvaus datankeräyksestä ja -käytöstä sekä mahdollisuus opt-outvaihtoehtoon, jolla käyttäjä voi kieltäytyä personoinnista

kokonaan. (Strycharz ym. 2019, 2.) Läpinäkyvyyttä vaativat kuluttajat eivät Awadin ja Krishnanin (2006, 13) tutkimuksen mukaan ole halukkaita joutumaan yritysten profiloitavaksi. Läpinäkyvyys on yksi keskeisimpiä tekijöitä, joka vaikuttaa kuluttajien personoinnin hyväksymiseen. Kuluttajat ovat myönteisempiä läpinäkyviä toimintoja kohtaan. (Rott ym. 2022, 21.)

Opt-outhallintatoimet eivät kuitenkaan ole tyypillisiä. Esimerkiksi vuonna 2017 yksittäisiä mainoksia estettiin vain noin 5 miljardia kertaa, mikä on suhteessa mainosten määrään hyvin vähän, koska Google esittää päivässä noin 24 miljardia mainosta. Matalien opt-outlukujen syynä voi olla kuluttajien tietämättömyys siitä, miten hallita personointia tai tietämättömyys personoinnista. Teknisen osaamisen puute voi siis vaikuttaa opt-outvalintoihin. Lisäksi vain 9 % kuluttajista tietää opt-outvaihtoehdosta. (Strycharz ym. 2019, 2.)

Opt-outvaihtoehdon hyödyntämiseen liittyy myös kuluttajan motivaatio suojautua datankeräykseltä. Yksilön motivaatio suojella itseään datankeräyksen uhkilta syntyy kahdesta kognitiivisesta prosessista: riskin ja selviytymisen arvioinnista. Riskin arvioinnissa tieto laukaisee itsesuojelun, kun kuluttaja arvioi riskin vakavuutta ja todennäköisyyttä. Selviytymisen arvioinnissa kuluttaja arvioi kykyään suojella itseään haitalta sekä suojan tehokkuutta. Tämän teorian perusteella kuluttajan yksityisyyshuolet laukaisee tekninen tietämys yksityisyydestä, ja se motivoi kuluttajaa valitsemaan opt-outvaihtoehdon. Tässä vaikuttaa enemmän kuluttajan oletus suojautumistaidoistaan kuin todelliset taidot. (Strycharz ym. 2019, 4.)



Kuva 5 Tilasto sivustojen opt-outvaihtoehdoista (GetApp 2022)

4.4 Hallinnollinen ja itsehallinnollinen sääntely

Yli neljässäkymmenessä maassa on yksityisyyslakeja. Näiden lisäksi tai niiden tilalla voi olla käytössä itsesääntelyä koskien yksityisyydensuojaa. Se tarkoittaa monissa organisaatioissa käytössä olevia sisäisiä suuntaviivoja kuluttajadatan käsittelyä varten. Monet toimialajärjestöt ovat myös kehittäneet yksityiskäytäntöjä, joiden mukaan järjestöihin kuuluvien organisaatioiden tulee toimia. Sekä yritysten että järjestöjen itsesääntely, kuten niiden yksityisyyskäytännöt, vaikuttavat personointijärjestelmien tavoitteisiin ja toimintatapoihin. (Kobsa 2007, 647–649.)

Culnan ja Bies (2003, 332) ehdottavat yksityisyysongelmien ratkaisuksi alan itsesääntelyä. Toimialakohtaiset yksityisyyshuolet, -lainsäädännöt ja -normit sekä yrityskohtaiset yksityisyyskäytännöt vaikuttavat verkossa kuluttajan kohtaamiin käyttöjärjestelmiin (Kobsa 2007, 145).

Useilla valtioilla ja hallinnollisilla alueilla on yksityisyyttä säätelevää lainsäädäntöä, joka EU:ssa on GDPR. Sen taustalla on Saksassa syntynyt omnibus-lainsäädäntö. (Schwartz 2009, 908.) Useat organisaatiot ja toimialat ovat kuitenkin lainsäädännön lisäksi tai sen

sijaan ottaneet käyttöön oman normiston itsesääntelyä varten. Nämä pohjautuvat usein abstrakteihin periaatteisiin koskien reiluja käytäntöjä kuluttajadatan käsittelyssä. (Kobsa 2007, 628–670.)

Keskustelua on käyty siitä, onko hallinnollinen sääntely vai itsesääntely paras ratkaisu kuluttajien tietoturvallisuuden varmistamiseen. Aikaisemmin datan leviämisestä ei ole tarvinnut ilmoittaa kuluttajille elleivät he itse kysy asiasta, mikä viittaa itsesääntelyn tehottomuuteen. Tutkimukset osoittavat, että kustannukset tietoturva- ja datasuojarikkomusten ilmoittamisesta ovat vähäpätöiset. Vaikka yritysten tuleekin nykypäivänä raportoida datahyökkäyksistä hallinnollisen sääntelyn seurauksena, se ei silti poista datavarkauden riskiä kokonaan. (Gerlick & Liozu 2020, 90.)

Useissa maissa kuluttajadatan käyttöä ja siirtoa hallinnollisten alueiden välillä säädellään tarkasti. Sääntely jättää vähän tilaa neuvottelulle, joten osa yrityksistä toimii harmaalla alueella. Jotkut yritykset hyväksikäyttävät sääntelyn aukkoja datan myynnissä. (Spiekermann ym. 2015, 162.)

Rubin ja Lenard (2002, Gerlick ja Liozu 2020 mukaan) vaativat organisaatioille itsesääntelyä, koska hallinnollisesta sääntelystä aiheutuisi aiheettoman suuria kustannuksia. EU:ssa on puututtu datankeräykseen vuoden 2018 yleisellä tietosuoja-asetuksella (GDPR), jolla vaaditaan yksityishenkilön suostumusta datan keräykseen ja jota voidaan tehdä vain hyväksyttävästä syystä. Asetus puuttuu myös EU:n ulkopuolisten yritysten toimintaan, mikäli ne keräävät EU:n kansalaisilta dataa. (Gerlick & Liozu, 2020, 90.)

4.5 Kryptografiset salauskeinot

Kryptografia tarjoaa eri tason suojausta ja turvaa verkossa. Kryptografialla voidaan varmistaa dataturvallisuus avaimilla, jotka todentavat käyttäjän ja estävät käyttöoikeuden. (Felici 2013, 70–86.) Kryptografiaa voitaisiin käyttää datan suojaamisen sijaan luotetun alustan tai ohjelmiston suojaamiseen. Tämä käytönvalvonnan hyödyntäminen pääsynhallinnan sijaan voi aiheuttaa organisaatiolle uusia haasteita, joita voivat olla luottamussuhteet yritysten välillä, toimitusketjun turvallisuus, prosessit tehokkaaseen valvontaan ja seuraamukset väärinkäytöksistä. (Spiekermann ym. 2015, 164.)

Onnistuneet suojausmenetelmät pyrkivät kolmeen asiaan: luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuus on pyrkimystä estää luvaton pääsy tietoihin yksilöiden tai järjestelmien toimesta. Datan eheys tarkoittaa, että data pysyy täsmällisenä ja

johdonmukaisena sen elinkaaren aikana. Saatavuus tarkoittaa kykyä käyttää haluttua tietoa tai resurssia. (Geneiatakis ym. 24.)

On olemassa työkaluja ja metodeja järjestelmän turvaamiseen, käyttäjän tunnistamiseen, todentamiseen, pääsynhallintaan ja salaukseen, joita voidaan käyttää käyttäjämallinnuksessa. Käyttäjämallinnusjärjestelmät nojaavat käyttäjäystävälliseen suunnitteluun ja niiden avulla voidaan kerätä, säilyttää ja hyödyntää kuluttajadataa useissa kanavissa. (Kobsa 2007, 136–154) Kuitenkaan eri lähteistä kerättyä dataa ei saa yksityisyyslainsäädännön mukaan yhdistää (Kobsa 2007, 648–649).

Yksityisyydensuojajärjestelmät on erotettu yksityisyyskäytännöistä. Yksityisyyskäytännöt voivat näkyä yrityksessä esimerkiksi tekstidokumenttina. Yksityisyyskäytäntöjen hallinta yksityisyydensuojajärjestelmän avulla on vaikeaa, etenkin kun muutoksia täytyy tehdä, sillä muutoksilla voi olla laaja vaikutus nykyiseen järjestelmään. Muutosten tekeminen suojausjärjestelmään on kallista ja kaikkien vaadittavien yksityisyyskäytäntöjen toteutuminen voi olla vaikea todentaa. (Bezzi 2013, 55–66.)

Yksityisyyttä parantavia teknologioita voitaisiin hyödyntää kuluttajadatan markkinoilla. Datan minimointiin käytettyjä metodeja voidaan esimerkiksi käyttää pääsynhallinnan välineenä. Käytäntöjä voitaisiin sitten koodata yksityisyyskäytäntöihin käytettyyn kieleen. Kehitteillä on uusia salauskeinoja, mutta ne ovat vielä tehottomia suuren henkilötietomäärän salaukseen. Kryptografian ongelmien kiertämiseen voitaisiin salata luotetun alustan ja järjestelmän toimivuus henkilödatan sijaan. Yritykset eivät kuitenkaan halua ottaa käyttöön käyttöoikeuksien hallintaa suojaavia DRM-teknologioita ilman kannustinta. Jos datasta tehtäisiin rahallinen hyödyke ja datan kohteille tulisi antaa korvausta, datayritykset pyrkisivät saamaan rahansa muualta. (Spiekermann ym. 2015, 163–164.)

Kyberturvallisuuskeskuksen mukaan yritysten tulee sopia internetpalveluntarjoajan kanssa palvelunestohyökkäysten torjuntakeinoista. Hyökkäyksen kohteena voi olla esimerkiksi organisaation henkilötiedot tai julkinen verkkosivusto. Keinoja suojautumiseen ovat esimerkiksi haavoittuvien järjestelmien päivitys ja ymmärrys tietotekniikasta, kuten siitä, kuka on palvelun omistaja, kenellä on pääsy tietoihin ja mitkä järjestelmät ovat yhteydessä toisiinsa. Toimenpiteillä voidaan varmistaa järjestelmien ja verkkosivujen toimivuuden varmistaminen kaikissa tilanteissa. (Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 8–11)

Suuri määrä kerättyä dataa voi mahdollistaa kyberturvallisuusrikkomukset, varsinkin jos data on tunnistettavissa tietyn yksilön dataksi tai jos se sisältää maksutietoja. Estääkseen

datan vaarantumisen, organisaatioiden tulee turvata data teknologian ja organisaatioprosessien avulla. Tämä ei kuitenkaan poista riskiä täysin. (Acquisti ym. 2015, 1–2.) Kyberrikokset voivat tuhota yrityksen imagon tai jopa koko alan imagon. Kyberrikoksista huolimatta yksityisyydensuojassa on tapahtunut kehitystä. Kehitystä on tapahtunut myös datamarkkinoilla, sillä data nähdään rahanarvoisena. (Acquisti ym. 2015, 2.) Organisaatiossa täytyy ymmärtää yksityisyysuhat, arvioida ne ja kommunikoida johdon, asiantuntijoiden ja hallituksen välillä. Organisaatiossa tulee asettaa kyberturvallisuus tavoitteisiin ja rakentaa organisaatiokulttuuri sen ympärille. (Kyberturvallisuus ja yrityksen hallituksen vastuu 2020, 18–25.)

5 JOHTOPÄÄTÖKSET

Tämän tutkielman tarkoituksena oli selvittää, miten organisaatiot voivat suojata kuluttajien yksityisyyttä verkosta kerätyssä kuluttajadatassa. Tutkimusongelma jakautui kahteen osaongelmaan. Ensimmäinen osaongelma oli, minkälaista dataa kuluttajista kerätään verkosta. Kuluttajadataa voidaan kerätä evästeiden avulla, jotka tallentavat kuluttajan tietoja verkkovierailun aikana seuraavaa vierailukertaa varten. Evästeiden käytössä organisaation tulisi kuitenkin toimia läpinäkyvällä tavalla ja mahdollistaa asiakkaalle evästeiden poistamisen, jos ei halua tulla tunnistetuksi.

Kolmannen osapuolen data mahdollistaa dataprofiilien luomisen kuluttajasta sekä katkeamattoman sarjan dataa asiakkaan toiminnasta, sillä dataa vastaanotetaan useasta lähteestä. Tämä vaatii yhteistyötä eri toimijoiden välillä. Tämän keräystavan hyödyt kuitenkin harvoin kattavat kustannuksia, joten organisaatioiden tulisi pääasiassa turvautua itsekerättyyn kuluttajadataan.

Mobiilisovellukset mahdollistavat myös kuluttajadatan keräyksen helposti tarjoamalla ilmaista palvelua kuluttajalle. Tämä keräystapa kuitenkin vaarantaa keräystavoista eniten kuluttajan yksityisyyden, sillä mobiilisovellukset ovat alttiita yksityisyysrikkomuksille. Kuluttajista kerättyä dataa käytetään lukuisiin markkinoinnin tarkoituksiin, kuten dataprofiileihin, personointiin ja asiakassuhteiden hallintaan. Kuluttajan yksityisyyshuolet kuitenkin nousevat pintaan datankeräyksen seurauksena.

Toinen osaongelma oli, mitä keinoja organisaatioilla on suojata kuluttajien yksityisyyttä verkkodatassa. Alatalo ja Siponen (2001, 6–7) ehdottavat, että yritykset noudattaisivat seuraavia ohjeita: Anna kuluttajalle päätösvalta tiedoistaan ja siitä, mitä tietoja hän haluaa luovuttaa. Älä luovuta tai muulla tavoin vaaranna datan joutumista kolmansille osapuolille luvatta. Kunnioita kuluttajan päätöstä siitä, mitä palveluita tai alustoja hän haluaa käyttää. Kuluttajien tulee olla samanarvoisia yksityisyyspreferensseistä huolimatta. Palveluiden käytön tulee olla helppoa. Yksityisyyspreferenssien ei tule heikentää palvelun käytön helppoutta. Nämä ohjeet tulivat myös tutkielmassa esille useiden lähteiden kautta.

Organisaatioiden tulisi lisätä läpinäkyvyyttä datan jakamisesta, jolloin kuluttajat voivat paremmin hallita datansa käyttöä ja luotetuilta tahoilta vaaditaan vastuuta tiedonhallinnasta. Läpinäkyvä liiketoimintamalli datankäsittelyssä auttaa välttämään laillisia ongelmia. Sen lisäksi taloudelliset, sosiaaliset ja teknologiset aspektit järjestyisivät ajan myötä, kun läpinäkyvyys otetaan organisaatioissa käyttöön. (Spiekermann ym. 2015, 165.)

Tutkielma tuottaa yrityksille hyödyllistä tietoa kuluttajadatan suojauksesta. EU:n yleinen tietosuoja-asetus pyrkii tietoturvan yhtenäistämiseen Euroopan alueella, mutta jättää kuitenkin paljon tilaa datan käsittelylle ja yksityisyysrikkomuksille. Tämän vuoksi yritys voi ottaa sen ohella käyttöön itsehallinnollisen sääntelyn keinoja, joilla turvata kuluttajadata, koska suojattomuus voi johtaa asiakkaiden menettämiseen. Itsesääntelyä on ehdotettu kustannusten säästämiseksi hallinnollisessa sääntelyssä, mutta se nähdään osittain tehottomana.

Organisaatioiden tulisi tarjota palveluitaan mahdollisimman pienellä määrällä kuluttajadataa ja esittää verkkosivuillaan selkeät yksityisyyskäytännöt. Selkeän suostumuksen saaminen kuluttajadatan keräykseen verkossa on ehdotonta, minkä vuoksi verkkosivustojen tulee tarjota myös opt-outvaihtoehto.

6 YHTEENVETO JA EHDOTUS JATKOTUTKIMUKSELLE

Tutkielmassa käsiteltiin verkosta kerättyä kuluttajadataa ja sen keräystapoja, mihin organisaatiot hyödyntävät kuluttajadataa ja miten sitä voidaan suojata. Tutkielmassa tuotiin esille kuluttajadatan keskeisimpiä keräystapoja ja kuluttajien yksityisyyshuolia verkkodatankeräykseen liittyen. Tärkeimpänä tutkielmassa nousi esille kuluttajadatan suojaustavat. Niitä ovat lainsäädännön seuraaminen ja läpinäkyvyys, yksityisyyskäytäntöjen esittäminen verkkosivuilla, mieluiten personointia korostaen, opt-outmahdollisuuden tarjoaminen kuluttajalle, itsesääntely ja kryptografiset salauskeinot. Tärkeää kuluttajadatan suojauksessa on kunnioittaa kuluttajan oikeutta yksityisyyteen ja tarvittavien mahdollisuuksien tarjoaminen datankeräyksestä kieltäytymiseen.

Myöhemmässä tutkimuksessa voisi liittää datan matkailualaan, joka oli tutkielman alkuperäinen suunnitelma. Matkailualan palveluntarjoajat hyötyisivät tutkimuksesta, jos ne löytäisivät keinon kerätä kuluttajadataa kuitenkaan menettämättä mainettaan kuluttajien keskuudessa. Myöhempi tutkimus voisi myös syventyä järjestelmiin, jotka keräävät ja järjestelevät dataa. Paneuduin yksityisyyshuoliin vain verkkoympäristössä, koska verkkoympäristö on nykypäivänä keskeisemmässä roolissa, mutta niitä voisi tutkia myös verkkoympäristön ulkopuolella. Datankeräystä personointitarkoitusta varten on tutkittu rajallisesti, koska personointi on uusi aihe, joten sitä voisi tutkia jatkossa.

LÄHTEET

Acquisti, Alessandro – Brandimarte, Laura – Loewenstein, George (2015) Privacy and human behavior in the age of information. *Science (American Association for the Advancement of Science*, Vol. 347, 509–514.

Acquisti, Alessandro - Varian, Hal (2005) Conditioning prices on purchase history. *Marketing Science*, Vol. 24(3), 367–381.

Adak, Tahir Enes - Sahin, Yunus – Zaval, Mounes – Aktas, Mehmet S. (2022) Methodology for product recommendation based on user-system interaction data: A case study on computer systems e-commerce web site. *Computational Science and Its Applications – ICCSA 2022 Workshops*, 70–81. Malaga, Spain.

Alatalo, Toni – Siponen, Mikko (2001) Addressing the personalization paradox in the development of electronic commerce systems. Department of Information Processing Science. University of Oulu, Finland.

Anderson, Simon – Baik, Alicia – Larson, Nathan (2023) Price Discrimination in the information age: Prices, poaching, and privacy with personalized targeted discounts. *The Review of Economic Studies*, Vol. 90(5), 2085–2115.

Awad, Naveen Farag – 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.

Blasco-Arcas, Lorena – Meg Lee, Hsin-Hsuan – Kastanakis, Minas N. – Alcañiz, Mariano – Reyes-Menendez, Ana (2022) The role of consumer data in marketing: A research agenda. *Journal of Business Research*, Vol. 146, 436–452.

Buhalis, Dimitrios – Amaranggana, Aditya (2015) Smart Tourism Destinations Enhancing Tourism Experience Through Personalisation of Services. *Information and Communication Technologies in Tourism*, 377–389.

Chapdelaine, Pascale (2020) Algorithmic Perzonalized Pricing. *NYU journal of law & business*, Vol.17(1), 1–47.

Cranage, David A. – Lee, Chung Hun (2011) Personalisation–privacy paradox: The effects of personalisation and privacy assurance on customer responses to travel web sites. *Tourism Management*, Vol. 32(5), 987–994.

Culnan, Mary – Bies, Robert (2003) Consumer Privacy: Balancing Economic and Justice Considerations. *Journal of Social issues*, Vol. 59, 323–342.

Degeling, Martin – Utz, Christine – Lentzsch, Christopher – Hosseini, Henry – Schaub, Florian – Holz, Thorsten (2019) We value your privacy ... Now take some cookies: Measuring the GDPR's impact on web privacy. *Informatik-Spektrum*, Vol. 42(5), 345–346.

Elia, Gianluca – Polimeno, Gloria – Solazzo, Gianluca – Passiante, Giuseppina (2020) A multi-dimension framework for value creation through Big Data. *Industrial marketing management*, Vol. 90, 617–632.

Zeng, Fue – Ye, Qing – Yang, Zhilin – Li, Jing – Song, Yiping Amy (2022) Which privacy policy works, privacy assurance or personalization declaration? An investigation of privacy policies and privacy concerns. *Journal of business ethics*, Vol. 176(4), 781–798.

Eurooppa-neuvosto. Tietosuoja EU:ssa. [Verkkojulkaisu. Viitattu 10.10.2023] <https://www.consilium.europa.eu/fi/policies/data-protection/#gdpr>, haettu 6.3.2024.

Ezrachi, Ariel – Stucke, Maurice E. (2016) *Virtual competition: The promise and perils of the algorithm-driven economy*. Harvard University Press, ProQuest Ebook Central.

Fyall, Alan – Legohérel, Patrick – Frochot, Isabelle – Wang, Youcheng (2019) *Marketing for tourism and hospitality: collaboration, technology and experiences.*

Geneiatakis, Dimitris – Kounelis, Ioannis – Loeschner, Jan – Fovino, Igor Nai – Stirparo, Pasquale (2013) Security and privacy in mobile cloud under a citizen's perspective. *Cyber Security and Privacy*, 16–27.

Gerlick, Joshua A. – Liozu, Stephan M. (2020) Ethical and legal considerations of artificial intelligence and algorithmic decision making in personalized pricing. *Journal of revenue and pricing management*, Vol. 19(2), 85–98.

Gerlick, Joshua A. – Liozu, Stephan M. (2019) A conceptual framework of ethical considerations and legal constraints in the algorithm-driven pricing function. Proceedings of the Ninth International Conference on Engaged Management Scholarship.

Ho, Shuk Ying – Kwok, Sai Ho (2003) The attraction of personalized service for users in mobile commerce: An empirical study. *SIGecom exchanges*, Vol. 3(4), 10–18.

Huang, Jen-Hung – Chang, Ching-Te – Chen, Cathy Yi-Hsuan (2005) Perceived fairness of pricing on the Internet. *Journal of economic psychology*, Vol. 26(3), 343–361.

Hufnagel, Gerrit – Schwaiger, Manfred – Weritz, Louisa (2022) Seeking the perfect price: Consumer responses to personalized price discrimination in e-commerce. University of Münich.

Kangasniemi, Mari – Utriainen, Kati – Ahonen, Sanna-Mari – Pietilä, Anna-Maija – Jääskeläinen, Petri – Liikanen, Eeva (2013) Kuvaileva kirjallisuuskatsaus: eteneminen tutkimuskysymyksestä jäsennettyyn tietoon. *Hoitotiede*, Vol. 25(4), 291–301.

Kortesoja, Matti (2022) Tapaus Vastaamo: Symptomaattinen luenta potilastietosuojan murtumisen yhteiskunnallisista syistä ja seurauksista. *Tutkimus & kritiikki*, Vol. 2(1), 9–32.

Krämer, Andreas – Friesen, Mark – Shelton, Tom (2017) Are airline passengers ready for personalized dynamic pricing? A study of German consumers. Journal of Revenue and Pricing Management, Vol. 17, 115–120.

Kyberturvallisuuskeskus, 2020, Kyberturvallisuus ja yrityksen hallituksen vastuu. *Traficomin julkaisuja*, 2/2020, 8–25.

Lei, Soey Sut Ieng – Wang, Dan (2023) Staging personalization: A service design perspective. *Tourism analysis*, Vol. 28, 439–453.v

Let's Tech IT Easy 2020 [Verkkojulkaisu] <https://letstechiteasy.com/blog/virtual-private-cloud-how-is-vpc-isolated-within-a-public-cloud-advantages-of-vpc/>, haettu 11.3.2024.

Li, Xiao-Bai – Raghunathan, Srinivasan (2014) Pricing and disseminating customer data with privacy awareness. Decision Support Systems, Vol.59, 63–73.

McKinsey The value of getting personalization right or wrong is multiplying. [Verkkojulkaisu] <https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-value-of-getting-personalization-right-or-wrong-is-multiplying> haettu 2.12.2023.

Mulvenna, Maurice – Anand, Sarabjot – Büchner, Alex (2000) Personalization on the net using Web mining. *Communications of the ACM*, Vol. 48(8), 122–125.

Mutimukwe, Chantal – Kolkowska, Ella – Grönlund, Åke (2020) Information privacy in e-service: Effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. *Government information quarterly*, Vol.37 (1), 1–13.

Müller, Nicolas M. – Kowatsch, Daniel – Debus, Pascal –Mirdita, Donika – Böttinger. Konstantin (2019) On GDPR Compliance of Companies' Privacy Policies. *Text, Speech, and Dialogue*, 151–159.

Neumann, Nico – Tucker, Catherine E. – Subramanyam, Kumar – Marshall, John (2023) Is first- or third-party audience data more effective for reaching the 'right' customers? The case of IT decision-makers. *Quantitative marketing and economics*, Vol.21 (4), 519–571.

Office of Fair Trading (2013) The economics of online personalised pricing, 11-12.

Pavlou, Paul A. (2011) State of the information privacy literature: Where are we now and where should we go? MIS Quarterly, Vol. 35(4), 977–988.

Priester, Anna – Robbert, Thomas – Roth, Stefan (2020) A special price just for you: effects of personalized dynamic pricing on consumer fairness perceptions. *Journal of Revenue and Pricing Management*, Vol. 19, 99–112.

Rao, Ashwini – Schaub, Florian – Sadeh, Norman (2015) What do they know about me? Contents and concerns of online behavioral profiles.

Rott, Peter –Strycharz, Joanna –Alleweldt, Frank (2022) Personalised pricing. European Parliament. Policy Department for Economic, Scientific and Quality of Life Policies. *Directorate-General for Internal Policies*, 23–37.

Salminen (2011, 6) Mikä kirjallisuuskatsaus? Johdatus kirjallisuuskatsauksen tyyppeihin ja hallintotieteellisiin sovelluksiin. Vaasan yliopisto.

Kobsa, Alfred (2007) Privacy-enhanced web personalization. *The adaptive web*, 628–670.

Schwartz, Paul M. (2009) Preemption and privacy. *The Yale law journal*, Vol. 118(5), 902–947.

Shi, Yue – Larson, Martha – Hanjalic, Alan (2014) Collaborative Filtering beyond the user-item matrix: A survey of the state of the art and future challenges. *ACM computing surveys*, Vol. 47(1), 1–45.

Silvestru, Cătălin Ionuț – Ifrim, Ana Maria – Oncioiu, Ionica – Lupescu, Marian-Ernuț – Ramido, Steliana (2021) AR & VR Marketing: when and where? *Proceedings of the International Conference on Business Excellence*, Vol. 15(1), 664–671.

Silvestru, Cătălin Ionuț – Ifrim, Ana Maria – Oncioiu, Ionica – Lupescu, Marian-Ernuț – Ramido, Steliana (2021) AR & VR Marketing: when and where? *Proceedings of the International Conference on Business Excellence*, Vol. 15(1), 664–671.

Skeva, Sevasti - Larmuseau, Maarten H. D. - Shabani, Mahsa (2020) Review of policies of companies and databases regarding access to customers' genealogy data for law enforcement purposes. *Personalized medicine*, Vol. 17(2), 141–153.

Skiera, Bernd (2022) Challenges of marketing automation: Linking MarTech & Sales-Tech. *NIM marketing intelligence review*, Vol. 14(2), Nuremberg.

Spiekermann, Sarah – Acquisti, Alessandro – Böhme, Rainer – Hui, Kai-Lung (2015) The challenges of personal data markets and privacy. *Electronic markets*, Vol. 25, 161–167.

Strycharz, Joanna – Duivenvoorde, Bram Benjamin (2021) The exploitation of vulnerability through personalised marketing communication: Are consumers protected? *Internet policy review*, Vol. 10(4), 1-27.

Joanna Strycharz – Guda van Noort – Natali Helberger – Edith Smit (2018) Contrasting perspectives – practitioner's viewpoint on personalised marketing communication. *European journal of marketing*, Vol. 53(4), 635–660.

Strycharz, Joanna – Segijn, Claire M. (2024) Ethical side-effect of dataveillance in advertising: Impact of data collection, trust, privacy concerns and regulatory differences on chilling effects. *Journal of business research*, Vol. 173.

Strycharz, Joanna – Noort, Guda, van – Smit, Edith – Helberger, Natali (2019) Protective behavior against personalized ads: Motivation to turn personalization off. *Cyberpsychology*, Vol.13 (2).

Talón-Ballestero, Pilar – Nieto-García, Marta – González-Serrano, Lydia (2022) The wheel of dynamic pricing: Towards open pricing and one to one pricing in hotel revenue management. *International Journal of Hospitality Management*. Vol. 102, 103–184. Mostoles, Spain.

Talón-Ballestero, Pilar – González-Serrano, Lydia – Soguero-Ruiz, Cristina – Muñoz-Romero, Sergio – Rojo-Álvarez, José Luis (2018) Using big data from customer relationship management information systems to determine the client profile in the hotel sector. *Tourism Management*, Vol. 68, 187–197.

Tietosuojavaltuutetun toimisto. Usein kysyttyä EU:n tietosuoja-asetuksesta. <https://tietosuoja.fi/GDPR>, haettu 3.5.2024.

Victor, Vijay – Thoppan, Jose – Jeyakumar Nathan, Robert – Fekete Farkas, Maria (2018) Factors influencing consumer behavior and prospective purchase decisions in a dynamic pricing environment—An exploratory factor analysis approach. *Social Sciences*, Vol. 7(9), 1–15.

VPN Mentor. 100+ Data Privacy and Data Security Statistics You Need to Watch [Blogi]. <https://www.vpnmentor.com/blog/data-privacy-security-stats/>, haettu 7.3.2024.