

Tomi Lukkari

**VALVONTAKAPITALISMI KULUTTAJAN  
NÄKÖKULMASTA**



JYVÄSKYLÄN YLIOPISTO  
INFORMAATIOTEKNOLOGIAN TIEDEKUNTA  
2024

# TIIVISTELMÄ

Lukkari, Tomi

Valvontakapitalismi kuluttajan näkökulmasta

Jyväskylän yliopisto, 2024, 70 s.

Tietojärjestelmätiede, pro gradu -tutkielma

Ohjaaja: Halttunen Veikko

Valvontakapitalismilla tarkoitetaan liiketoimintaa, joka perustuu siihen, että rahaa tehdään ihmisistä jäävillä digitaalisilla jäljillä. Valvontakapitalismin taustalla olevalle liiketoiminnalle on ominaista, että yritysten käyttäjistään keräämä tieto syötetään tuotantoprosessiin, jonka avulla datasta jalostetaan ennustetuotteita. Ennustetuotteiden avulla yritykset voivat ennakoita kuluttajien tulevaa käyttäytymistä ja hyödyntää sitä voiton tavoittelemiseksi. Tietoja kerätään käyttäjien kaikesta toiminnasta digitaalisilla alustoilla. Kaikki käyttäjädata on merkittävää, mukaan lukien käyttäjien Facebook-tykkäykset, Google-haut, sähköpostit, tekstiviestit, valokuvat, kuunnellut kappaleet ja katsotut videot. Myös verkkomainnon avulla kerätään valtavia määriä dataa yksittäisillä klikkauksilla aina kun kuluttajat käyttävät internetiä tai mobiilisovelluksia. Mainosverkostossa evästeiden avulla liikkuva tieto koskee muun muassa kuluttajan laitetta, sitä mitä hän on katsonut ja kuinka kauan. Tämä tutkielma koostuu kirjallisuuskatsauksesta ja laadullisesta tutkimuksesta, joka toteutettiin haastatteluiden avulla. Tutkimus muodostuu näin ollen teoreettisesta ja empiirisestä osuudesta. Tutkimuksen tavoitteena oli tutkia, kuinka tietoisia kuluttajat ovat valvontakapitalismin toimintatavoista ja sen vaikutuksista heidän kulutuskäyttäytymiseensä sekä millaisia vaikutuksia valvontakapitalismilla on kuluttajan ja yhteiskunnan näkökulmasta. Haastatteluista kävi ilmi, että kuluttajat havaitsevat valvontakapitalismin ilmenemismuotoja arkielämässään, mutta heidän tietämyksensä sen syvemmästä toimintalogiikasta on rajoittunutta. Haastatteluista ilmeni myös, että valvontakapitalismilla on vaikutusta kuluttajien kulutuskäyttäytymiseen ja kuluttajien tietoihin valintoihin. Kuluttajan näkökulmasta valvontakapitalismin keskeisimmät vaikutukset liittyvät kuluttajien tietojen keräämisestä ja eteenpäin myymisestä aiheutuviin yksityisyyden loukkauksiin. Yhteiskunnan kannalta kirjallisuudessa havaittuja haittavaikutuksia ovat ennen kaikkea teknologiajättien valta-asema ja disinformaation leviäminen.

Asiasanat: valvontakapitalismi, kuluttaja, valvontamainonta, yksityisyys

## ABSTRACT

Lukkari, Tomi

Surveillance capitalism from the consumer perspective

Jyväskylä: University of Jyväskylä, 2024, 70 pp.

Information Systems Science, Master's Thesis

Supervisor: Veikko Halttunen

Surveillance capitalism is a business based on making money from the digital traces left by people. The business behind surveillance capitalism is characterised by the fact that data collected by companies about their users is fed into a production process that turns the data into predictive products. These predictive products allow companies to predict future consumer behavior and use it to make a profit. Data is collected on all user activity on digital platforms. All user data is relevant, including users' Facebook likes, Google searches, emails, text messages, photos, songs listened to and videos watched. Online advertising also collects huge amounts of data through individual clicks whenever consumers use the internet or mobile apps. In the advertising network, the data that is circulated through cookies includes the consumer's device, what they have viewed and for how long. This thesis consists of a literature review and a qualitative study conducted through interviews. The study thus consists of a theoretical and an empirical part. The aim of the study was to investigate how aware consumers are of the practices of surveillance capitalism and its impact on their consumption behavior, and what the effects of surveillance capitalism are from the consumer's and society's perspective. The interviews revealed that consumers perceive the forms of surveillance capitalism in their daily lives, but their knowledge of its deeper logic is limited. The interviews also revealed that surveillance capitalism has an impact on consumers' consumption behavior and their conscious choices. From a consumer perspective, the main effects of surveillance capitalism relate to the privacy violations caused by the capture and resale of consumer data. From a society perspective, the main negative effects identified in the literature are the dominance of technology giants and disinformation.

Keywords: surveillance capitalism, consumer, surveillance advertising, privacy

# SISÄLLYS

## TIIVISTELMÄ ABSTRACT

1	JOHDANTO.....	6
2	VALVONTAKAPITALISMI.....	9
2.1	Valvontakapitalismin määritelmä.....	9
2.2	Valvontakapitalismin kehittyminen.....	11
2.2.1	Googlen ja Facebookin alkutaival.....	12
2.2.2	Startup-yrityksistä valvontaimperiumeiksi.....	14
2.3	Valvontakapitalismin taustalla oleva liiketoimintaperiaate.....	15
2.3.1	Ihmisten käyttäytyminen raaka-aineena.....	16
2.3.2	Käyttäjien manipulointi.....	18
2.3.3	Datan kerääminen mainosverkostoista.....	21
3	VALVONTAKAPITALISMI JA KULUTTAJA.....	23
3.1	Kuluttajakäyttäytyminen internetalustoilla.....	23
3.2	Kuluttajien tietosuojat ja yksityisyys.....	26
4	VALVONTAKAPITALISMI JA YHTEISKUNTA.....	30
4.1	Teknologiajättien valta-asema.....	30
4.2	Väärä tieto ja sen leviäminen.....	33
5	TUTKIMUSMENETELMÄ.....	38
5.1	Lähestymistavan valinta.....	38
5.2	Aineiston hankinta.....	39
5.3	Tutkimusaineiston analysointi.....	40
5.4	Tutkimuksen luotettavuus.....	41
6	TUTKIMUSTULOKSET.....	43
6.1	Kuluttajan tietoisuus valvontakapitalismista.....	43
6.1.1	Valvontakapitalismin termi ja liiketoimintalogiikka.....	43
6.1.2	Mainonnan ja sisällön kohdentaminen.....	45
6.1.3	Internetissä olevan tiedon luotettavuus.....	46
6.2	Valvontakapitalismin vaikutukset kulutuskäyttämiseen.....	47
6.2.1	Kuluttajien riippuvuus älylaitteista ja internetalustoista.....	47
6.2.2	Käyttöehtojen tuntemus.....	48
6.2.3	Kulutusvalinnat.....	52
6.3	Kuluttajien kokemat valvontakapitalismin vaikutukset.....	53
6.3.1	Valvontakapitalismin hyödyt ja haitat.....	53
6.3.2	Valvontakapitalismin seuraukset.....	56
6.3.3	Kuluttajien ratkaisuehdotukset.....	57

7	JOHTOPÄÄTÖKSET .....	59
	LÄHTEET .....	63
	LIITTEET	

# 1 JOHDANTO

Valvontakapitalismilla (engl. surveillance capitalism) tarkoitetaan liiketoimintaa, joka perustuu siihen, että rahaa tehdään ihmisistä jäävillä digitaalisilla jäljillä. Shoshana Zuboff on käyttänyt ilmaisua surveillance capitalism vuodesta 2014 lähtien. Valvontakapitalismi pitää sisällään suurimman osan mobiilisovelluksista, kuten TikTokin, Instagramin, Facebookin ja Amazonin. (Suoranta, 2021, s. 120-121 ja Morozov, 2019).

Viime vuosina useat tapahtumat ovat nostaneet teknologiayritysten roolin yhä tärkeämmälle sijalle ihmisoikeusasioissa. Ensinnäkin useat korkean profiilin tapaukset, kuten itävaltalaisen aktivistin Facebookia vastaan nostama yksilö- ja ryhmäkanne, Yhdysvaltojen presidentinvaaleihin vuonna 2016 liittynyt keskustelu vale uutisista ja Cambridge Analytica -skandaali, ovat johtaneet siihen, että pienen teknologiayritysryhmän valtaoikeudet on tunnustettu yhä paremmin, ja ne ovat herättäneet huolta tavasta, jolla niiden liiketoimintakäytännöt voivat häiritä ihmisoikeuksia ja demokraattisia prosesseja. Osana tätä keskustelua jotkut kommentoijat ovat esittäneet, että näiden yritysten koko ja markkinaosuus tekevät niistä tosiasiallisesti monopoleja, jotka ovat liian voimakkaita palvelemaan yleistä etua, ja vaatineet yleishyödyllisten laitosten kaltaista sääntelyä. Vastauksena tähän taloustieteilijät ovat argumentoineet, että Google ja muut teknologiajätit eivät ole monopoleja, koska ne eivät suinkaan täytä koko markkinaa. Riippumatta siitä, muodostavatko nämä yritykset teknisessä mielessä monopoleja, keskustelu osoittaa, että tällä hetkellä on vaikea löytää asianmukaisia poliittisia ratkaisuja teknologiajättien valtaan. (Jørgensen, 2019, s. 28-29)

2000-luvun alussa vasta 25 prosenttia maailman tiedoista oli tallennettu digitaalisesti. Google oli pieni startup-yritys, joka loi loistavan hakutoiminnon, mutta sai siitä vain vähän tuloja. (Zuboff, 2021a, s. 2-3) Vuonna 2001 dotcomromahduksen keskellä, Googlen johtajat löysivät läpimurron keksinnöllä, joka muutti mainonnan. Heidän tiiminsä oppi yhdistämään massiiviset henkilötietojen tietovirrat ja kehittyneet laskennalliset analyysit, jotta he pystyivät ennustamaan, miten mainos tulisi sijoittaa, jotta sitä klikattaisiin mahdollisimman paljon. Ennusteet laskettiin aluksi analysoimalla tietojälkiä, joita käyttäjät tietämättään jättivät yhtiön palvelimille, kun he etsivät tietoa internetistä ja selasivat Googlen

sivuja. Googlen asiantuntijat oppivat poimimaan ennakoivaa metatietoa ylijäämädatasta ja käyttämään sitä analysoidakseen todennäköisiä käyttäytymisen malleja. (Zuboff, 2021a, s. 3) Viime vuosikymmenten aikana henkilötietojen kerääminen ja hyödyntäminen on kasvanut räjähdysmäisesti. Keskeinen syy kehitykseen on ollut se, että uudet teknologiat, muun muassa pilvipalvelut ovat edistyneet ja mahdollistaneet tietojenkäsittelyn yhä suuremmissa määrin. (Keller, 2023, s. 138).

Datataloutta on käsitelty aikaisemmassa tutkimuksessa paljon ja erityisesti siitä näkökulmasta, miten data muodostaa modernin talouden perustan. Datatalous on terminä neutraali eikä se herätä erityisiä tunteita tai ärtymystä. Datakapitalismi on jo puolestaan voimakkaampi käsite, koska termiin sisältyy sana kapitalismi. Kapitalismi terminä herättää tuntemuksia sekä puolesta että vastaan. Valvontakapitalismin käsite valikoitui tutkielman kantavaksi termiksi, koska sen avulla tutkimus on mahdollista kohdistaa paremmin kuluttujanäkökulmaan ja kuluttajalta piilossa oleviin asioihin. Suuri joukko ihmisistä käyttää internetalustoilla olevia palveluita tietämättä tarkemmin niiden vaikutuksista. Nykypäivänä onkin lähes mahdotonta elää niin, ettei käyttäisi älypuhelinta tai sosiaalista mediaa. Alustapalveluiden taustalla on yrityksiä, joiden liiketoiminta perustuu siihen, että käyttäjät saadaan koukuttettua palvelun käyttöön mahdollisimman hyvin, ja sen avulla saadaan kerättyä tietoa heidän käyttäytymisestään. Näin ollen tutkielmassa syvennytään tähän datatalouden kääntöpuoleen. Mitä enemmän kuluttaja louhii tietoa verkossa, sitä enemmän hän antaa tietoa itsestään ja auttamattomasti jää teknologiayrityksiin nähden alakynteen.

Tämän Pro gradu -tutkielman tarkoituksena on selvittää, kuinka tietoisia kuluttajat ovat valvontakapitalismin olemassaolosta ja onko heillä konkreettista käsitystä valvontakapitalismin toimintamalleista. Lisäksi tämän tutkielman tarkoituksena on selvittää, vaikuttaako valvontakapitalismi kuluttajan tietoisiin kulutusvalintoihin ja kulutuskäyttäytymiseen. Tutkielman keskeinen tarkoitus on myös selvittää, millaisia vaikutuksia valvontakapitalismista aiheutuu kuluttajille ja yhteiskunnalle. Tutkielman tavoite on tehdä valvontakapitalismin termi näkyväksi ja tutuksi kuluttajille sekä lisätä tietoisuutta aiheeseen liittyen. Tämän tutkimuksen avulla pyritään kehittämään järjestelmää, koska tietoisuus näistä asioista ei pitäisi olla vain teknologia-alan yrityksillä. Tämä on opetuksellinen tutkielma, jossa kirjallisuuskatsaukseen ja empiiriseen osioon perehtymällä lukija voi oivaltaa keinoja, joilla hän pystyy positioimaan itsensä valvontakapitalismin markkinakentässä ja tekemään aiempaa tietoisempia valintoja verkkoympäristöissä.

Tutkielman tutkimuskysymyksiksi on rajattu seuraavat kolme kysymystä:

- Mikä on kuluttajan tietoisuus valvontakapitalismista ja sen toimintamalleista verkkoympäristöissä?
- Vaikuttaako valvontakapitalismi kuluttajan tietoisiin kulutusvalintoihin ja kulutuskäyttäytymiseen?

- Millaisia vaikutuksia valvontakapitalismista aiheutuu kuluttajille ja yhteiskunnalle?

Tutkimus toteutettiin kirjallisuuskatsauksen ja haastatteluiden avulla. Tutkimus muodostuu näin ollen teoreettisesta osuudesta ja empiirisestä osuudesta. Empiirisen osan tutkimusmenetelmä kuvataan tarkemmin luvussa 5. Kirjallisuuskatsaus toteutettiin siten, että perehdyttiin aiheen kannalta keskeiseen kirjallisuuteen ja aikaisempia tutkimuksia etsittiin Google Scholarista, JYKDOK:sta ja erilaisista tietokannoista esimerkiksi Springerista, IEEE Xploresta ja Elsevierista. Hakuun käytettiin yksittäisiä hakusanoja ja hakusanojen yhdistelmiä sekä suomeksi että englanniksi. Hakusanoina käytettiin muun muassa sanoja "valvonta", "valvontakapitalismi", "disinformaatio", "big data", "digital nudging" ja "algorithm", "yksityisyys", "tietosuojat".

Tämä tutkielma on jaettu 7 lukuun. Tutkielman alussa on johdanto, jossa johdatellaan lukija aiheeseen. Lisäksi johdannossa tuodaan esiin tutkielman tavoite, tutkimusongelma ja tutkimuskysymykset. Tutkielman luvussa 2 määritellään tarkemmin aiheen kannalta keskeiset käsitteet. Lisäksi 2 luvussa kerrotaan valvontakapitalismin kehittymisestä sekä sen taustalla olevasta liiketoimintaperiaatteesta. 3 luku käsittelee kuluttajakäyttäytymistä internetalustoilla. 3 luvussa käsitellään myös valvontakapitalismia kuluttajan näkökulmasta sekä kuluttajien tietosuojaa ja yksityisyyttä. Luvussa 4 käsitellään valvontakapitalismin vaikutuksia yhteiskunnallisesta näkökulmasta. 5 luvussa käsitellään valittua tutkimusmenetelmää. Lisäksi 5 luvussa tuodaan esiin empiiriseen osaan kuuluva tutkimusprosessi ja tutkimuksessa käytetty tutkimusmenetelmä. Luvussa 6 käsitellään tutkimustuloksia. Seitsemäs eli viimeinen luku käsittelee johtopäätöksiä. Lisäksi johtopäätöksissä pohditaan tulevaisuuden näkymiä ja mahdollisia jatkotutkimusaiheita.



## 2 VALVONTAKAPITALISMI

Vaikka moni internetissä oleva sisältö vaikuttaa kuluttajalle ilmaiselta, todellisuudessa se ei sitä kuitenkaan ole. Tyypillistä on, että kuluttaja maksaa sisällöstä rahan sijaan omilla henkilötiedoillaan. Keller havainnollistaa, että internetissä toimiva mainosverkosto on verrattavissa hyvinvointiyhteiskunnan verojärjestelmään, jolla rahoitetaan näennäisesti ilmaisia palveluita. Ihmisillä on usein ajatus, että esimerkiksi Suomessa koulutus ja terveydenhuolto ovat ilmaisia palveluita, mitä ne todellisuudessa eivät ole, vaan ne rahoitetaan verovaroin. Sama sääntö pätee internetiin. Siellä sisältö on tavallaan ilmaista, mutta todellisuudessa se rahoitetaan internetin mainosverkostoissa kulkevalla henkilödatalla. (Keller, 2023, s. 138-143)

### 2.1 Valvontakapitalismin määritelmä

Karl Marxin kuvaamassa teollisen kapitalismin mallissa vastakkain ovat kaksi luokkaa. Ensimmäiseen luokkaan kuuluvat kapitalistit, joilla on pääomaa ja jotka omistavat tuotantovälineet. Toiseen luokkaan kuuluvat työntekijät, joilla ei ole pääomaa ja jotka tarvitsevat esimerkiksi ruokaa, suojaa ja terveydenhuoltoa selviytyäkseen. Työntekijät eivät voi itse tuottaa näitä asioita, koska heillä ei ole käytössään tuotantovälineitä. Sen sijaan he myyvät työvoimansa kapitalisteille ja saavat vastineeksi palkkaa, joka riittää heidän tarvitsemiensa asioiden ostamiseen. Työvoiman ja pääoman yhdistäminen tuottaa tuotteen, jonka kapitalisti myy markkinoilla. Jos tämän tuotteen myyntihinta ylittää työntekijälle maksetun palkan, kapitalisti saa voittoa. Teollisessa kapitalismissa työntekijät ovat vieraantuneet omasta työkyvystään, työnsä tuotteista sekä työnantajistaan. Valvontakapitalismissa käyttäjät ovat samaan tapaan vieraantuneet käyttäytymisestään, tämän käyttäytymisen tuotteista sekä valvontakapitalisteista, joihin he luottavat. Aivan kuten työntekijöiden myymä työkyky hyödykkeenä, käyttäjien käyttäytyminen (klikkaukset, tykkäämiset, liikkeet verkossa) muuttuvat hyödykkeiksi. (Venkatesh 2021 s. 1-10)

Tietokapitalismi eli datakapitalismi on järjestelmä, jossa datan eli tiedon kaupallistaminen mahdollistaa vallan uudelleenjaon informaatioaikakaudella. Koska viestintä ja tieto ovat historiallisesti olleet keskeinen vallan lähde, datakapitalismi johtaa vallan epäsymmetriseen jakautumiseen, jolloin valta painottuu toimijoille, joilla on pääsy tietoon ja mahdollisuus tehdä sen avulla päätöksiä. (West 2019, s. 23) Zuboff (2015, s. 76) on määritellyt valvontakapitalismin tietokapitalismin uudeksi muodoksi, jonka tarkoituksena on ennakoida ja muokata ihmisten käyttäytymistä taloudellisen tuoton saavuttamiseksi. Valvontakapitalismille on ominaista, että se käyttää yksipuolisesti ihmisen käyttäytymistä ilmaisena raaka-aineena, joka muunnetaan käyttäytymistä koskevaksi dataksi (Zuboff, 2019, s. 8). Zuboffin mielestä teollinen kapitalismi muutti luonnon raaka-aineet hyödykkeiksi, kun taas valvontakapitalismi vaatii ihmislunnon aineksia uutta hyödykettä varten (Zuboff 2019, s. 94). Myös West on havainnut selviä yhtäläisyyksiä tietokapitalismin ja Zuboffin määrittelemän valvontakapitalismin kanssa. Hänen mielestään Zuboff tuo oivaltavasti esiin, kuinka valvontakapitalismi muodostaa uuden tiedon kasaantumislogiikan, joka on syntynyt kaikkialle ulottuvan tietokoneväilyksen tuloksena. (West 2019, s. 23) Valvontakapitalismi poikkeaa jyrkästi uusliberalistisista ajatuksista, joiden mukaan markkinoita ei voida ennustaa. Big data analytiikan ehkä tärkein periaate onkin, että jokainen toimija, tapahtuma tai liiketoimi voidaan tehdä näkyväksi ja laskettavissa olevaksi (Cinnamon, 2017, s. 610).

Valvontakapitalismin nousu viimeisten kahden vuosikymmenen aikana on jäänyt pitkälti vaille vastalauseita ja digitaalinen kasvu on ollut nopeaa. Zuboff nostaa esiin, että ei ole yllättävää, että niin monet ryntäsivät seuraamaan valkoista jänistä tunneliansa pitkin luvattuun digitaaliseen ihmemaahan, jossa Liisan tavoin ihmiset joutuivat harhakuvitelmien uhreiksi. Ihmemaassa ihmiset juhlivat uusia digitaalisia palveluita ilmaisina, mutta nyt on havaittavissa, että palvelujen takana olevat valvontakapitalistit pitävät käyttäjiään ilmaisina hyödykkeinä. Aluksi ajateltiin, että käyttäjät etsivät tietoa Googlesta, mutta myöhemmin on oivallettu, että Google etsii kaikkea mahdollista tietoa käyttäjistään. Käyttäjät ovat olettaneet, että he käyttävät sosiaalista mediaa yhteydenpitoon, mutta ovat myöhemmin saaneet tietää, että yhteys on sitä, miten sosiaalinen media hyödyntää käyttäjistä saatavaa dataa. Kuluttajat eivät ole tietoisia, että jopa heidän vapaasti luovuttama tieto sisältää runsaasti dataa, joka on enemmän kuin mitä itse palvelun tuottamiseen tai parantamiseen tarvitaan. Kyse ei ole vain siitä, mitä käyttäjät kirjoittavat verkossa, vaan myös siitä, käyttävätkö he esimerkiksi huutomerkkejä, kuinka he muokkaat valokuviaan tai missä he liikkuvat. Kyse on enemmänkin kasvojen mikroilmeistä välittyvistä tunnetiloista kuin kasvojen identiteetistä. Kyse ei ole vain siitä, mistä käyttäjät tykkäävät, vaan myös tykkäysten taustalla olevista tottumuksista. (Zuboff, 2020, s. 1-3)

Valvontakapitalismin käsitteen ohella on keskeistä ymmärtää big datan käsite. Datalla laajemmassa merkityksessä tarkoitetaan kaikkea materiaalia, joka on tallennettu tai on mahdollista tallentaa. Tavallisesta datasta big datan erottaa

sen suuri määrä, monimuotoisuus sekä nopea kasvu. (Gritsenko, 2018 s. 48) Big data nähdään tyypillisesti informaatioajan teknologisenä ilmiönä ja sen kuvailussa käytetään usein kolmea termiä – määrä (volume), nopeus (velocity) ja monimuotoisuus (variety). Ne viittaavat tietokokonaisuuksien laajuuteen, tiedon tuottamisnopeuteen sekä tietotyyppien ja -muotojen valikoimaan. (Shahin & Zheng, 2020, s. 27) Zuboff kutsuu big dataa valvontakapitalismin edellytykseksi ja ilmentymäksi. Zuboffin mukaan big data on ennen kaikkea perustavanlaatuinen osa tätä uutta kasaantumislogiikkaa, eli valvontakapitalismia. Big datan avulla on mahdollista luoda uusi liiketoiminnan alue, joka koostuu reaaliaikaisesta ihmisten käyttäytymistä koskevasta tiedosta, ja se luo mahdollisuuksia puuttua ihmisten käyttäytymiseen ja muuttaa sitä voiton tavoittelemiseksi (Zuboff, 2015, s. 84). Facebook ja monet muut suuret internetpohjaiset yritykset jakavat tämän logiikan, ja siitä näyttää tulleen myös useimpien verkossa toimivien startup-yritysten ja sovellusten oletusmalli. Google on maailman suosituin verkkosivusto. Googlea pidetään laajalti big datan edelläkävijänä, ja näiden saavutustensa ansiosta se on myös ollut edelläkävijä laajemmalle kasaantumisen logiikalle. (Zuboff, 2015, s. 75-77)

Tristan Harrisin mukaan valvontakapitalismin liiketoimintaperiaatetta hyödyntävillä yrityksillä on kolme tavoitetta. Ensimmäinen tavoite on käyttäjien sitouttaminen. Mitä kauemmin internet sivu tai mobiilisovellus saa käyttäjän pysymään aktiivisena alustalla, sitä enemmän valvontakapitalistit saavat kerättyä dataa hänestä ja hänen käyttäytymisestään. Toinen tavoite on kasvu. Alustapalvelu kannustaa käyttäjää kutsumaan ystäviään rekisteröitymään uusiksi käyttäjiksi, jotta hekin voivat kutsua ystäviään ja niin edelleen. Tällä tavalla yritys saa jatkuvasti uusia käyttäjiä. Kolmantena tavoitteena on mainostulojen maksimointi edellä kuvattujen tavoitteiden avulla. Kun yritys saa lisättyä käyttäjien ruutuaikaa ja lisää käyttäjiä, myös sen mainostulot kasvavat. (Orlowski, Coombe & Curtis, 2020).

Nykypäivänä valvontakapitalismi on aikamme hallitseva taloudellinen instituutio. Koska rajoittavaa lainsäädäntöä ei ole, tämä järjestelmä pääsee puuttumaan kaikkiin näkökohtiin, jotka liittyvät ihmisten yhteyteen digitaalisen tiedon kanssa. Lupaus valvontaosingosta liittyy valvontatalouden nykypäivänä osaksi normaalia taloutta. Kaikki sovellukset ja ohjelmistot, riippumatta siitä, kuinka hyväntahtoisilta ne vaikuttavat, on pääasiassa suunniteltu maksimoimaan tietojen keräämistä niiden taustalla olevien yritysten tuoton maksimoimiseksi. (Zuboff, 2021a, s. 6)

## 2.2 Valvontakapitalismin kehittyminen

Zuboff on kuvannut, että valvontakapitalismin kehitys etenee neljässä vaiheessa. Ensimmäistä vaihetta hän on kuvannut oikeuksien haltuun ottona, joka luo perustan sille, että yritykset keräävät vapaana raaka-aineena käyttäjien käyttäytymistä koskevaa dataa ja julistavat sen yksityiseksi omaisuudekseen. Toista vaihetta leimaa käyttäjän ja valvontakapitalistien välisen epätasa-arvon

yrkkä kasvu, joka ilmenee erona siinä, mitä yritys saa tietää käyttäjästään ja mitä käyttäjä saa tietää yrityksestä. Kolmatta vaihetta, jota elämme tällä hetkellä, Zuboff kuvaa episteemiseksi kaaokseksi, joka johtuu voittoa tavoittelevasta algoritmista korruptoituneen tiedon vahvistamisesta, levittämisestä ja sen kohdistamisesta. Tästä tiedosta suuri osa on tuotettu koordinoituilla disinformaatiojärjestelmillä. Sen vaikutukset näkyvät reaali maailmassa muun muassa yhteiskunnallisessa keskustelussa sekä lamauttamalla demokraattista politiikkaa ja toisinaan lietsomalla väkivaltaa ja jopa kuolemaa. Neljännessä vaiheessa edellä kuvattu valta-asema institutionalisoituu ja syrjäyttää demokraattisen hallinnon. Episteeminen kaaos valmistelee maaperää episteemiselle vallalle heikentämällä demokraattista yhteiskuntaa. (Zuboff, 2021b, s. 4-5)

Meidän aikanamme Googlesta tuli valvontakapitalismin edelläkävijä, löytäjä, yhteistyökumppani, kokeilija, johtava toimija, roolimalli ja levityskeskus (Zuboff, 2019, s. 63). Facebook oli Googlen ensimmäinen seuraaja, mutta ei suinkaan viimeinen. Google, Facebook, Amazon, Microsoft ja Apple ovat yksityisiä valvontaimperiumeja, joilla kaikilla on omat liiketoimintamallinsa. Google ja Facebook ovat datayhtiöitä ja valvontakapitalistisia pelimerkkejä. Näillä yrityksillä on lisäksi erilaisia liiketoiminta-alueita, jotka voivat sisältää dataa, palveluja, ohjelmistoja ja fyysisiä tuotteita. Vuonna 2021 nämä viisi yhdysvaltalaista teknologiajättiä edustivat viittä kuudesta markkina-arvoltaan suurimmasta julkisesti noteeratusta pörssi-yhtiöstä. (Zuboff, 2021a, s. 6) Seuraavissa kappaleissa tarkastellaan tarkemmin Googlen ja Facebookin kehitystä pienistä start-up-yrityksistä nykypäivän valvontaimperiumeiksi.

## 2.2.1 Googlen ja Facebookin alkutaival

Vuonna 2000 vain 25 prosenttia maailman tiedoista oli tallennettu digitaalisesti. Pieni Piilaakson internetalan startup-yritys Google kohtasi eksistentiaalisen uhan finanssikriisin aikana, joka tunnetaan nimellä dotcom-romahdus. Googlen perustajat Larry Page ja Sergey Brin eivät olleet aiemmin keksineet keinoa muuttaa hakukoneitansa tuottavaksi. Vuosina 2000 ja 2001, kun yhtiön sijoittajat uhkasivat lopettaa sijoittamisen, Page ja Googlen tiimi löysivät ratkaisun. Googlen asiantuntijat oppivat tunnistamaan ylijäämädataan upotettuja käyttäytymissignaaleja, jotka jäivät jäljelle käyttäjien haku- ja selailutoiminnoista. Nämä käytöstä poistetut käyttäytymisjäljet olivat ylijäämää - enemmänkin kuin mitä tuotteen parantamiseen tarvittiin. Käyttäytymisen ylijäämään sisältyvät signaalit voitiin yhdistää ja analysoida käyttäjien käyttäytymisen ennustamiseksi. Tiimi oppi ennustamaan klikkausprosentin, eli laskukaavan, joka pelasti pienen yrityksen taloudelliselta tuholta. (Zuboff, 2022, s. 11)

Sen sijaan, että Google olisi myynyt pelkkää hakupalvelua käyttäjilleen, se teki hakukoneestaan hienostuneen valvontakoneiston ihmisten tietojen keräämiseksi. Yrityksen johtajat pyrkivät pitämään nämä taloudelliset toimet salassa käyttäjiltä, lainsäätäjiltä ja kilpailijoilta. Massiiviset louhintatoimet olivat uuden taloudellisen rakennelman kulmakivi, joka syrjäytti muut näkökohdat, alkaen tiedon laadusta. Valvontakapitalismin logiikassa tiedon eheys ei ole

yhteydessä tuloihin. Hyödylliset ennusteet edellyttivät ihmisten tietovirtoja valtavassa mittakaavassa. Käyttäjät eivät osanneet epäillä, että heidän tietojansa jahdattiin salaa ja kaapattiin internetin joka kolkasta sekä myöhemmin myös muualta, kuten sovelluksista, älypuhelimista, laitteista, kameroista ja sensoreista. Käyttäjien tietämättömyys ymmärrettiin olevan ratkaisevan tärkeää menestyksen kannalta. Yritykset sitoutuivat käyttäjiä uusien tuotteiden avulla, ja samalla salasivat laittomat louhintatoimensa. (Zuboff, 2021a, s. 3-4)

Google loi ensimmäiset järjestömän tuottoiset markkinat humanfutuureilla käytävälle kaupalle, jonka nykyään tunnemme nimellä kohdennettu verkkomainonta. Kohdennettu verkkomainonta perustuu ennusteisiin siitä, mitä mainoksia käyttäjät klikkaavat. Kohdennettua verkkomainontaa käsitellään tarkemmin kappaleessa 2.3.3. Vuosien 2000-2004 välillä kun uusi taloudellinen logiikka oli vasta syntymässä, Google listautui pörssiin, ja sen tulot kasvoivat 3 590 prosenttia. Tämä hätkähdyttävä luku edustaa valvontaosinkoa, joka kiinnitti nopeasti sijoittajien huomion, ja lopulta se sai startup-yritykset, sovelluskehittäjät ja muut yritykset siirtymään liiketoimintamalleissaan kohti valvontakapitalismia. Lupaus siitä, että humanfutuuriin myynnistä saatavat tulot olisivat nopeasti suuria, johti ensin Facebookin syntyyn ja sen jälkeen yleisemmin teknologia-alan kasvuun ja myöhemmin myös muuhun talouteen. Valvontakapitalismi on ulottunut sen jälkeen niinkin erilaisille aloille kuten vakuutus- ja rahoitusosalalle, vähittäiskaupan alalle, koulutukseen ja terveydenhuoltoon, kiinteistöalalle sekä viihdealoille. (Zuboff, 2020, s. 4)

Mark Zuckerberg perusti Facebookin vuonna 2005. Facebookin käyttäjämäärät kasvoivat nopeasti, mutta sen tulot eivät. Kuten Google muutamaa vuotta aiemmin, Zuckerberg ei pystynyt muuttamaan suosiota voitoksi. Sen sijaan hän ajalehti virheestä virheeseen. Käyttäjien yksityisyydensuojan odotusten törkeä loukkaaminen, aiheutti voimakkaita julkisia vastareaktioita, vetoamuksia ja ryhmäkanteita. Zuckerberg näytti ymmärtävän, että vastaus hänen ongelmiinsa oli käyttäjien tietojen louhinta mainostulojen hankkimiseksi, mutta uuden logiikan monimutkaisuus ei ollut hänelle tuttua. Hän kääntyi Googlen puoleen saadakseen vastauksia. Maaliskuussa 2008 Zuckerberg palkkasi Sheryl Sandbergin, joka toimi aikaisemmin Googlen globaalista verkkomainonnasta vastaavana johtajana. Sandberg oli tullut Googlen palvelukseen vuonna 2001 ja oli keskeinen toimija valvontakapitalismin vallankumouksessa. Sandberg ymmärsi Facebookin valtavat mahdollisuudet saada runsaasti ennustettavaa dataa, kuten tiedot käyttäjien sukupuolesta, iästä ja sijainnista. Vuoden 2009 lopulla Facebook raivasi tietä valvontataloudelle uudella yksityisyydensuojaa koskevilla käytännöillä. Uuden asetuksen mukaisesti tiedot olivat kaikille julkisesti saatavilla olevia tietoja. Electronic Frontier Foundation varoitti, että uudet "kaikille julkiset" -asetukset poistivat mahdollisuudet rajoittaa henkilökohtaisten tietojen näkyvyyttä. Facebookin strategia oli tällä tavalla pakottaa käyttäjät valitsemaan uudet yksityisyysvaihtoehdot edistääkseen julkisia päivityksiä ja siten rajoittaa Facebookin omaa vastuuta mahdollisista tulevaisuudessa ilmenevistä väärinkäytöksistä. Jos sosiaalista verkostoa vastaan

tuli merkittäviä vastareaktioita, Facebook pystyi väittämään, että käyttäjät tekivät vapaaehtoisena valinnan jakaa tietonsa kaikkien kanssa. Tällä tavalla Zuckerberg ja Facebook kiersivät sääntöjä, koska mikään laki ei estänyt heitä liittymästä Googlen joukkoon. (Zuboff, 2021a, s. 4–6)

## 2.2.2 Startup-yrityksistä valvontaimperiumeiksi

Yksi kirjoittamaton sääntö valvontakapitalismin ja valvontayhteiskunnan kehityksessä on valvonnan poikkeuksellisuuden -politiikka, joka syntyi syyskuun 11. päivän terrori-iskujen jälkeen. Yhdysvaltojen hallituksen huoli siirtyi yksityisyyden suojaamisesta täydellisen tietoisuuden saavuttamiseen. Tuon ajan poliittisessa ympäristössä Piilaaksosta nousseet aloittelevat valvontakapasiteetit näyttivät tähän tarpeeseen soveltuvilta. (Zuboff, 2020, s. 7) Myös Chandler ja Fuchs (2019, s. 48) ovat tuoneet esiin, että digitaalinen ratkaisukeskeisyys voimistui terrori-iskujen jälkeen. Hallitukset eivät kyenneet vastaamaan poliittiseen monimutkaisuuteen, jonka seurauksena ne edistivät ratkaisukeskeistä ideologiaa, jonka mukaan laajamittaisella datalla ja verkkovalvonnalla voitiin ennustaa, ehkäistä ja valvoa terrorismia ja järjestäytyntä rikollisuutta. Näin determinismin logiikka laajeni ja voimistui entisestään. Valvontayhteiskunnassa yhdistyivät valvontaideologia, valvontavaltio ja valvontakapitalismi.

Kourallinen yrityksiä kehittyi pienistä startup-yrityksistä biljoonien dollarien globaaleiksi valvontaimperiumeiksi. Nämä yritykset ja niiden ekosysteemit muodostavat nykyään laajamittaisen poliittistaloudellisen institutionaalisen järjestyksen, joka ulottuu yli toimialojen ja talouksien. Valvontakapitalismin institutionaalinen järjestys on informaatio-oligopoli, jossa dataa hyödyntää muutama toimija. (Zuboff, 2022, s. 3) Zuboffin (2021b, s. 8) mukaan nuoret yrittäjät, joilla ei ollut demokraattisia valtuuksia, saivat haltuunsa loputtomasti tietoa ja heille kuulumatonta valtaa. Googlen perustajat käyttivät määräysvaltaa maailman tiedon tuotannossa, järjestämisessä ja sen esittämisessä. Niin ikään Facebookin perustajalla on ollut samanlainen määräysvalta siinä, millaisesta tiedosta tuli osa maailmanlaajuista viestintää ja uutisointia. Facebookin käyttäjämäärät kasvoivat siten, että käyttäjät olivat tietämättömiä siitä, mitä sen taustalla tapahtui.

Liiketoiminnan ja yhteiskunnan alan akateemisessa keskustelussa tietotekniikka ja big data -teollisuus ovat pitkään jääneet suhteellisen vähälle huomiolle. Oikeastaan uusien palveluiden vastaanotto ja mahdolliset hyödyt on nähty pikemminkin myönteisessä valossa, mikä on vahvistanut ja rohkaissut yritysten roolia yhteiskunnassa. (Flyverbom, Deibert & Matten, 2019, s. 8) Valvontakapitalismin nousu voidaan pitkälti liittää poliittisten ja taloudellisten rakenteiden uusliberalisoitumiseen, jota on nähty Atlantin alueella 1900-luvun jälkipuoliskolla. Piilaakso ja laajemmin länsimainen teknologia-ala on kasvanut vapaan markkinatalouden lisääntyessä ja noussut kokoonsa nähden yhdeksi vähiten säännellyistä teollisuudenaloista modernin historian aikana. Tilannetta pahentaa se, että useimpia nykyisiä sääntelyinstituutioita ei ole suunniteltu

vastaamaan datatalouden haasteisiin, sillä ne on luotu aikakaudella, jolloin teollistuminen oli kehityksen ensisijainen moottori. Tämän seurauksena useimmat suuret teknologiayritykset ovat saaneet kehittää valvontateknologioitaan ilman valtion valvontaa. Normaalisti nämä toimet saattaisivat herättää hälytyksen valtion lainsäätäjissä. Kun tietotekniikka on alkanut työntää sivilisaatiota kohti uusia kapitalististen suhteiden muotoja, ainakin kaksi auktoriteettia on pyrkinyt valvomaan näiden teknologioiden vaikutusta yhteiskuntaansa ja osoittamaan tiettyä demokraattista (Euroopan unioni) tai auktoriteettista (Kiina) itsemääräämisoikeutta teknokapitalismin voimia vastaan. Suuressa osassa muuta maailmaa, Yhdysvallat mukaan luettuna, massatietovalvontaan perustuvat liiketoimintamallit näyttävät laajenevan. Jopa Cambridge Analytica -skandaalin, jota kuvataan tutkielmassa myöhemmin tarkemmin sekä Yhdysvaltojen vuoden 2016 presidentinvaaleissa tapahtuneen ulkomaisen sekaantumisen jälkeen, valtio ei ole vielä hyväksynyt merkittäviä tietosuojaa koskevia lakeja liittovaltion tasolla. (Aho & Duffield, 2020, s. 191)

### 2.3 Valvontakapitalismin taustalla oleva liiketoimintaperiaate

Henkilötietojen käsittely ulottuu nykypäivänä kaikille yhteiskunnan aloille ja niitä käsitellään suuria määriä. Viime vuosina on alettu kiinnittää erityistä huomiota henkilötietojen hyödyntämiseen mainosverkostoissa. Ihmisten henkilötietojen kerääminen ja hyödyntäminen ei kuitenkaan rajoitu pelkästään tähän asiayhteyteen. On mahdollista, että henkilötietoja pyritään myymään yritykseltä toiselle suoraan tai vaihtoehtoisesti yritykset analysoivat henkilötietoja ja myyvät toisille yrityksille valmiita analyyskejä. (Keller, 2023, s. 142)

Valvontakapitalismin taustalla olevalle liiketoiminnalle on ominaista, että yritysten keräämä ylijäämädata syötetään kehittyneeseen tuotantoprosessiin, joka tunnetaan nimellä koneälykyys (machine intelligence). Ylijäämädata jalostetaan ennustetuotteiksi, joiden avulla yritykset voivat ennakoita, mitä teet nyt, pian ja tulevaisuudessa. Ylijäämädatan määrittely ”jätämateriaaliksi” palvelee yrityksen etua ja tällä tavalla sen louhintaa ja mahdollista rahaksi muuttamista pidetään vähemmän kiistanalaisena yhteiskunnan ja kuluttajan näkökulmasta. (Zuboff, 2015, s. 79). Lopuksi datasta jalostettuja ennustetuotteita myydään uudennlaisella käyttäytymisenennusteiden markkinapaikalla, jota Zuboff kutsuu käyttäytymisfutuurimarkkinaksi (behavioral future markets). Valvontakapitalistit ovat rikastuneet valtavasti näistä kaupankäyntitoimista, sillä monet yritykset ovat innokkaita lyömään vetoa kuluttajien tulevasta käyttäytymisestä. (Zuboff, 2019, s. 8).

Big data, kaikkialle ulottuva seuranta, koneoppiminen ja muunlainen tekoäly muokkaavat yhä enemmän yritysten ja kuluttajien välistä vuorovaikutusta. Algoritmien avulla yritykset käyttävät näitä työkaluja mainonnan, myyntiportaalien, palautus- ja peruutusprosessien, hinnoittelun ja jopa itse tuotteiden ja palvelujen suunnitteluun. Kun käsitellään suuria

tietokokoelmia, algoritmipohjaista tiedonlouhintaa voidaan käyttää suurten tietokokonaisuuksien käsittelyyn ja suodattamiseen. Vaikka termi algoritmi voidaan hyvin yksinkertaisesti määritellä laskennallisten vaiheiden sarjaksi, joka muuttaa syötteen tulosteeksi, koneoppimisalgoritmit muokkaavat käsittelytoimintojaan itsenäisesti uusien tietojen perusteella. Tässä tapauksessa algoritmit on ohjelmoitu voittojen optimoimiseksi. Samalla digitaaliset käyttöliittymät voivat hyödyntää verkkoympäristön ominaisuuksia manipulointiin ja harhaanjohtamiseen, mikä on niin yleinen ilmiö, että siitä on käytetty termiä pimeät käytänteet (dark patterns). (Willis, 2020, s. 116 ja Murphy, 2017, s. 226). Seuraavissa alaluvuissa esitellään valvontakapitalismia hyödyntävien yritysten tapoja kerätä dataa käyttäjistään.

### 2.3.1 Ihmisten käyttäytyminen raaka-aineena

Ihmistä kerättävä data muodostuu keräämällä pientä dataa yksilöiden tietokonevälitteisistä toimista ja ilmaisista. Kaikki tieto on merkittävää, mukaan lukien ihmisten Facebook-tykkäykset, Google-haut, sähköpostit, tekstiviestit, valokuvat, kuunnellut kappaleet ja katsotut videot, sijaintitiedot, viestintätottumukset, verkostot, ostokset, liikkeet, klikkaukset, kirjoitusvirheet ja nettisivujen katselu. Tällaisia tietoja hankitaan, käsitellään, abstrahoidaan, kootaan, analysoidaan ja pakataan, myydään, analysoidaan edelleen ja myydään uudelleen. (Zuboff, 2015, s. 79) Yksi intuitiivinen mutta merkittävä havainto on se, että tiedot tiedoista eli metatiedot voivat olla yhtä tärkeitä ja ennustavia kuin sisältö siitä, mitä kuluttajat katsovat tai tekevät verkossa. Esimerkiksi tiedetään hyvin, että persoonallisuuden kohdentaminen voi lisätä myös markkinoinnin tehokkuutta. Big datan avulla on ilmennyt, että kuluttajien verkossa julkaisemien valokuvien värisävy, kirkkaus ja värikylläisyys voivat kertoa käyttäjien persoonallisuudesta yhtä paljon kuin valokuvien sisältö. (Willis, 2020, s. 125)

Facebook on kehittänyt toimintatapaansa käyttäjäprofiloinnin suuntaan, jolloin sen tarkoitus on, että Facebook kerää tietoa kaikesta, mitä alustan käyttäjät tekevät Facebookissa tai yhtiön omistamalla muilla alustoilla, myydäkseen käyttäjiensä tarkat kuluttajaprofiilit mainostajille. Facebookin kohdalla erityisen hyödyllisiä ennusteprofiilien luomisessa ovat tykkäämistä sekä muita tunteita osoittavat reaktionappulat sekä se, että Facebookin tunnuksilla voidaan kirjautua moniin eri verkkopalveluihin. Tällä tavalle Facebook laajentaa omia valvontamahdollisuuksiaan edelleen myös muille kuin yhtiön omille verkkoalustoille. Reaktionappuloiden avulla voidaan osoittaa selkeästi yrityksille, miten verkkomarkkinointi on onnistunut ja mikä tuotemerkki on pidetty sekä se, milloin käyttäjä on sellaisessa mielentilassa, että vastaanottaa tehokkaimmin mainontaa. (Sirkkunen, 2016, s. 122) Facebookin tekoäly imuroi biljoonia datapisteitä joka päivä tuottaakseen tuhansia käyttäytymismalleja. Nämä laskelmat syötetään ennustepalveluun, joka tuottaa yli 6 miljoonaa ennustetta sekunnissa. Nämä ovat ennustustuotteiden rakennuspalikoita, joita myydään yrityksille, mainostajille, poliittisille kampanjoille ja muille ostajille, jotka ovat kiinnostuneita tietämään, vahvistamaan tai estämään yksilöiden ja ryhmien ennustettua käyttäytymistä. (Zuboff, 2022, s. 12) Jo varhaisessa



vaiheessa oli selvää, että koneälylle on syötettävä suuria tietomääriä. Parhaat algoritmit vaativat myös erilaisia tietoja, jotta yritys voi saavuttaa merkittäviä mittakaavaetuja. Tämä johti aikanaan mobiilivallankumoukseen, jonka jälkeen kamerat, tietokoneet ja mikrofonit tulivat osaksi uusia älypuhelimia ja osaksi ihmisten arkielämää. (Zuboff, 2020, s. 5)

Varmuus ja tieto ihmisten asioista on futuurimarkkinoiden elinehto, joka ajaa valvontakapitalistit kilpailemaan ennustetietojen volyyymistä (Zuboff, 2020, s. 3). Huomionarvoista on, että valvontakapitalismin toiminnoilla ei ole muodollista kiinnostusta tosiasioihin. Kaikki tieto on tervetullutta samanarvoisina, vaikka kaikki tieto ei todellisuudessa olekaan samanarvoista. Jos valvonta-alan yritystä pyydetään hylkäämään sisältö, se on sama kuin pyytäisi hiilikaivostoimintaa hylkäämään hiilipakkaukset sen vuoksi, että ne ovat liian likaisia. Siksi sisällön suodattaminen on valvontakapitalistien näkökulmasta viimeinen keino. Facebookin tapauksessa tietojen suodattamiseen ryhdytään joko siksi, että minimoidaan riski käyttäjien vetäytymisestä tai poliittisten sanktioiden välttämiseksi. Niiden avulla pyritään pikemminkin lisäämään kuin vähentämään tietovirtoja. (Zuboff, 2021b, s. 10–11)

Yksi tulevaisuuden merkittävä valvontatietovirtojen lähde, jonka odotetaan kasvavan tulevaisuudessa räjähdysmäisesti, on uusiin laitteisiin, esineisiin ja paikkoihin upotetut sensorit, joiden avulla tietoja kerätään. Googlen uudet investoinnit koneoppimiseen, lennokkeihin, puettaviin tuotteisiin, itseajaviin autoihin, nanohiukkasiin sekä älykkäisiin kodin laitteisiin, ovat kaikki olennainen osa tätä kasvavaa älysensoreiden ja internet -laitteiden verkostoa. (Zuboff, 2015, s. 78) Osana digitaalitaloutta kuluttajille tarkoitettavat puettavat kuntolaitteet tarjoavat niihin liittyville sovelluksille, alustoille, yrityksille ja kolmansille osapuolille esteettömän pääsyn myös arkaluonteisiin lääketieteellisiin ja terveyteen liittyviin tietoihin. Valvontakapitalismin näkökulmasta käyttäjien pitkäaikainen sitouttaminen laitteisiin on ensiarvoisen tärkeää. Puettavilla laitteilla tarkoitetaan muun muassa älykelloja, joiden avulla käyttäjät voivat seurata aktiivisuuttaan sekä kehonsa rajoja ja kyvykkyyksiä. Todellisuudessa puettavan kuntoilulaitteen käyttäjät luovuttavat myös tietonsa vastineeksi eräänlaisen ”tekno-utopian” saavuttamisesta. Markkinoilla näiden laitteiden merkitys käyttäjien pitkäaikaisen sitoutumisen kannalta perustuu kykyyn ylläpitää sitä yksinomaan tietopääoman keräämisen vuoksi. Riippumatta siitä, tarkastellaanko suunnitteluun, toiminnallisuuteen tai käyttäytymiseen liittyviä tekijöitä, puettavien kuntolaitteiden perimmäinen tehtävä on tuottaa tietoa, josta voidaan saada voittoa. Ilman tätä perustarkoitusta puettavat kuntolaitteet sekä niiden mobiilisovellukset ja -alustat ovat melko hyödyttömiä yrityksille. (Gidaris, 2019, s. 133-134)

Myös merkittävä tietovirtojen lähde on yritysten ja hallitusten tietokannat, kuten pankkien, maksujenvälittäjien, luottoluokituslaitosten, lentoyhtiöiden, vero- ja väestölaskentatietokantojen, terveydenhuollon, luottokortti-, vakuutus-, lääke- ja televiestintäyritysten tietokannat. Näistä tietokannoista kerätty data sekä kaupallisten liiketoimien avulla kerätystä tietovirroista saatu data kerätään ja kootaan yhteen. Sen jälkeen tiedot analysoidaan, paketoitaan ja myydään

tiedonvälittäjien toimesta eteenpäin. Toiminnot tehdään lakisääteisen kuluttajansuojan ulkopuolella ja ilman kuluttajien tietoa tai suostumusta. (Zuboff, 2015, s. 78)

Suuri ja hieman kyseenalainen datan keräämisen lähde on yksityisistä ja julkisista valvontakameroista saatavat tiedot, mukaan lukien kaikki kamerat, älypuhelimista satelliitteihin ja Street View -palvelusta Google Earthiin. Esimerkiksi Googlen Street View lanseerattiin vuonna 2007, ja se kohtasi vastustusta kaikkialla maailmassa. Muun muassa Saksan viranomaiset havaitsivat, että jotkut Street View -autot olivat varustettu skannerilla, jotka kaappasivat tietoja yksityisistä Wi-Fi-verkoista. (Zuboff, 2015, s. 78) Toinen tapahtuma, josta Google joutui arvostelun kohteeksi, oli se, kun yksi sen alihankkijayrityksistä käytti vilpillistä taktiikkaa skannatessaan ihmisten kasvoja teknologiajätin data-arsenaalia varten. New York's Daily News -lehden mukaan Googlen alihankkija ohjeisti työntekijöitään kohdistamaan työnsä tummaihoisiin ihmisiin sekä kodittomiin, tarjoamalla heille viiden dollarin lahjakortteja. Työntekijöitä myös oheistettiin valehtelemaan ja kiirehtimään koehenkilöitä suostumussopimusten kanssa. Eräs työntekijä on myös kertonut, että heitä käskettiin lausumaan harhaanjohtavia kannustimia, kuten "Leiki puhelimella pari minuuttia ja saat lahjakortin" ja "Meillä on uusi sovellus, kokeile sitä ja saat 5 dollaria". Kyseessä oli yritys kasvattaa Googlen tietokantaa Pixel 4 -älypuhelimta varten, joka käyttää kasvontunnistusbiometriaa. (Elias, 2019)

Kasvontunnistusjärjestelmien nopea kehitys paljastaa, että valvontakapitalistit ovat vaatineet oikeutta ottaa talteen kasvojamme kaikkialta, missä ne esiintyvät – esimerkiksi kadulla tai Facebook-sivulla. Financial Times -lehti kertoi, että Microsoftin kasvontunnistuskoulutuksen 10 miljoonan kuvan tietokantaa käytettiin IBM:n kaltaisten yritysten ja valtion virastojen, kuten Yhdysvaltain ja Kiinan armeijan hyväksi. Näiden yritysten joukossa oli kaksi kiinalaista laitetoimittajaa, jotka toimittivat laitteita viranomaisille Xinjiangissa, jossa uiguuriyhteisön jäsenet elävät ulkoilmavankiloissa kasvontunnistuksen järjestelmien avulla jatkuvan valvonnan alaisina. (Zuboff, 2020, s. 2)

### 2.3.2 Käyttäjien manipulointi

Tristan Harris on Zuboffin tavoin tuonut esiin, kuinka kourallinen ihmisiä, jotka työskentelevät teknologiayrityksissä, ohjaavat valinnoillaan sitä, mitä miljardi ihmistä ajattelee tänään. Harris nostaa artikkelissaan esiin, että aina kun käyttäjä ottaa puhelimensa esiin ja suunnittelee, miten tämä toimii tai mitä syötteessä näkyy, se aikatauluttaa pieniä aikaloikoja käyttäjän mieleen. Kun käyttäjä näkee ilmoituksen, se pakottaa hänet ajattelemaan asioita, joita hän ei ehkä aikonutkaan ajatella. Jos käyttäjä pyyhkäisee ilmoituksen yli, se pakottaa hänet käyttämään siihen hieman aikaa, jolloin käyttäjä joutuu perehtymään johonkin, mihin ei alun perin aikonutkaan perehtyä. Kaiken teknologian taustalla on piilotettu tavoite eli kilpailu käyttäjien huomiosta. Jokainen uutissivusto, pelit ja jopa mediasovellukset kilpailevat käyttäjien huomiosta, jota on vain rajallinen määrä. Paras tapa saada ihmisten huomio on tietää, kuinka ihmismieli toimii. (Harris, 2017) Uusien markkinoiden kilpailudynamiikka ajaa valvontakapitalistit

hankkimaan yhä enemmän ennakoivia käyttäytymismallien lähteitä, kuten ihmisten ääntä, persoonallisuutta ja tunteita. Lopulta valvontakapitalistit ovat huomanneet, että tehokkain tapa saada ennustettavinta dataa käyttäytymisestä, on puuttua ja manipuloida eri tilanteita tönäisemällä, houkuttelemalla, virittämällä ja kuuntelemalla käyttäjiä yritystä palvelevien tulosten saavuttamiseksi. (Zuboff, 2019, s. 8) Kaiken tämän tarkoituksena on kauko-ohjatusti lähettää alitajuisia vihjeitä ja kohdistaa viestintää psykologisesti käyttäjään sekä asettaa oletusarvoisia valinta-arkkitehtuureja siten, että käyttäjien tietämättömyys säilyy (Zuboff, 2020, s. 5). Näistä edellä mainituista manipuloinnin keinoista käytetään englanninkielistä termiä nudge. Termin perusta on kognitiivisen psykologian kokeissa, joissa pyritään ymmärtämään ihmisten päätöksentekoa ja havaitaan huomattavia eroja sen välillä, miten yksilöt todellisuudessa tekevät päätöksiä ja miten päätöksentekotavat eroavat toisistaan. (Yeung, 2019, s.120) Digitaalisten aineistojen suunnittelun automatisoituessa, nämä aineistot väistämättä manipuloivat kuluttajia kaupallisen ja/tai poliittisen hyödyn saamiseksi. (Willis, 2020, s. 120)

Kuluttajien ja yritysten käyttämiä digitaalisia valintaympäristöjä on esimerkiksi erilaisilla verkkosivustoilla, mobiilisovelluksissa, peleissä ja ohjelmistoissa. Digitaalisissa yhteyksissä tehtävien päätösten kasvavan määrän vuoksi nudging on muodostunut lupaavaksi tietojärjestelmätutkimuksen alaksi, ja tutkijat ovat kiinnittäneet siihen yhä enemmän huomiota. Nudgingin lisäksi on olemassa digitaalista nudgingia. Digitaalisella nudgingilla tarkoitetaan käyttöliittymän suunnitteluelementtien hyödyntämistä ihmisten käyttäytymisen ohjaamiseksi digitaalisissa valintaympäristöissä ja heidän päätöksentekonsa parantamiseksi. (Mirsch, Lehrer & Jung, 2018, s. 2) Ihmiset joutuvat päivittäin tekemään valintoja, mutta valinnan lopputulokseen vaikuttavat paitsi rationaalinen harkinta käytettävissä olevista vaihtoehdoista myös valintaympäristön suunnittelu, jossa tiedot esitetään. Tämä voi vaikuttaa käyttäjän valitsemaan lopputulokseen alitajuisesti. Toisin sanoen se, mitä valitaan, riippuu usein siitä, miten valinta esitetään ja niin että valinta-arkkitehtuuri muuttaa ihmisten käyttäytymistä ennustettavalla tavalla. Jopa yksinkertaiset muutokset valintaympäristössä, jossa vaihtoehdot esitetään, voivat vaikuttaa ihmisten valintoihin ja saada heidät käyttäytymään tietyllä tavalla. Itse asiassa ei ole olemassa mitään neutraalia tapaa esittää valintoja. (Weinmann, Schneider & Brocke 2016, s. 433)

Perinteisen talousteorian mukaan ihmisten käyttäytyminen on rationaalista, mutta nudging toimii, koska ihmiset eivät aina käyttäydy rationaalisesti. Erityisesti psykologinen tutkimus on osoittanut, että kognitiivisten rajoitustensa vuoksi ihmiset toimivat rajoitetun rationaalisesti ja että erilaiset heuristiikat ja ennakkoluulot vaikuttavat heidän päätöksentekoonsa. Heuristiikat ovat "nyrkkisääntöjä", joita ihmiset käyttävät keventääkseen kognitiivista kuormitusta päätöksiä tehdessään. Heuristiikat voivat vaikuttaa päätöksentekoon myönteisesti tai kielteisesti. Niistä voi olla apua yksinkertaisten ja toistuvien päätösten tekemisessä, koska ne vähentävät käsiteltävän tiedon määrää, jolloin ihmiset voivat keskittyä eriytettyihin tekijöihin ja vähentää

henkistä ponnistelua. Määritelmän mukaan digitaalisessa nudgingissa keskitytään yksilöiden käyttäytymisen ohjaamiseen, mutta yksilöiden digitaalisen nudgingin vaikutukset voivat ulottua myös organisaation tai yhteiskunnan tasolle. (Weinmann, Schneider & Brocke 2016, s. 434)

Digitaalisissa ympäristöissä tapahtuvaa manipulointia käytetään yhä useammin vaikuttamaan reaali maailman käyttäytymiseen. Esimerkkinä tästä voidaan mainita aktiivisuusmittarit ja älykellot, joissa digitaalisia tönäisykeinoja (esimerkiksi muistuttaminen liikunnasta, palautteen antaminen aktiivisuudesta, ystävien tilastojen esittäminen) käytetään kannustamaan ihmisiä lisäämään aktiivisuuttaan. Digitaalisella nudgingilla on nähty olevan merkittävä vaikutus tulevaan tietojärjestelmätutkimukseen ja -käytäntöön, erityisesti suunnitteluorientoituneeseen tietojärjestelmätutkimukseen. (Weinmann, Schneider & Brocke 2016, s. 434)

Erityisen havainnollistavan esimerkin nudgingista tuo esiin vuonna 2016 Googlen kehittämä lisätyn todellisuuden peli Pokémon Go, joka testasi toimintataloutta kaduilla. Pelistä tuli läpimurtomenestys, ja se innoitti uutisointia pelin terveysvaikutuksista ja yhteisöllisyyttä lisäävästä voimasta. Peli oli kuitenkin vain hieno, söpö ja värikäs tapa kerätä valtavia määriä tietoa miljoonilta ihmisiltä. (Varghese, 2019) Pelin pelaajat eivät tienneet, että he olivat pelinappuloita todellisessa reaali maailman pelissä, jossa pelaajien käyttäytymistä muokattiin palvelemaan yritysten tarkoituksia. Pokémon-hahmojen metsästämisestä saatavia palkkioita ja rangaistuksia käytettiin ihmisten ohjaamiseen esimerkiksi McDonald'siin, Starbucksiin ja paikallisiin pizzapaikkoihin, jotka maksoivat yhtiölle kävijämääristä aivan samalla tavalla kuin verkkomainostajat maksavat klikkauksista verkkosivustoilleen. (Zuboff, 2020, s. 5). Toinen vastaava esimerkki käyttäjien manipuloinnista tapahtuu Google Maps -sovelluksessa sen navigointitoiminnon ja sen ehdottamien suositusten avulla. Kuljettajaa ei pakoteta toimimaan tietyllä tavalla, vaan Google Maps tarjoaa kuljettajalle ehdotuksia. Jos kuljettaja ei noudata ehdotettua suuntaa, Google Maps määrittää ohjauksensa uudelleen. (Yeung 2019, s.121-122)

Vuonna 2017 Facebookia koskevat dokumentit vuosivat julkisuuteen, ja niistä ilmeni, että Facebook halusi analysoida keräämästään datasta, milloin nuoret ovat tunteneet olonsa stressaantuneiksi, ahdistuneiksi tai esimerkiksi epäonnistuneiksi. Facebookin tarkoituksena oli tällä tavalla selvittää, kuinka tätä tietoa voitaisiin hyödyntää mainonnassa, ja tehdä siitä entistäkin tehokkaampaa. (Keller 2023, s. 148) Tämän tiedon avulla Facebook pystyi määrittelemään tarkalleen ajanjakson, jolloin nuori tarvitsee itseluottamuksen vahvistusta ja on alttiimpana tietyille alitajuisten vihjeiden ja laukaisimien yhdistelmälle. Tietoja on käytetty muun muassa sovittamaan kuhunkin tunnevaiheeseen sopivia mainosviestejä, jotta mahdollisimman suuri todennäköisyys myynnille saavutetaan. Facebook kiisti nämä toimintatavat. (Zuboff, 2020, s. 5-6)

Ahon ja Duffieldin (2020, s. 190) näkemyksen mukaan edellä kuvattu ei tarkoita sitä, että teknologia olisi muuttanut yksilön aivottomaksi automaatioksi, jonka vapaa tahto on alistettu dataoperaattoreiden ohjaamien algoritmien valtaan. Heidän mukaansa, kun yhä useammat ihmiselämän osa-alueet siirtyvät

analogisesta digitaaliseen, on kuitenkin tärkeää ottaa huomioon, että useimmat digitaaliset käyttöliittymät ovat yritysten kehittämiä, joiden motiiveina on ennen kaikkea voitto. Kun nudge-valmiudet lisääntyvät, näitä käyttöliittymiä suunnitellaan yhä enemmän käyttäytymisen muokkaamista silmällä pitäen.

### 2.3.3 Datan kerääminen mainosverkostoista

Valvonnan digitalisoituminen on muuttanut radikaalisti mainonnan luonnetta. Vanha järjestelmä, jossa mainostajat ostivat mainostilaa tai -aikaa mediasta siinä toivossa, että mediankäyttäjä huomaisi mainoksen, on muuttunut vanhanaikaiseksi. Mainostajien ei enää tarvitse tukea journalismia tai mediasisällön tuotantoa tavoittaakseen kohdeyleisönsä. Sen sijaan kaikkialle ulottuvan seurannan ansiosta, mainostajat voivat tavoittaa halutun kohdeyleisön ja paikantaa heidät sinne, missä he liikkuvat verkossa ja fyysisesti. (Foster & McChesney 2014, s. 23)

Google käynnisti kohdennetun verkkomainonnan alan, joka tunnetaan parhaiten valvontamainontana. Zuboff kuvaa sitä Troijan hevoseksi, joka kätkee sisäänsä monimutkaisen massiivisen louhinnan koneiston ihmisten tuottamaa tietoa (Zuboff, 2022, s. 11). Evästeet merkitsivät muutoksen alkua ja lopulta muokkasivat mainontaa ja sosiaalista huomiota verkossa enemmän kuin mikään muu keksintö itse selainta lukuun ottamatta (Turow, 2011, s. 47).

Verkkomainonnan avulla kerätään valtavia määriä dataa yksittäisillä klikkauksilla aina kun ihmiset käyttävät internetiä tai mobiilisovelluksia. Mainosverkostossa evästeiden avulla liikkuva tieto koskee muun muassa tietoa käyttäjän laitteesta ja selaimesta, sijainnista, aikavyöhykkeestä, sekä tietoa millä nettisivuilla käyttäjä on vierailut, ja mitä hän on tehnyt sivustolla. Näiden lisäksi evästeiden avulla kulkee käyttäjää koskevia demografiatietoja, kuten sukupuolta ja ikäryhmää koskevia tietoja sekä arvioita käyttäjän segmenteistä. Segmentit sisältävät tietoa esimerkiksi käyttäjän ostokäyttäytymisestä, asuuko käyttäjä omistusasunnossa vai vuokra-asunnossa, millainen tulotaso käyttäjällä on ja millaisia hänen kiinnostuksenkohteensa ovat ja niin edelleen. Segmentit vaihtelevat paljon tapauskohtaisesti. (Keller, 2023, s.144-145)

Yhdysvalloissa on tyypillistä, että yritykset korostavat sitä, ettei yritys myy käyttäjien henkilötietoja. Sillä yleisimmin tarkoitetaan sitä, että esimerkiksi mainosverkostoissa ei liiku käyttäjää tarkasti yksilöiviä tietoja. Mainosverkostoissa käyttäjää koskevat tiedot on yhdistetty tiettyyn cookie ID:hen tai user ID:hen. Tällä tavalla mainonta kohdennetaan oikein, vaikka mainosverkostossa toimivat yritykset eivät nimenomaisesti tiedä kuka käyttäjä on. Lisäksi on syytä nostaa esiin, että kaikki evästeet eivät liity mainontaan, vaan niillä on myös muita käyttötarkoituksia, kuten esimerkiksi muistaa nettisivulla käyttäjän tekemä kielivalinta sekä analysoida nettisivun toimivuuteen liittyviä ongelmia. (Keller, 2023 s. 145) Evästeiden kehittäjät tekivät tietoisien päätösten, jonka mukaan evästeiden oli tarkoitus toimia pyytämättä erikseen tietokoneen käyttäjää hyväksymään tai antamaan tietoja. Tällä lähestymistavalla on ollut kuitenkin kääntöpuolensa. Koska ohjelmoijat eivät vaatineet tietokoneen käyttäjältä lupaa evästeen hyväksymiseen, he laillistivat avoimuuden puutteen

ja asettivat sen keskelle kuluttajien ja yritysten välisiä digitaalisia liiketoimia (Turow, 2011, s. 48).

Digitaalisen markkinoinnin ja myynnin ihanteena on tarjota jokaiselle kuluttajalle ainutlaatuinen kokemus, joka on mikrotasolla kohdennettu kahdella tavalla. Se on personoitu kyseiselle kuluttajalle ja sen lisäksi se on optimoitu reaaliaikaisesti. Monilla yrityksillä ei ole yhtä ainoaa verkkosivustoa, vaan verkkosivuston etusivut, aloitussivut ja sisäsivut kootaan reaaliaikaisesti ja räätälöidään tietyyppisille kohdennetuille kuluttajille. Tämä pätee myös sovelluksiin. Aivan kuten henkilökohtainen myynti, digitaalinen teknologia romahduttaa markkinoinnin ja myynnin välisen eron. Mikrotargetoitu digitaalinen aineisto on samanaikaisesti sekä viestintää kuluttajille että käyttöliittymä, jonka kautta yritykset myyvät palveluitaan tai tuotteitaan. Verkkokäyttöliittymien suunnittelussa personointi tarkoittaa kaiken sen huomioon ottamista, mitä kuluttajista tiedetään tai voidaan päätellä heitä koskevista tiedoista, kuten esimerkiksi heidän tottumuksistaan, viimeaikaisista elämäntapahtumista sekä demografisista ja psykografisista profiileista. Nykyään teknologian avulla voidaan personoida sitä, mitä kullekin käyttäjälle milloinkin markkinoidaan sekä sitä, miten tuotetta tai palvelua markkinoidaan ja myydään. Reaaliaikaisesti optimoitu käyttöliittymä suunnitellaan sen perusteella, että kuluttajat reagoisivat yrityksen toivomalla tavalla. Tällaisia tekijöitä voivat olla esimerkiksi vuorokaudenaika, viikontähti tai vuorokaudenaika, sijainti, sää, kuluttajan tämänhetkinen toiminta ja tunnetila. Konsulttiyritys McKinsey on raportoinut, että datan aktivoima markkinointi, joka perustuu henkilön reaaliaikaisiin tarpeisiin, kiinnostuksen kohteisiin ja käyttäytymiseen, voi lisätä yrityksen kokonaisyntä 15-20 prosenttia. Eräessä kokeessa tutkijat havaitsivat, että jopa yhden bannerimainoksen räätälöinti lähes kaksinkertaisti kuluttajien klikkausten määrän. (Willis, 2020, s. 121-123)

### 3 VALVONTAKAPITALISMI JA KULUTTAJA

Yksityisyyden rajat ovat muotoutumassa uudelleen niin lainsäädännössä, yritystoiminnassa kuin tavallisten ihmisten arkielämässäänkin. Jotkut tutkijat käyttävät nimitystä notkean valvonnan aika. Olemme siirtyneet aikaan, jossa vaihdamme yksityisyytemme verkkoympäristössä toimiviin alustapalveluihin, jotka seuraavat meitä, tallentavat tekemisemme ja ajatuksemme, eikä meillä ole juurikaan mahdollisuutta vaikuttaa niiden toimintaan. (Sirkkunen & Haara, 2017, s. 7) Ihmisoikeudet ovat joukko oikeudellisesti kodifioituja normeja, jotka koskevat kaikkia ihmisiä kansallisista rajoista riippumatta. Kansainvälisessä ihmisoikeuslainsäädännössä asetetaan hallituksille velvoitteita toimia tietyllä tavalla tai pidättäytyä tietyistä teoista yksilöiden tai ryhmien ihmisoikeuksien edistämiseksi ja suojelemiseksi. Sinänsä se sääntelee yksilön ja valtion välistä suhdetta, mutta se ei suoraan sääntele yksityisen sektorin toimintaa, vaikka valtiolla onkin velvollisuus suojella yksilöitä ihmisoikeusloukkauksilta yksityisten tahojen toiminnassa. (Jørgensen, 2019, s. 19) Tässä luvussa käydään läpi kirjallisuudessa ja aikaisemmassa tutkimuksessa havaittuja kuluttajakäyttäytymisen ilmiöitä. Lisäksi luvussa esitellään kuluttajien tietosuoja sekä oikeutta yksityisyyteen, joka on määritelty jokaisen perus- ja ihmisoikeudeksi.

#### 3.1 Kuluttajakäyttäytyminen internetalustoilla

Sovellukset mahdollistavat paljon ja niiden avulla on saavutettu paljon hyvää. Mobiilisovelluksiin liittyy kuitenkin kääntöpuoli, josta monet kuluttajat eivät ole tietoisia, tai eivät välitä siitä. Keller on kuvannut kohdennetun mainonnan haittojen olevan tahdonvastainen puuttuminen käyttäjän elämänpäiiriin, kontrollin menettäminen käyttäjän omiin henkilötietoihin sekä käyttäjän autonomian menetys mainonnan avulla tehtävän manipuloinnin tai vaikuttamisen vuoksi. (Keller 2023, s. 147). Teknologian avulla yritykset voivat nykyään tuottaa lukuisia erilaisia verkkomainoksia, verkkosivustoja ja

sovelluksia. Nämä voidaan räätälöidä ja toimittaa valituille kuluttajille, tietyissä yhteyksissä ja tiettyinä aikoina. Onnistuneen mikrotargetoinnin avulla kuluttajat tavoitetaan niissä yhteyksissä ja siihen aikaan, kun he todennäköisimmin reagoivat yrityksen toivomalla tavalla. (Willis, 2020, s. 117-118)

Ihmiset tekevät monenlaisia päätöksiä tietokoneiden, tablettien ja älypuhelinien näyttöjen avulla. Päätökset vaihtelevat informatiivisen tai viihdyttävän sisällön valinnasta, ostosten ja taloudellisten investointien tekemiseen ja jopa oikean kumppanin valintaan. Verkkotoiminnassaan yksityishenkilöt joutuvat tekemään lisäksi yksityisyyttä ja turvallisuutta koskevia päätöksiä. Näitä päätöksiä ovat muun muassa näkyvyyden määrittely sosiaalisissa verkostoissa, päätös ladataanko sovellus tai luotetaanko verkkosivustoon sekä avataanko sähköpostissa ollut linkki vai jätetäänkö se huomiotta. Monet tekijät tekevät yksityisyyttä ja turvallisuutta koskevista päätöksistä erityisen monimutkaisia verkossa. Tietotekniikka ja verkkouhat kehittyvät jatkuvasti, minkä vuoksi käyttäjät ovat tilanteessa, jota taloustieteilijät kutsuvat epätäydelliseksi ja epäsymmetriseksi tiedoksi. Käyttäjien on usein vaikea määrittää, kuinka paljon heidän tietojaan kerätään ja miten niitä käytetään, ja heidän on lähes mahdotonta arvioida täysin, millaisille tietoturva- ja yksityisyydensuojaa koskeville haavoittuvuuksille he saattavat altistua, jos he päättävät olla vuorovaikutuksessa tietyn järjestelmän kanssa. Vaikka informaatiotulvan aikakaudella saatavilla olevan tiedon valtava määrä tarjoaa ennennäkemättömän määrän vaihtoehtoja, se ylittää usein yksilöiden kognitiivisen käsittelykyvyn. Lisäksi päätökset näytöillä tehdään usein hätäisesti ja lähes automaattisesti, mikä johtaa usein huonoihin valintoihin. Esimerkiksi kun ihmisille esitetään verkkosivustoilla lukuisia terveydenhuoltovaihtoehtoja, heidän kykynsä valita paras vaihtoehto on rajallinen. Psykologian ja käyttäytymistaloustieteen tutkimustulokset osoittavat, että tällaiset päätökset riippuvat suuresti heuristiikoista ja ennakkoluuloista sekä valintaympäristön suunnittelusta. Suositujen verkkopalvelujen ja -järjestelmien käyttöliittymät käyttävätkin joskus näitä heuristiikkoja ja ennakkoluuloja hyväkseen ja yllyttävät käyttäjiä toimimaan tavoilla, jotka eivät aina vastaa käyttäjien omia aikomuksia. (Acquisti ym., 2017, s. 2 ja Mirsch, Lehrer & Jung, 2018, s. 1)

Sirkkunen ja Haara (2017, s. 57-58) ovat tehneet tutkimuksessaan havainnon, että suurin osa ihmisistä haluaa tietää tarkemmin, mitä tietoja heistä kerätään ja mihin tarkoitukseen näitä koottuja tietoja kerätään. Heidän tutkimuksestaan ilmeni myös, että kuluttajat tutustuvat palveluiden käyttöehtoihin yleensä pintapuolisesti ja ne hyväksyttiin, jotta kuluttaja pääsee käyttämään palvelua. He myös totesivat tutkimuksessaan, että moni kuluttaja kokee, että käyttäjät on asetettu ota tai jätä -tyyppiseen tilanteeseen, jossa käyttäjä voi joko hyväksyä ehdot sellaisenaan tai ei käytä palvelua lainkaan. Heidän tutkimukseensa osallistuneista valtaosa on myös todennut, että dataa kerätään joka tapauksessa ilman, että asialle voi tehdä mitään. Kellerin (2023, s. 150-151) esiin tuoma esimerkki havainnollistaa edellä kuvattua kuluttajalle tarjottua valinnanvapautta. Mikäli kuluttaja haluaa lukea saksalaista sanomalehteä, ilmestyy hänen käyttämälleen laitteelle koko näytön kokoinen ikkuna, joka on



pienen tekstin peitossa. Näkymästä on lähes mahdotonta päästä eroon ilman, että perehtyy tekstiin edes hieman. Yleensä jo tässä vaiheessa kuluttaja turhautuu siihen, ettei pääse lukemaan haluamaansa uutista. Evästebanneri tarjoaa kuluttajalle kaksi eri vaihtoehtoa. Hän voi joko hyväksyä evästeet tai maksaa palvelusta kuukausimaksun. Mikäli kuluttaja maksaa kuukausimaksun, lehti ei seuraa häntä evästeiden avulla tai esimerkiksi kohdenna mainontaa kuluttajan onlinekäyttäytymisen mukaisesti. Tämä toimintapa ilmentää ”ilmaisen” palvelun taustalla olevaa bisneslogiikkaa, vaikka kuluttaja tulisikin tietoisesti siitä, mihin suostumuksensa antaa. Bisneslogiikka on joka tapauksessa se, että palvelu ei ole ilmainen. Se rahoitetaan kuluttajan henkilötiedoilla. Kuluttajan pohdittavaksi näin ollen jää, hyväksyykö hän henkilötietojensa laajan hyväksikäytön vai maksaako hän palvelusta. Kolmas vaihtoehto onkin, että kuluttaja ei saa lainkaan palvelua käyttöönsä.

Vaikka kuluttajat tekisivät päätöksen olla käyttämättä Facebookia, mutta käyttäisivät siitä huolimatta jotain toista Facebookin omistamaa palvelua (esimerkiksi Whatsappia tai Instagramia), saa Facebook silti näidenkin käyttäjien käyttäytymisdatan käyttöönsä (Nielsen, 2020). Ongelma on tätäkin suurempi ja monitahoisempi Googlen kohdalla. Kuluttaja voi päättää olla käyttämättä Googlea, mutta mikäli hän omistaa puhelimen, jossa on Android-käyttöjärjestelmä, se ei ole mahdollista. Google saa puhelimen avulla kuluttajan käyttäytymisdataa käyttöönsä. Myös internetin selaaminen ja tiedon hakeminen saattaa olla haastavaa ilman Googlea, koska Googlea käytetään monien selainten oletushakukoneena. Googlen Chrome-selain onkin yksi maailman suosituimmista internet-selaimista. (Nielsen, 2019)

Zuboffin näkemyksen mukaan valvontakapitalismi voidaan ymmärtää markkinoiden epäonnistumisena. Sen sijaan, että kysyntä ja tarjonta olisivat kohdanneet, ihmiset käyttävät näitä palveluja, koska heillä ei ole vastaavia vaihtoehtoja ja koska he ovat tietämättömiä valvontakapitalismin varjo-operaatioista ja niiden seurauksista. Pew Research Center on raportoinut, että 81 prosenttia amerikkalaisista uskoo, että yritysten tiedonkeruun mahdolliset riskit ovat suuremmat kuin hyödyt, mikä viittaa siihen, että yritysten menestys riippuu pikemminkin pakottamisesta ja tiedon pimittämisestä kuluttajalta kuin ihmisten todellisiin tarpeisiin vastaamisesta. (Zuboff, 2020, s. 7) Vastoin Zuboffin tulkintaa, Venkateshin näkemys on, että marxilainen tarina teollisuuskapitalisteista ja työntekijöistä on läheisesti yhteydessä valvontakapitalistisiin yrityksiin ja niiden käyttäjiin. Aivan kuten työläiset joutuvat myymään työvoimansa teollisuuskapitalisteille aineellisen toimeentulon tarpeen vuoksi, käyttäjillä on tarve sosiaaliseen osallistumiseen, jota he eivät pysty yksin tyydyttämään. Tämä tarve ajaa heidät myymään tietonsa valvontakapitalisteille. Kuten teolliset kapitalistit helpottavat työntekijöiden tarpeita palkoilla, valvontakapitalistit helpottavat käyttäjien tarpeita pääsyllä alustoilleen. (Venkatesh 2021, s. 3-4)

Informaatioteknologian professori Alessandro Acquisti on eräässä tutkimuksessaan selvittänyt opiskelijoidensa kanssa ihmisten halukkuutta maksaa tietosuojastaan. Hän lähetti ryhmän opiskelijoita ostoskeskukseen, jossa opiskelijat tarjosivat osalle vastaan tulevasta ihmisistä kymmenen dollarin

lahjakortin. Sen jälkeen opiskelijat tarjosivat näille henkilöille kaksi dollaria lisää, mikäli henkilöt suostuisivat siihen, että heidän ostoksiaan seurataan. Näistä henkilöistä puolet olivat kieltäytyneet kahden dollarin lisävaluutasta. Opiskelijat ottivat tarkasteltavakseen toisen ryhmän vastaan tulevia henkilöitä. Näille henkilöille he tarjosivat ensin 12 dollarin lahjakorttia, jonka jälkeen he tarjosivat mahdollisuuden vaihtaa kortti 10 dollarin lahjakorttiin, jolloin henkilö saisi käyttää rahat täysin anonyymisti. Tähän ryhmään kuuluneista henkilöistä 90 prosenttia valitsi pitää ensin tarjotun 12 dollarin lahjakortin, vaikka henkilö joutuisi paljastamaan lahjakortilla tekemänsä ostokset. Acquistin johtopäätöksen mukaan ensimmäisellä tarjouksella on suuri merkitys. Ensimmäisessä ryhmässä olleet henkilöt eivät halunneet antaa tietoja ostoksistaan, koska heillä oli lähtökohtaisesti omien tietojensa omistusoikeus. Toisella ryhmällä lähtökohta oli, että heillä ei ollut omistusoikeutta omiin tietoihinsa, ja sen vuoksi he eivät olleet halukkaita maksamaan siitä. Acquisti on havainnut tutkimuksissaan, että vaikka kuluttajat arvostavatkin omaa yksityisyyttään, he eivät ole valmiita maksamaan siitä. Kellerin mielestä on haastavaa määritellä hintaa omalle tietosuojalleen, etenkin kun kuluttajat eivät itse ole osapuolina omien henkilötietojensa kaupassa. Kuluttaja tekee tietosuojansa koskevia päätöksiä arkisissakin tilanteissa esimerkiksi tilanteessa, jossa kuluttaja käyttää kanta-asiakaskorttiaan kaupassa. Kyse on tietosuojapäätöksestä, mutta ei kuluttajan näkökulmasta tietoisesta sellaisesta, koska kuluttajalle tarjotaan sillä tavalla alennusta tuotteista. Kuten Acquistikin on tutkimuksissaan todennut, ihmisten tietosuojaa koskevat päätökset ovat liian helposti ohjailtavissa, jonka vuoksi tutkimustuloksista ei voida tehdä suoraa päätelmää, että ihmiset todellisuudessa pitävät oikeuttaan tietosuojaan arvossa. Esimerkiksi kohdennetun mainonnan ollessa monimutkainen järjestelmä, kuluttajien on lähes mahdotonta nykypäivänä ymmärtää, mihin he nimenomaisesti antavat suostumuksensa hyväksyessään nettisivuilla tai mobiilisovelluksissa olevat evästeet. (Keller, 2023, s. 149-150) Suostumussopimus on usein pelkkä rasti ruutuun tai allekirjoitettu paperi, jonka täydelliset ehdot ovat saatavilla verkossa ainoastaan pitkän URL-osoitteen kautta. Tällaisissa tapauksissa on vaikeampi väittää, että yksityisyyden suojasta on yhteisymmärryksessä luovuttu. Toisaalta Macnishin mielestä on kuitenkin otettava huomioon se, että mikäli henkilö antaa suostumuksensa yksityisten tietojen luovuttamisesta, hänellä ei ole oikeutta valittaa, jos vastaanottaja hyödyntää annettuja tietoja (Macnish, 2019, s. 11)

### **3.2 Kuluttajien tietosuoja ja yksityisyys**

Kuten edellä on kuvattu, yleistyvä verkottuminen tarkoittaa, että yhä enemmän tietoa on verkossa. Tietovarastot ovat entistä useammin saatavilla sähköisessä muodossa analysointia varten. On kehitetty uusia algoritmeja, joiden avulla voidaan poimia tietoa kerätystä tietomerestä. Nettotuloksena on, että uudenlaisia tietoja kerätään ja tallennetaan valtavia määriä ja pitkiksi ajoiksi, ja tietojen salaaminen tai vaikea saatavuus on yhä vähemmän käytännöllinen tapa

suojella yksityisyyttä. Koska tietotekniikan kustannukset laskevat jatkuvasti, yksityishenkilöiden, yritysten ja hallitusten käytettävissä on yhä enemmän tekniikoita, joilla voidaan kerätä ja analysoida henkilötietoja useista eri lähteistä. (Waldo, Lin & Millett, 2010, s. 6)

Yksityisyys on kansainvälisesti suojattu ihmisoikeus, joka muodostaa perustan sanan- ja yhdistymisvapaudelle, ja se on näin ollen demokraattisten yhteiskuntien yhdistävä tekijä ja keskeinen käsite, johon vedotaan haastettaessa lisääntyviä datavalvontakäytäntöjä (Cinnamon, 2017, s. 610). Westin (2003, s. 431) ja Keller (2023, s. 52) ovat määritelleet yksityisyyden suojan yksilön oikeudeksi määritellä, mitä tietoja hänestä pitäisi tulla muiden tietoon. Tähän liittyy myös se, milloin nämä tiedot ovat saatavilla ja miten muut niitä käyttävät. Kun yksityisyyden suojaa koskeva vaatimus tunnustetaan laissa ja sosiaalisissa sopimuksissa, voidaan puhua yksityisyyden suojaa koskevista oikeuksista.

Yksityisyyttä ja tietosuojaa suojataan Suomessa kansallisen lainsäädännön lisäksi kansainvälisillä ihmisoikeussopimuksilla, jolloin ne ovat sekä perus- että ihmisoikeuksia. Tietosuojan termi mielletään julkisessa keskustelussa usein samaan asiayhteyteen yksityisyyden kanssa. Monet mieltävät tietosuojan siten, että tietosuoja toteutuu, kun käsitellään mahdollisimman vähän ihmisten henkilötietoja. Keskeistä on kuitenkin se, että tietosuojan avulla varmistetaan henkilötietojen käsittely asianmukaisesti esimerkiksi sääntelemällä, kuka henkilötietoja käsittelee, kuinka kauan henkilötietoja saa säilyttää ja mitä tarkoitusta varten henkilötietojen käsittely tapahtuu. Myös yksityisyyden suoja usein mielletään virheellisesti siten, että kaikki henkilöä koskevat tiedot tulisi pitää salassa. Yksinkertaistetusti on mahdollista todeta, että tietosuoja on osa yksityisyyttä, jolloin yksityisyys on terminä tietosuojaa kattavampi. Toisesta näkökulmasta tietosuojalla suojataan yksityisyyden lisäksi myös monia muita perus- ja ihmisoikeuksia. Tietosuojan voidaan nähdä liittyvän yksityisyyden tiedolliseen puoleen eli henkilötietojen käsittelyyn, vaikka yksityisyys ei pelkisty ainoastaan tähän näkökulmaan. (Keller, 2023, s. 58-59) Aikaisemmin tehtyjen yksityisyyden merkitystä mittaavien kyselytutkimusten avulla on selvitetty, että verkon käyttäjät ovat huolissaan yksityisyyden menettämisestä sekä heitä koskevien henkilötietojen keräämisestä (Sirkkunen 2016, s. 118). Vaikka valvonnan kohteeksi joutuminen tai identiteettivarkauden uhkaaminen ovat selvästi uhkia yksityisyydelle, on sekä valvontatutkimuksen että big data -tutkimuksen piirissä syntyneessä yksimielisyys siitä, että datavalvontakäytäntöjen luonnehtiminen yksityisyyden loukkauksina on riittämätöntä ja se vie huomion pois muista vakavista sosiaalisista haitoista, joita voi syntyä, kun ihmiset ja heidän tietonsa erotetaan toisistaan (Cinnamon 2017, s. 611).

Lainsäädännön tasolla Suomessa ja Euroopassa tietosuoja ja tietoturva on nivottu yhteen tietosuoja-asetuksen eli GDPR:n tasolla. Se asettaa yrityksille velvoitteita asianmukaisten teknisten ja organisatoristen toimenpiteiden toteuttamiseksi, jotta henkilötietojen suojaaminen on mahdollista. (Keller, 2023 s. 55) GDPR:n mahdollisuudet yhtenäistää tietosuojan eettisiä periaatteita, erityisesti ihmisten käyttäytymiseen liittyvien tietojen osalta ovat rajalliset, koska

tietosuoja-asetuksessa olevat poikkeukset mahdollistavat väylän, jonka kautta yritykset voivat kiertää asetuksen rajoitukset. Andrew ja Barker ovat jopa väittäneet, että todellisuudessa asetus luo jopa tilaa käyttäytymistietomarkkinoille. (Andrew & Barker, 2021, s. 576)

Yksityisyyden suoja on monimutkainen kysymys, koska kyse on monista eri eduista. Jos tiedoilla ei olisi mitään arvoa kenellekään (ei keruuhetkellä eikä tulevaisuudessa) yksityisyyden suoja ei olisi ongelma, koska tietoja ei kerättäisi alun alkaenkaan. Joissakin tapauksissa yksityisyyden suojaamista koskevat paineet johtuvat kerättyjen tietojen käyttötarkoituksesta, ei itse tietojen keräämisestä. Yksityisyyden suojan näkökulmasta tämä korostaa yksilöiden kannalta merkittävää ongelmaa, koska tietojen lopullisten käyttötarkoitusten tunteminen voi olla vaikeaa tai jopa mahdotonta. (Waldo, Lin & Millett 2010, s. 7-8)

Yksi tunnetuimmista esimerkeistä yksityisyyden ja tietosuojan heikentymisestä tuli laajasti julkisuuteen Edward Snowdenin paljastusten myötä kesäkuussa 2013. Silloin paljastui, että useat suuret internetyhtiöt olivat antaneet tietoja sekä amerikkalaisista että eurooppalaisista käyttäjistään Yhdysvaltain NSA-turvallisuusvirastolle. Guardianin ja Washington Postin artikkelit julkaisivat sarjan paljastuksia Yhdysvaltojen ja muiden maiden kyseenalaisista verkkoseurantatoimista, mikä on horjuttanut luottamusta niin kansainvälisen tiedustelutoiminnan eettisyyteen kuin yksityisyyden turvaamiseen internetissä ja sen suosituimmissa palveluissa yleisesti ottaen. (Sirkkunen & Haara, 2017, s. 14) Yritysmailmassa on havaittu ongelma ”yksityisyyden paradoksin” kanssa. Paradoksi tarkoittaa sitä, että ihmiset väittävät arvostavansa yksityisyyttä, mutta antavat siitä huolimatta valtavasti henkilökohtaisia tietoja itsestään internetissä ilman minkäänlaista korvausta tai vain vähäistä korvausta vastaan. Yksityisyyttä koskevissa keskusteluissa käytetään usein ainakin kahta suosittua perustelua. Ensimmäisessä niistä yksityisyys nähdään turvallisuuden vastakohtana, jolloin pyrkimys on joko suojella yksityisyyttä tai taata turvallisuus. Tämä on nollasummapelejä, ja sen mukaan turvallisuus on yksityisyyttä tärkeämpää. Toisen perustelun mukaan, jos et ole tehnyt mitään väärää, sinulla ei ole mitään pelättävää yksityisyytesi heikentymisen puolesta. Ensimmäinen näistä perusteluista, yksityisyyden ja turvallisuuden asettaminen vastakkain, perustuu käsitykseen siitä, että valtio pyrkii kansalliseen tai yhteiskunnalliseen turvallisuuteen valvomalla kansalaisiaan. Toisen perustelun mukaan, jos et ole tehnyt mitään väärää, sinulla ei ole pelättävää valvonnan suhteen. Tämäkin väite epäonnistuu usealla tasolla. Ensinnäkin siinä oletetaan, että on olemassa objektiivinen väärän standardi, joka ei koskaan muutu. Näin ollen käytännössä vääräksi katsotulla asialla on usein poliittinen ulottuvuus. Väite asettaa perusteettoman suuren luottamuksen valvontaviranomaiselle. Macnishin mukaan ne, jotka kannattavat valvonnan lisäämistä tietyissä olosuhteissa, kuten terrori-iskun tai ilmiantajiin liittyvän vuodon yhteydessä, voivat käyttää näitä perusteluja vilpittömässä mielessä. Perustelujen puutteet osoittavat kuitenkin, että niitä ei pitäisi käyttää valvonnan lisäämisen tukena. (Macnish, 2019, s. 11-13)

Lisäksi Acquistin, Brandimarten ja Loewensteinin (2015, s. 513) mielestä yksityisyyden määrittelystä kansainvälisellä tasolla tekee haastavaa se, että yksityisyyttä ja julkisuutta koskevat normit ja käyttäytymismallit vaihtelevat suuresti eri kulttuureissa. Esimerkiksi amerikkalaisten sanotaan olevan avoimempia seksuaalisista asioista kuin kiinalaisten, kun taas kiinalaiset ovat avoimempia taloudellisista asioista, kuten tuloistaan, asunnon hinnasta ja omaisuudestaan. Kulttuurien sisälläkin ihmiset eroavat huomattavasti toisistaan siinä, kuinka paljon he välittävät yksityisyydestään ja mitä tietoja he pitävät ylipäättään yksityisinä. Näin ollen yksityisyyden suojaan liittyvät huolenaiheet voivat vaihdella huomattavasti yksilöiden ja yhteiskuntien välillä ajan myötä.

Yritykset, jotka seuraavat käyttäjiä internetissä kohdennettujen mainosten lähettämistä varten, ovat yksi suurimmista yksityisyyteen liittyvistä ongelmista (Blank, Dutton & Lefkowitz, 2019, s. 12). Kohdennettuun mainontaan liittyviä haittoja on tutkittu merkittävässä määrin, mutta siitä huolimatta tulevaisuus näyttää epäselvältä. Tästä herää kysymys, elämmekö yhteiskunnassa, jossa yksilöiden henkilötiedot ovat maksuvälineenä internetissä ja mobiilisovelluksissa, ja yksityisyyden vaihtaminen ilmaisiin palveluihin on yhteiskunnan yhteisesti tekemä valinta. Vaikka mainosverkostoissa toimivien yritysten näkökulmasta tieto on suurimmaksi osaksi anonyymiä tai pseudonyymiä, riski tietojen väärinkäytöstä syntyy, kun tietoa kerätään sadoilla evästeillä ja tieto liikkuu evästeiden kautta sadoille eri yrityksille. Vaikka evästeiden käytön avulla kerättyjä tietoja on lähes mahdotonta yhdistää tiettyyn henkilöön eikä niiden avulla tulisi kerätä henkilöiden sensitiivistä dataa, silti sitä voi tapahtua. Jos riittävästä tietoturvallisuuden tasosta ei huolehdi, data voi paljastua väärälle taholle esimerkiksi tietovuodon seurauksena. Tietosuojaa koskevissa artikkeleissa on tuotu esiin, että kohdennettu mainonta on vahingollista käyttäjien itsemääräämisoikeuden näkökulmasta etenkin tietovuotojen takia, koska kohdennettu mainonta tekee päätöksen käyttäjän puolesta siitä, millainen käyttäjä ylipäättään on tai mistä käyttäjä pitää. (Keller, 2023, s. 146-148)

Ennen digitalisaatiota yksityisyyden suojaan kohdistuvat loukkaukset olivat yksittäistapauksia, joista yleisimpiä olivat kirjesalaisuuden rikkominen, salakatselu, salakuuntelu tai salakuvaaminen. Viime vuosina yksityisyyden asemassa on tapahtunut monia muutoksia, jotka liittyvät talouteen, teknologiaan, sekä politiikkaan ja lainsäädäntöön. Nykypäivänä valvontateknologiat liittyvät ihmisten arkipäiväiseen elämään ja internetiä ja mobiileita viestintävälineitä voidaankin pitää kaikkein perusteellisimpina yksityisyyteen liittyvien rakenteiden ja käytäntöjen muuttajina. Asiantuntijat ovat nostaneet esiin, että yksityisyyttä ja tietoturvaa ei ole riittävästi otettu huomioon internetin kehitystyössä. (Sirkkunen & Haara 2017, s. 13-14) Nykypäivänä asianmukaisesti hoidetulla tietoturvalla on suuri merkitys tietosuojan ja yksityisyyden suojan varmistamisessa, koska suurin osa henkilötietojen käsittelystä tehdään digitaalisesti (Keller, 2023, s. 56).

## 4 VALVONTAKAPITALISMI JA YHTEISKUNTA

Shoshana Zuboffin mielestä valvontakapitalismi kaappasi digitaalisen maailman ja median ja hän kritisoi erityisesti sitä, että valvontapääoma ei näytä edistävän yritysten innovointia yhteiskunnan hyväksi. Valvontakapitalismin avulla kerättyä informaatiomäärää ei ole hänen mukaan esimerkiksi hyödynnetty yhteiskunnan kannalta kiireellisten haasteiden ratkaisemiseen, kuten hiilivapaan energian kehittämiseen, nälänhädän poistamiseen, syövän parantamiseen, valtamerten puhdistamiseen muovista tai maailman täyttämiseen hyvin palkatuilla, älykkäillä ja rakastavilla opettajilla ja lääkäreillä. Sen sijaan dataa käytetään tuottoisalle tieteelle ja taloudelle, joka liittyy ihmisten käyttäytymisen ennustamiseen ja siten yritysten voiton tavoittelemiseen. (Zuboff, 2020, s. 7) Tässä luvussa esitellään aikaisemmassa tutkimuksessa ja kirjallisuudessa tunnistettuja valvontakapitalismin haittavaikutuksia yhteiskunnallisesta näkökulmasta.

### 4.1 Teknologiajättien valta-asema

Elämme tällä hetkellä digitaalisella vuosisadalla tietosivilisaation muotoutumisvaiheessa. Aikamme on verrattavissa teollistumisen alkuaikoihin, jolloin omistajilla oli kaikki valta ja heidän omistusoikeutensa oli kaiken muun yläpuolella. Nykytilanne on, että Yhdysvallat ja monet muut demokraattiset valtiot ovat toistaiseksi luovuttaneet kaiken digitaalisen omistuksen ja päätösvallan yksityiseen valvontapääomaan poliittiselle taloudelle, joka kilpailee demokratian kanssa perusoikeuksista ja peruseriaatteista. (Zuboff, 2021b, s. 6) Tavallisesti suuret yrityskeskittymät on assosioitu yhteiskunnassa taloudelliseksi haitaksi. Kun ihmisten tietoja käytetään raaka-aineena ja ennusteet ihmisten käyttäytymisestä ovat tuotteena, haitat ovat enemmän sosiaalisia kuin taloudellisia. Oman haasteensa tuo se, että sosiaaliset ja taloudelliset haitat mielletään erillisinä, jopa toisiinsa liittymättöminä ongelmina, jolloin niiden ratkaiseminen on lähes mahdotonta. Sosiaalisia vaikutuksia

voidaankin pitää uutena epätasa-arvon muotona, joka ilmenee edellä kuvatulla tavalla epäsymmetriassa sen välillä, mitä yritykset tietävät käyttäjistään ja mitä käyttäjät tietävät yrityksistä. (Zuboff, 2021a, s. 8) Useissa yhteiskuntatieteellisissä teoksissa on todettu, että internet- ja alustayritysten monopolistisella poliittisella ja taloudellisella asemalla voi olla synkkiä ja odottamattomia seurauksia työntekijöille, kuluttajille ja valtioiden kansalaisille (Trittin-Ulbrich ym. 2021, s. 15).

Internetin alkuaikoina teknologian ajateltiin palvelevan sekä demokraattisia että taloudellisia tavoitteita, eikä tästä syystä teknologiaa tai siihen liittyviä innovaatioita haluttu rajoittaa. Näitä tavoitteita ajatellen sääntely pysyi vähäisenä ja yritysten vastuuvapauksien nojalla pyrittiin tilanteeseen, jossa mahdolliset oikeudelliset seuraukset eivät olleet esteenä innovaatioille teknologiassa ja liiketoiminnassa. Optimismi ja pyrkimys vapauteen ovat vaihtuneet sääntelytavoitteiden väliseksi taisteluksi, jossa valtioille on asetettu painetta puuttua suuryritysten valtaan. Internetin jatkuvaan kehitykseen liittyvä usko on hiipunut merkittävien viestintään liittyvien skandaaleiden ja kohujen seurauksena. Esimerkiksi vuoden 2016 Yhdysvaltojen presidentinvaalit, Iso-Britannian Brexit-kansanäänestys sekä monet sosiaalisen median alustoihin liitetyt skandaalit ovat muovanneet poliittista sekä yleistä ilmapiiriä alustoihin kohdistuvalle sääntelylle suotuisaksi. Skandaalien lisäksi alustojen ja internetin toimijoiden henkilötietojen käsittely on aiheuttanut suurta huolta. (Neuvonen, 2023, s. 1121-1122)

Kilpailun näkökulmasta se, että tietoa ja dataa hyödynnettäisiin laajamittaisemmin, olisi hyvä asia. Kun data keskittyy ainoastaan muutamien suurien yhtiöiden haltuun, se on vahingollista kilpailulle ja sillä on nähty olevan myös tietosuojaa heikentävä vaikutus. Google, Amazon, Facebook ja Apple ovat viimeisen noin 30 vuoden aikana ostaneet yhteensä 500 yritystä. Näiden monen teknologiayrityksen kasvun taustalla on ”acquire-copy-or-kill” -strategia. Sillä tarkoitetaan strategiaa, joka perustuu siihen, että yritykset seuraavat kilpailevien yritysten toimintaa, ja mikäli kilpailijan tuote tai palvelu on lähellä yrityksen omaa palvelua, pyritään kilpailija ostamaan pois markkinoilta. Mikäli kilpailijan ostaminen ei onnistu, yritys ryhtyy kopioimaan kilpailijan suosituimpia ominaisuuksia yrityksen omiin tuotteisiin tai palveluihin, tai muulla tavoin hankaloittamaan kilpailevan yrityksen toimintaa markkinoilla. Esimerkiksi vuonna 2013 Facebook yritti ostaa Snapchatin. Facebook ei tässä onnistunut, joten se kopioi Snapchatille ominaisen ja suosituksen Story-toiminnon Instagramiin. Lopulta tämä uusi ominaisuus saavutti nopeasti enemmän käyttäjiä Instagramissa kuin Snapchatissa. Snapchat on dokumentoinut Facebookin kilpailua vahingoittavia liikkeitä, mukaan lukien edellä mainitun tapahtumainkulun Project Voldemort -nimisessä hankkeessaan. Hankkeen tuloksia on hyödynnetty myös Yhdysvaltain kauppakomissio FTC:n tekemässä tutkimuksessa. (Keller 2022, s. 155)

Vuoden 2020 lopulla uutisoitiin, että Yhdysvaltojen liittovaltion ja osavaltiotason kilpailuviranomaiset olivat nostaneet kanteen Facebookia vastaan. Facebookia syytettiin kilpailusäännösten rikkomisesta sekä valta-aseman

väärinkäytöstä. (STT-Yle, 2020) Kilpailuviranomaiset vaativat, että Instagram ja Whatsapp tulisi irrottaa emoyhtiöstään kilpailutilanteen tasoittamiseksi. Lopulta kesäkuussa 2021 Facebook voitti oikeusjutun, kun Yhdysvaltain liittovaltion tuomioistuin hylkäsi syytteet yhtiötä vastaan. Tuomari oli tuomiossaan ottanut kantaa siihen, että kanne oli puutteellinen ja epäuskottava, eikä hänen mielestään kauppakomissio ollut esittänyt tarpeeksi todisteita väitteidensä tueksi siitä, että Facebookin emoyhtiö hallitsisi 60 prosenttia koko sosiaalisen median markkinaosuudesta. Edellä kuvattua päätöstä on pidetty merkittävänä takaiskuna amerikkalaisten poliitikkojen tavoitteille rajoittaa teknologiajättien valta-asemaa. (Rigatelli, 2021)

Zuboffin tapaan Macnish (2019, s. 9) on tuonut esiin, että yritysten tekemät yksityisyyden loukkaukset ovat lisääntyneet merkittävästi viimeisten 15 vuoden aikana sosiaalisen median tietojen myötä. Yritykset ovat voineet olla yhteydessä asiakkaisiin täysin uudella tavalla ja tarjota heille entistä henkilökohtaisempia palveluja. Toisaalta se on kuitenkin tarjonnut joillekin yrityksille ennennäkemättömän mahdollisuuden tutustua asiakkaiden elämään, joskus jopa ilman heidän tietämystään tai suostumustaan. Cambridge Analytica -skandaalin tapauksessa tällainen tunkeutuminen on johtanut yrityksiin manipuloida poliittista prosessia kohdennetulla ja erillisellä mainonnalla, joka perustuu tunnettuihin, mutta usein yksityisiin intresseihin. Maaliskuussa 2018 Christopher Wylie ilmiantoi entisen työnantajansa Cambridge Analytica -nimisen poliittisen konsulttiyrityksen. Hän myönsi tuolloin, että työnantajayrityksessään he hyödynsivät Facebookia kerätäkseen miljoonien ihmisten profiileja sekä rakensivat malleja, joiden avulla he hyödynsivät tietoa, jota olivat käyttäjistä saaneet. He myös kohdistivat tietonsa omien tarkoituspereensä mukaisesti käyttäjien ”sisäisiin demoneihin”. Wylie luonnehti näitä entisen työnantajansa tekniikoita informaationsodankäynniksi ja arvioi, että tällaiset varjosodat perustuvat tiedon ja sen tarjoaman vallan epäsymmetriaan. Yleisölle tai lainsäätäjille ei ollut selvää, että poliittinen konsulttiyritys käytti hyväkseen valvontakapitalismin vakiomuotoisia keinoja eli toimintatapoja, joille miljardeja käyttäjiä altistetaan rutiininomaisesti joka päivä. Cambridge Analytican todellinen innovaatio oli koko yrityksen kääntäminen kaupallisista päämääristä poliittisiin tavoitteisiin. (Zuboff, 2020, s. 6) Cambridge Analytica -skandaali kiinnitti maailman huomion Facebookiin uudella tavalla ja tarjosi mahdollisuuden muutokselle. Kansa alkoi ymmärtää, että Facebookin poliittinen mainonta on liiketoimintakeino ja sitä käytettiin kaupallisesti poliittisten tavoitteiden täyttymiseksi. Lisäksi on osoitettu, että Facebookin algoritmisen kohdentamisen mekanismeilla on syy-yhteys eripuraa aiheuttavan viraalin sisällön leviämiseen, joka on edistänyt jopa erilaisten ääriryhmien toimintaa (Zuboff, 2021b, s. 12).

Zuboff pitää erityisen vahingollisena teknologiajättien kasvavaa valtaa, jonka avulla ne pystyvät käyttämään määräysvaltaansa kriittisessä tietoinfrastruktuurissa kilpaillakseen demokraattisesti valittujen lainsäätäjien kanssa yhteiskunnallisesta valta-asemasta. Keskeinen esimerkki tästä on se, että koronaviruspandemian (COVID-19) alkuvaiheessa esimerkiksi Apple ja Google



kieltäytyivät mukauttamasta käyttöjärjestelmiään siten, että niissä voitaisiin käyttää kansanterveysviranomaisten kehittämiä sovelluksia. Facebook myös sulki monia sivujaan Australiassa merkkinä siitä, että se kieltäytyi neuvottelemasta Australian parlamentin kanssa uutissisällöstä perittävistä maksuista. (Zuboff, 2021a, s. 8)

Zuboff (2021a, s.9) summaa, kuinka Google, Facebook tai mikään muu tämän uuden talousjärjestelmän toimija ei ole lähtenyt tuhoamaan yhteiskuntaa sen enempää kuin fossiilisia polttoaineita tuottava teollisuus on lähtenyt tuhoamaan maapalloa. Kuten ilmaston lämpeneminen, myös teknologiajätit ja heidän kanssakulkijansa ovat olleet halukkaita kohtelemaan ihmisiin ja yhteiskuntaan kohdistuvia vaikutuksia sivullisina vahinkoina. Sivulliset vahingot ovat valitettavia, mutta väistämättömiä sivutuotteita taloudellisesta toiminnasta, joka on tehnyt näistä yrityksistä yksiä maailman rikkaimmista ja vaikutusvaltaisimmista yrityksistä kapitalismin historiassa. Banerjee (2008, s. 37) on Zuboffin kanssa yhtä mieltä siitä, että yrityksillä ei ole kykyä korvata valtioiden hallitusten roolia yhteiskunnallisen hyvinvoinnin edistämässä yksinkertaisesti siksi, että niiden yritystoiminta perustuu lähtökohtaisesti taloudellisiin tarpeisiin. Tästä syystä yritykset eivät voi korvata valtioiden hallituksia.

## 4.2 Väärä tieto ja sen leviäminen

Googlen valta-asema sananvapauden ja yksityisyyden suojan määrittelyssä on valtava. Google pystyy tekemään yksittäisiä päätöksiä siitä, mikä tieto on vanhentunutta tai epäasiallista. Se pystyy myös määrittämään, millä tiedolla on yhteiskunnallisesti merkitystä ja mitä hakutulosta ei tulisi poistaa. (Keller, 2023, s.126) Googlen, Facebookin, Applen, Microsoftin, Twitterin ja LinkedInin kaltaisilla yrityksillä on yhä tärkeämpi rooli sellaisten palvelujen ja alustojen hallinnoijina, jotka muokkaavat tehokkaasti normeja ja rajoja sille, miten käyttäjät voivat muodostaa ja ilmaista mielipiteitään, löytää tietoa, keskustella, olla eri mieltä, mobilisoida ja säilyttää yksityisyyden tunteensa. (Jørgensen, 2019, s. 18)

Yksi valvontakapitalismin haittavaikutuksista on nähty olevan se, että valvontakapitalismin avulla leviää merkittävässä määrin väärää tietoa. Kuten aiemmin on tuotu esiin, valvontakapitalismin logiikassa tiedon eheys ei ole yhteydessä tuloihin. Tällaisessa taloudellisessa toimintaympäristössä disinformaatio voittaa. Esimerkiksi Google, jonka tehtävänä on järjestää ja saattaa saataville tietoa, ei pysty erottamaan disinformaatiota tai korruptoitunutta tietoa faktatiedosta. (Zuboff, 2021a, s. 3-4) Lisäksi huomionarvoista on se, että yritysten pay-per-click -ominaisuuden avulla liiketoimintamalli asettaa etusijalle sisällön, joka on suunniteltu koukuttamaan käyttäjien huomio alustaan sen sijaan, että se tarjoaisi todenmukaista tietoa. Kun otetaan lisäksi huomioon se, että resursseja tiedon tarkastamiseen on rajallisesti, sosiaalisen median alustat priorisoivat viettelevää sisältöä, salaliittoteorioita,

klikkauskoukkuja (click-baitteja) sekä ääritietoja, koska sen avulla voidaan saavuttaa käyttäjien pitkäjänteisempää sitoutumista. Väärän tiedon lisäksi valeuutisten roolista on esitetty huolenaiheita. Valeuutisten keskeisenä ominaisuutena oleva tunnepitoinen sisältö ei ole sosiaalisen median tahaton seuraus, vaan osa sosiaalisen median liiketoimintamalleja ja sen keskeinen tulonlähde. Nämä organisaatiot haluavat usein välttää valtioiden sääntelyn ja tekevät siitä syystä mieluummin yhteistyötä ”faktojen tarkastajien” kanssa. Tällä tavalla he voivat välttää riskin siitä, että valtion hallitukset osallistuisivat entistä enemmän niiden toiminnan sensurointiin. Aitoa huolta on syntynyt myös siitä, miten valeuutisia voitaisiin määritellä poliittisesti neutraalilla tavalla, kun huomioidaan tämän aihepiirin keskustelun poliittisesti latautunut luonne. Lopulta tämä informaatiohäiriö sabotoi demokratian laatua ja sosiaalista yhteenkuuluvuutta vahingoittamalla ihmisten kykyä arvioida politiikkaa ja altistamalla käyttäjät harhaanjohtavalle sisällölle. (Butcher 2019, s. 3 ja Trittin-Ulbrich ym. 2021, s. 15)

Väärä informaatio (misinformation) voidaan määritellä yksinkertaisesti vääräksi, virheelliseksi tai harhaanjohtavaksi tiedoksi. Disinformaatio puolestaan tarkoittaa väärän, virheellisen tai harhaanjohtavan tiedon levittämistä tai väittämistä tarkoituksellisesti, tahallisesti tai pyrkimyksenä johtaa harhaan. Sitä voidaankin kuvata asenteelliseksi väärän tiedon levittämiseksi. (Fetzer 2004, s. 231) Disinformaation lisäksi valvontakapitalismin suurena haittana on havaittu valeuutiset. Valeuutiset määritellään väärennetyiksi tiedoiksi, jotka jäljittelevät uutismedian tuotoksia muodoltaan, mutta eivät organisatoriselta prosessiltaan tai tarkoitukseltaan. Valeuutiset eivät etenäkään vastaa uutismedian toimituksellisia normeja ja prosesseja, joilla varmistetaan tiedon oikeellisuus ja uskottavuus. Se on erityisen haitallista, koska se heikentää tavanomaisten uutistoimistojen uskottavuutta. (Lazer ym. 2018, s. 2) Gelfertin (2018, s. 86-87) mukaan epistemologiassa on korostettu, että uutismediaa pidetään luotettavana kuluttajille suunnatun faktatiedon lähteenä. Artikkelin mukaan kuluttajat luottavat esimerkiksi New York Timesiin tai BBC World Newsiin arvovaltaisina faktakertomusten lähteinä maailmasta. Lisäksi epistemologian näkökulmasta oletetaan, että pätevä lukija pystyy erottamaan tosiseikkoja sisältävät raportit mielipidekirjoituksista ja käyttäjä luotettavuuden arvioinnissa samoja perusmenetelmiä kuin arvioidessaan luotettavan ja pätevän keskustelukumppanin kertomusta.

Kun ihmisiä johdetaan harhaan tärkeistä asioista, kuten sijoitusmahdollisuuksista, lääketieteellisistä hoidoista tai poliittisista ehdokkaista, se voi aiheuttaa vakavaa henkistä, taloudellista ja jopa fyysistä vahinkoa. Epätarkat tiedot (tai väärät tiedot) voivat johtaa ihmisiä harhaan riippumatta siitä, johtuvatko ne inhimillisestä virheestä, huolimattomuudesta, tiedostamattomasta ennakkoluulosta vai (kuten disinformaation tapauksessa) tarkoituksellisesta harhaanjohtamisesta. Samalla tavalla kuin terroriteot ovat yleensä huolestuttavampia kuin luonnonkatastrofit, disinformaatio on erityisen ongelmallinen väärän tiedon muoto, koska ihmisiä ei johdeta harhaan sattumalta. Toisin kuin rehellinen erehdys, disinformaatio on peräisin henkilöltä, joka pyrkii

aktiivisesti harhauttamaan muita ihmisiä. Sen lisäksi, että disinformaatio aiheuttaa suoraa haittaa, se voi vahingoittaa ihmisiä myös epäsuorasti heikentämällä luottamusta ja estämällä siten kykyämme jakaa tehokkaasti tietoa keskenämme. (Fallis, 2015, s. 402)

Vaikka väärää tietoa ja propagandaa on ollut olemassa jo muinaisista ajoista lähtien, niiden merkitys ja vaikutus sosiaalisen median aikakaudella ei ole vieläkään selvä. Maailman talousfoorumin vuonna 2013 julkaisemassa raportissa massiivinen digitaalinen väärän tiedon levittäminen on nimittäin luokiteltu merkittäväksi teknologiseksi ja geopoliittiseksi riskiksi. Monet tutkimukset ovat viime aikoina tutkineet väärää tietoa sosiaalisissa verkostoissa, kuten Facebookissa, Twitterissä, YouTubea ja Wikipediassa. Näiden tutkimusten ja teoreettisen mallintamisen perusteella voidaan olettaa, että sosiaalisen vaikuttamisen ja vahvistusvinouman seurauksena sosiaalisiin verkostoihin syntyy käyttäjäyhteisöjä, jotka jakavat samankaltaiset uskomukset tietyistä aiheista. Uskomuksiin perustuvat totuudenmukainen informaatio ja perättömät väitteet leviävät yhtä todennäköisesti viraaliksi. (Bovet & Makse, 2019 s. 2) Marwickin ja Lewisin (2017, s. 26) mukaan äärioikeistolaiset käyttävät valtavirran sosiaalisen median sivustoja, kuten Twitteriä, Facebookia ja YouTubea levittääkseen viestejä suurille ihmisjoukoille ja saadakseen aiheita toimittajille. Facebookissa yksityiset ryhmät jakavat meemejä, joita sitten levitetään edelleen henkilökohtaisissa verkostoissa. Äärioikeistolaiset toimijat käyttävät usein hyväkseen Twitterin trending topics -ominaisuutta vahvistaakseen tiettyjä tarinoita tai viestejä. Myös YouTube tarjoaa foorumin salaliittoteoreetikoille ja marginaaliryhmille, jotka voivat tehdä vakuuttavia ja kiinnostavia videoita provosoivista aiheista. Tapaustutkimuksissa on annettu konkreettisia esimerkkejä äärioikeistolaisista toimijoista, jotka käyttävät valtavirran sosiaalisen median sivustoja lisätäkseen haluamiensa viestien näkyvyyttä. Vuonna 2018 Science-lehti julkaisi MIT:n tekemän tutkimuksen, jossa analysoitiin jokainen merkittävä kiistanalainen englanninkielinen uutinen Twitterin koko olemassaolon ajalta. Noin 126 000 tarinaa, jotka 3 miljoonaa käyttäjää twiittasi yli 10 vuoden aikana. Tutkimuksessa havaittiin, että totuus ei yksinkertaisesti pysty kilpailemaan huijausten ja huhujen kanssa. Tutkimuksen mukaan kaikilla yleisillä mittareilla mitattuna valheellisuus on Twitterissä johdonmukaisesti totuuden yläpuolella. Valeuutiset ja väärät huhut tavoittavat enemmän ihmisiä, tunkeutuvat syvemmälle sosiaaliseen verkostoon ja leviävät paljon nopeammin kuin oikeat tarinat. Tutkimuksen tekijät niin ikään totesivat, että väärä tarina leviää paljon todennäköisemmin kuin oikea tarina. Väärä tarina tavoittaa 1 500 ihmistä keskimäärin kuusi kertaa nopeammin kuin oikea tarina. Poliittikkaa koskevat valeuutiset menestyvät säännöllisesti parhaiten, vaikka valheelliset tarinat ovat totuuden yläpuolella lähes kaikissa muissakin aiheissa, kuten liike-elämässä, terrorismissa ja sodassa, tieteessä ja teknologiassa sekä viihteessä. (Meyer, 2018, s. 1)

Havainnollistava esimerkki disinformaation haitallisuudesta on Pizzagate-tapaus. Pizzagate-nimellä tunnettu salaliittoteoria sai kulttiyleisön äärioikeistolaisilla foorumeilla, ja lopulta eräs teoriaan uskova henkilö ryhtyi

ampumaan salaliittoteoreetikkojen leimaamaa pizzeriaa (Bleakley, 2023, s. 509). Tapauksessa Edgar Welch ajoi Pohjois-Carolinasta Washingtoniin pelastaakseen väitetyksi seksuaalisesti hyväksikäytettyjä lapsia, joiden hän uskoi olevan piilossa tunneleissa pizzerian alla. Hän ei kuitenkaan löytänyt piilotettuja lapsia, tunneleita tai todisteita lapsiseksiringistä ja huhut olivat valheellisia. (Fisher, Cox & Hermann, 2016, s. 1-2) Kuten monet muutkin internetin aikakauden salaliittoteoriat, Pizzagate sai alkunsa legitiimien ilmiantojen ja väärän tiedon tarkoituksellisen levittämisen yhtymäkohdasta. (Bleakley, 2023, s. 516) Tapaus osoittaa myös, millaista häirintää ja väkivaltaa voi syntyä reaali maailmassa suorana seurauksena median manipuloinnista ja vääränlaisesta tiedosta verkossa. (Marwick & Lewis, 2017, s. 55).

Kuten todettua, käyttäjien tuottamat valeutiset ja tekaistu verkkohuomio ovat sosiaalisen median botteja ja tekoälyä hyödyntävän puoliautomaattisen verkkopolitiikan ilmentymiä. Big datan maailmassa on tullut entistä vaikeammaksi erottaa, mitkä toimet ovat ihmisten ja mitkä bottien ja algoritmien käynnistämiä. Tämä algoritmisen politiikan ja äärioikeistolaisen ideologian yhdistyminen on lisännyt politiikan arvaamattomuutta. Moni ei esimerkiksi uskonut, että Donald Trumpista tulisi Yhdysvaltain presidentti, mutta galluppien ennustemallit pettivät. (Chandler & Fuchs, 2019, s. 48) Yhdysvaltojen presidentinvaalien lisäksi Brexitin aikana esiintyi erilaista valeutisointia, jotka olivat peräisin pääasiassa sosiaalisesta mediasta. Huoli valeutisista moninkertaistui vuonna 2020, kun sosiaalisessa mediassa levitettiin laajalti väärää tietoa ja disinformaatiota vuoden 2019 koronavirus-pandemiasta. (Dentith, 2016 s. 75 ja Pennycook & Rand 2021, s. 388) Helmikuussa 2020 Maailman terveysjärjestö WHO raportoi koronaviruspandemian yhteydessä levinneestä infodemiasta. Infodemia tarkoittaa tilannetta, jossa sosiaalisessa mediassa ja muualla internetissä on liikkeellä valtavia määriä epäluotettavaa ja virheellistä tietoa, joka leviää epidemianomaisesti (World Health Organization (WHO), 2024). Maaliskuuhun 2020 mennessä Texasin yliopiston M.D. Andersonin syöpäkeskuksen tutkijat huomasivat, että koronavirukseen liittyvää lääketieteellistä väärää tietoa on levinnyt hälyttävällä vauhdilla sosiaalisessa mediassa vaarantaen yleisen turvallisuuden (Zuboff, 2021b, s. 16).

Kysymykset väärän tiedon leviämisestä johtavat loogisesti kysymyksiin sen vaikutuksista. Jos väärä tieto voi levitä nopeasti ihmisten ja teknologian ennakkoluulojen avustamana, kuinka suuri vaara siitä lopulta aiheutuu? Miten ja missä määrin se vaikuttaa altistuneisiin? Facebookin lisäksi verkossa on useita väärää tietoa levittäviä paikkoja. Esimerkiksi Reddit, Pinterest ja YouTube ovat vielä liian vähän tutkittuja suhteessa niiden käyttäjäkunnan kokoon. Samaan aikaan väärän tiedon kulkua useilla eri alustoilla ei ole toistaiseksi tutkittu lainkaan. Laajemmin ottaen tarvitaan tutkimusta jakamisen taustalla olevasta käyttäytymisestä. (Guess & Lyons, 2020 s. 23-24) Valeutisten maailmanlaajuinen tunnettuus kasvaa jatkuvasti, ja yhä useammat tutkimukset ovat tarkastelleet ongelman eri ulottuvuuksia, kuten valeutisten kulutuksen laajuutta, valeutisten levittämisen taustalla olevia motiiveja ja sisältöä sekä sosiaalisen median mahdollisuuksia valeutisten kumoamiseksi. Vaikka yleisö

on yleisesti ottaen samaa mieltä valeuutisongelman vakavuudesta, keskusteluissa siitä, mitä valeuutiset tarkalleen ottaen ovat ja kenen pitäisi olla niistä vastuussa, esiintyy edelleen erimielisyyksiä ja epäselvyyksiä. (Li, & Su, 2020 s. 1-2).

## 5 TUTKIMUSMENETELMÄ

Tutkielman teoriaosuus käsitteli valvontakapitalismin määritelmää, valvontakapitalismin kehitystä sekä sen liiketoimintaperiaatetta. Kirjallisuuskatsauksessa perehdyttiin myös aikaisemman tutkimuksen ja aihetta koskevan kirjallisuuden avulla valvontakapitalismin vaikutuksiin kuluttajakäyttäytymisen näkökulmasta sekä tuotiin esiin valvontakapitalismin vaikutuksia kuluttajan ja yhteiskunnan näkökulmasta. Kuluttajakäyttäytymisen näkökulmasta keskeistä on, että ihmiset tekevät monenlaisia päätöksiä tietokoneiden, tablettien ja älypuhelimien näyttöjen avulla. Näillä päätöksillä on kuluttajan näkökulmasta merkitystä myös käyttäjien yksityisyyden ja turvallisuuden kannalta. Erityisen ongelmallista tästä tekee se, että käyttäjille tarjottava valinnanvapaus ei tarjoa käyttäjille todellista vapautta valita, vaan kyseessä on ota tai jätä -tyyppinen tilanne. Kuluttajan näkökulmasta valvontakapitalismin keskeiset vaikutukset liittyvät kuluttajien tietojen keräämisestä ja eteenpäin myymisestä aiheutuviin yksityisyyden loukkauksiin. Yhteiskunnan kannalta kirjallisuudessa havaittuja haittavaikutuksia ovat ennen kaikkea teknologiajätien valta-asema ja disinformaation leviäminen. Näillä vaikutuksilla on nähty olevan merkittäviä vaikutuksia myös demokratian heikentymisen kannalta. Kirjallisuuskatsaus muodosti tutkimuksen teoreettisen viitekehyksen. Tässä luvussa käydään läpi tutkimuksen empiirisen osan taustaa, valittua tutkimusmenetelmää ja tutkimuksen toteutusta. Lopuksi käydään läpi empiirisen tutkimuksen luotettavuutta.

### 5.1 Lähestymistavan valinta

Valvontakapitalismia tutkittiin kuluttajan näkökulmasta käyttäen laadullista tutkimusmenetelmää. Laadullinen menetelmä valittiin, koska haluttiin saada syvälinen ymmärrys kuluttajien mielipiteistä aiheeseen liittyen ja koettiin, että se ei ole mahdollista pelkästään kvantitatiivisen tutkimuksen avulla. Hirsjärvi, Remes ja Sajavaara (1997, s. 161) puoltavat ajatusta siitä, että kvantitatiiviset

menetelmät soveltuvat paremmin tarkasti määriteltäisiin kysymyksiin, kun taas kvalitatiiviset menetelmät ovat hyödyllisiä laajemman näkökulman saamiseksi aiheesta. Laadullisessa tutkimuksessa ei ole tarpeen selvittää kuinka paljon tai kuinka todennäköisesti käyttäjät ajattelevat tietyllä tavalla, vaan keskitytään vastaamaan kysymyksiin *mitä* ja *miksi*. Laadullisen tutkimuksen yksityiskohtaisuus on haaste, mutta se on myös mahdollisuus. Sen avulla voidaan kuvata mielenkiintoisia ilmiöitä yksityiskohtaisesti, tutkimukseen osallistuvien alkukielellä. Vaikka yksityiskohtaisuutensa vuoksi tutkimuksessa voi olla haastavaa tunnistaa yleisempiä teemoja, laadullinen tutkimus sopii erityisen hyvin ihmisten kokemusten tutkimiseen. (Trochim, 2020)

Laadullisessa tutkimuksessa teoria toimii aineistonkeruun pohjana. Teoriasta nousseet haastattelukysymykset pyrkivät varmistamaan, että tutkittava aihe käsitellään monipuolisesti, eikä haastattelu perustu pelkästään tutkijan henkilökohtaisiin mielenkiinnon kohteisiin. Teoria myös syventää tutkijan ymmärrystä tutkittavasta ilmiöstä ja auttaa rajamaan tutkimuskohdetta sekä luomaan perustaa aineistonkeruulle. (Puusa & Juuti, 2020, s. 83–84.) Tutkimushaastattelu voidaan nähdä vuorovaikutteisena keskusteluna, jonka päämääränä on kerätä aineistoa, joka mahdollistaa vakuuttavien päätelmien tekemisen tutkittuun aiheeseen liittyen (Puusa & Juuti, 2020, s. 103)

Tutkimus toteutettiin puolistrukturoidulla haastattelulla. Puolistrukturoitu haastattelu on yksi laadullisen tutkimuksen tutkimusmenetelmistä. Puolistrukturoitu haastattelu antaa enemmän vapautta verrattuna täysin strukturoituun haastatteluun, mikä mahdollistaa myös sellaisten asioiden esiintuomisen, joita tutkija ei välttämättä ole vielä huomionnut haastattelua suunnitellessaan (Kallio ym., 2016 ja Puusa & Juuti, 2020, s. 111–112).

Seuraavassa luvussa kuvataan yksityiskohtaisemmalla tasolla aineiston hankintaa ja siinä käytettyjä menetelmiä ja sitä seuraavassa alaluvussa tarkastellaan aineiston analysointiin liittyviä menetelmiä.

## 5.2 Aineiston hankinta

Haastateltavat olivat milleniaaleja, eli tällä hetkellä noin 25–38-vuotiaita henkilöitä, jotka tunnetaan myös nimellä Y-sukupolvi (McCrindle, 2003, s. 1). Milleniaalit ovat eläneet muutoksen keskellä ja he ovat eläneet myös aikaa ennen älylaitteiden ja internetalustojen vallankumousta. Tästä syystä tutkielmassa haluttiin tarkastella heidän kokemuksiaan sekä selvittää heidän tietämystään aihepiiriin liittyen. Haastatteluun osallistui kaikkiaan kahdeksan henkilöä. Ennen varsinaisten kahdeksan haastattelun aloitusta yksi testihaastattelu suoritettiin etukäteen, jotta nähtiin, että kysymykset toimivat, niin kuin niiden oli tarkoitus toimia. Harjoituskierroksen avulla pystyttiin myös arvioimaan haastattelun kestoa henkilöä kohden, jotta haastateltaville oli mahdollista informoida haastatteluun kuluva aika. Myös Hirsjärvi et al. (1997, s. 211) suosittelivat haastattelun testaamista etukäteen, jotta sitä voidaan tarvittaessa

muokata ja testihaastattelun avulla saadaan pilotoitua, kuinka haastattelu sujuu kokonaisuudessaan.

Laadullisen tutkimuksen suhteen ei ole olemassa yleispätevää lukumäärää siitä, minkä kokoisella otantajoukolla taataan riittävä tai hyvä tutkimustulos (Hirsjärvi, Remes & Sajavaara, 2009, s. 179-182). Kahdeksan henkilön otannan katsottiin kuitenkin riittäväksi saturaation nojalla. Saturaatiolla tarkoitetaan tilannetta, jossa haastatteluista ei enää saada uutta tietoa, vaan ne alkavat toistaa jo aiemmissa haastatteluissa esiin nousseita asioita (Eskola & Suoranta, 1998, s. 62-63).

Haastattelukysymykset luotiin tutkimuksen tutkimuskysymysten ja kirjallisuuskatsauksen pohjalta. Puolistrukturoidussa haastattelussa haastateltavat sanoittavat omat näkemyksensä, niin kuin he itse asiat kokevat (Puusa & Juuti, s. 2020, 112). Tästä syystä kysymykset asemoitiin niin, että haastateltavalla oli mahdollisuus vastata kysymyksiin omien kokemusten sekä tietämyksensä pohjalta. Tutkijalla oli omat apukysymykset, joiden avulla varmistettiin haastattelun sujuvuus ja pyrittiin löytämään monipuolisia vastauksia. Apukysymysten avulla pystyttiin nostamaan esille esimerkkejä ja käytännön tilanteita, jos vastaajalla ei heti tullut mieleen vastausta. Liitteessä 1 on nähtävillä tutkimuksessa käytetyn haastattelun kysymykset.

Haastattelut toteutettiin maaliskuun 2024 aikana. Haastattelut olivat yksilöhaastatteluja ja ne tehtiin videopuhelun tai tavallisen puhelun välityksellä. Haastattelut järjestettiin etänä, mikä helpotti ja nopeutti sekä haastattelun toteutusta että aikatauluttamiseen liittyviä haasteita molempien osapuolten kannalta. Tutkimusjoukkoon valikoitiin ihmisiä tutkimuksen tekijän lähipiiristä, joiden tiedettiin käyttävän erilaisia internetin alustapalveluita aktiivisesti arjessaan. Haastattelut nauhoitettiin myöhempää läpikäyntiä varten ja haastattelut kestivät 45-75 minuuttia. Osallistujia informoitiin haastattelun nahoituksesta ja siihen pyydettiin suostumus. Haastateltavia informoitiin myös vastausten anonymisoinnista lopullisen tutkielman suhteen. Osallistujilla oli oikeus peruuttaa osallistumisensa tutkimukseen milloin tahansa, myös haastattelun aikana. Haastattelun aikana kysyttiin tarvittavia apukysymyksiä, kuitenkin niin, ettei haastateltavia johdateltu heidän vastauksissaan.

### 5.3 Tutkimusaineiston analysointi

Laadullisen tutkimusmenetelmän valinnan vuoksi myös aineistoa analysoitiin laadullisen menetelmän avulla (Bhattacharjee, 2012, s. 23). Aineiston analysointi voi osoittautua vaativaksi, sillä yleispätevää ohjetta, joka soveltuisi kaikkeen aineistoon, ei ole (Hirsjärvi & Hurme, 2017, s. 35). Haastatteluiden analysoinnissa havaitaan erilaisia vaiheita, jotka voidaan jaotella aineiston luokitteluun, analysointiin ja tulkintaan (Nikander ym., 2010). Nämä vaiheet ovat tiiviisti yhteydessä toisiinsa ja voivat osittain tapahtua päällekkäin eri analyysimenetelmissä. Haastattelujen jälkeen suoritettiin tarkka litterointi, missä kaikki haastattelut muutettiin kirjalliseen muotoon. Nikanderin ym., (2010)



mukaan, äänitallenteet tai videot, jotka ovat peräisin laadullisesta tutkimuksesta, tulisi litteroida tekstiksi, jotta tutkijan olisi helpompaa hallita ja jatkojalostaa aineistoa. Aineiston keräämisen ja analysoinnin prosessi eteni siten, että ensin haastattelut muutettiin tekstiksi, sitten niitä luettiin läpi, teemoiteltiin, luokiteltiin, yhdisteltiin ja lopuksi tulokset raportoitiin. Ensimmäisessä vaiheessa haastattelut litteroitiin huolellisesti tallenteista tekstimuotoon, mikä on yleinen käytäntö laadullisessa tutkimuksessa. Haastattelut ja keskustelut litteroitiin kokonaisuudessaan ja tarkistettiin mahdollisten virheiden varalta. Aineisto luettiin perusteellisesti. Hirsjärven ja Hurmeen (2008, s. 143) mukaan tämä on välttämätöntä ennen analyysin aloittamista. Lukemisen tarkoituksena oli herättää ajatuksia ja kysymyksiä aineistoa kohtaan. Lukemisen jälkeen siirryttiin teemoitteluun ja luokitteluun, jossa aineistosta nousi esiin olennaisia teemoja tutkimuksen kannalta. Teemoittelussa hyödynnettiin koodaamista teemojen merkitsemiseen, mikä auttoi analyysin selkeyttämisessä (Saaranen-Kauppinen & Puusniekka, 2006). Samankaltaiset teemat koottiin yhteen helpottamaan luokittelua, joka on olennainen osa analyysia (Hirsjärvi & Hurme, 2008, s. 147). Luokittelussa havaittiin samankaltaisuuksia aiempien tutkimusten kanssa, mutta myös uusia näkökulmia. Luokkien yhdistelyssä pyrittiin löytämään säännönmukaisuuksia ja karsimaan epäolennaisia luokkia (Hirsjärvi & Hurme, 2008, s. 149). Yhdistely helpotti tulosten raportointia, jotka esitellään seuraavassa luvussa.

## 5.4 Tutkimuksen luotettavuus

Tutkimuksen luotettavuutta arvioidaan perinteisesti määrällisessä tutkimuksessa reliabiliteetin ja validiteetin avulla. Reliabiliteetti viittaa tutkimuksen kykyyn tuottaa samanlaisia tuloksia, kun tutkimus toistetaan uudelleen. (Hirsjärvi & Hurme, 2015, s. 186). Validiteetti jaetaan sisäiseen ja ulkoiseen validiteettiin. Sisäinen validiteetti tarkoittaa sitä, että tutkimus kohdistuu siihen, mitä sen pitikin tutkia ja ulkoinen validiteetti liittyy tulosten yleistettävyyteen. (Hirsjärvi & Hurme, 2015, s. 187-188). Laadullisessa tutkimuksessa nämä ovat kuitenkin samassa merkityksessä kiistanlaisia käsitteitä, ja tutkimuksen suhteen näitä ominaisuuksia on mahdollista arvioida laadullisten keinojen kautta. Laadullisen tutkimuksen luotettavuutta on siten suoritettava arvioiden kautta. Tästä syystä tutkimuksen toteutus on pyritty kuvaamaan lukijalle mahdollisimman kattavasti ja aineistonkeruun ja analyysin menetelmät on tuotu lukijalle esiin. Lisäksi valittujen keskeisten käsitteiden käyttö tutkimuksessa on perusteltu ja ne on sidottu tarkastelussa olevaan näkökulmaan. Kun tehdään tulkintoja aineistoista, käsitteiden määrittely auttaa arviomaan, pohjaavatko johtopäätökset tarkoin määriteltäviin käsitteisiin. Haastattelukysymykset tuottivat yhtenäisiä vastauksia ja lisäksi käytetty haastattelurunko on sisällytetty tähän työhön sekä liitteeksi (liite 1). Kirjallisuuskatsausta rikastettiin teemahaastattelulla, joka keskittyi tunnistettuihin kirjallisuuden teemoihin. Tutkimuksessa hyväksyttiin, että

tulokset voivat vaihdella eri aikoina ja paikoissa sekä se, että ihminen on luonteeltaan muuttuva ja tästä syystä täydellistä tulosten yleistettävyyttä ei odotettu. Tutkimus tarjoaa kuitenkin arvokasta tietoa kuluttajien tietoisuudesta valvontakapitalismista ja sen vaikutuksista kulutuskäyttäytymisen suhteen.

## 6 TUTKIMUSTULOKSET

Tässä osiossa käydään läpi tutkimustuloksia. Tutkimuksen alkukysymyksinä haastateltavilta kysyttiin, mitä älylaitteita he käyttävät. Haasteltavista kaikki käyttivät päivittäin älypuhelinta, tietokonetta sekä äly-tv:tä. Osalla oli näiden lisäksi käytössään myös pelikonsoleita sekä älykello. Haastateltavilta kartoitettiin myös, mitä internet-pohjaisia alustapalveluita he päivittäin käyttävät. Sosiaalisen median alustoista lueteltiin LinkedIn, Instagram, Facebook, Snapchat, TikTok ja Jodel. Viestintäpalveluista käytössä oli WhatsApp, Facebook Messenger sekä Tinder, ja sähköpostipalveluista mainittiin Gmail, Outlook ja Hotmail. Suoratoistopalveluista lueteltiin YouTube, Spotify, Netflix ja Nextstory ja hakukoneena kaikki haastateltavat käyttivät Googlea.

### 6.1 Kuluttajan tietoisuus valvontakapitalismista

Kuluttajan tietoisuus valvontakapitalismin termistä ja liiketoimintamallista olivat tämän haastattelun keskiössä. Haastateltaville luettiin aluksi lyhyt kappale valvontakapitalismin termistä sekä valvontakapitalismin hyödyntämästä bisneslogiikasta. Tämän jälkeen haastateltavilta kysyttiin, olivatko he törmänneet valvontakapitalismin termiin aikaisemmin tai oliko heille edellä kuvattu liiketoimintalogiikka tuttua. Tässä osiossa haastateltavilta kysyttiin, ovatko he huomanneet, että heille kohdennetaan mainontaa tai tietynlaista sisältöä. Haastattelussa keskusteltiin myös internetissä olevan tiedon luotettavuudesta ja miten haastateltavat arvioivat sitä. Tämän luvun alaluvuissa esitellään haastattelun tuloksia näihin ensimmäisiin teemoihin liittyen.

#### 6.1.1 Valvontakapitalismin termi ja liiketoimintalogiikka

Osalle haastateltavista valvontakapitalismin termi oli entuudestaan tuttu, mutta suurin osa haastateltavista ei ollut aikaisemmin termiä kuullut. Bisneslogiikka oli kaikille haastateltaville entuudestaan tuttua ainakin jollain tasolla. Mainittiin myös, että vaikka ei ole kovinkaan selkeää käsitystä siitä, miten

valvontakapitalismin liiketoimintalogiikka toimii, on omista päätelmissään eri asioita yhdistelemällä tullut siihen tulokseen, että jotenkin näin sen liiketoiminnan on pyörittävä.

Termiä en ole ikinä ennen kuullut. Mutta selvää on, että noin se niin kun menee. (H2)

Käsitys on itse muokkautunut päässä yhdistelemällä, mitä on lukenut ja mitä on kokenut. (H3)

Vaikka kaikilla haastateltavilla ei ollut valvontakapitalismin toteuttamisen laajuudesta käsitystä, niin monien mielestä maailma nykyään pyörii Internet-alustojen avulla ja sen vuoksi arveltiin, että toimintaa tehdään globaalisti. Eräs haastateltava nosti myös esiin, että esimerkiksi Googlasta voi käydä katsomassa mitä tietoja mainostajilla itsestä on. Osa haastateltavista sanoi, että heidän mielestään on jopa selvää, että valvontaa harjoittavat tietävät oikeastaan kaiken.

Ei ole tietoa, mutta mietin enemmän niin, että onko mitään tietoa, mitä ne musta ei ottaisi. Ikä ja sukupuoli ja se mitä tekee, sijainnit ja kaikki. Hetulla ne ei varmaan mitään tee, mutta muttu on, että kaikki muut paitsi henkilötunnus. Tosi laajasti varmastikin kerätään kaikkea. (H4)

Kerättävien tietojen osalta haastateltavat arvelivat, että heistä kerätään demografiatietojen lisäksi kaikkea omaan persoonaan ja nettikäyttäytymiseen liittyvää tietoa, jonka avulla voidaan profiloida käyttäjiä. Valvonnan ajateltiin koskevan kaikkea, mitä käyttäjä katsoo ja kuinka paljon viettää aikaa milläkin sivustolla ja minkäkin sovelluksen parissa.

Kyllä varmastikin kerätään kaikkea omaan persoonaan ja nettikäyttäytymiseen liittyvää tietoa, eli kaikkea mitä sisältöä katsoo ja kuinka paljon viettää aikaa missäkin sovelluksessa. Lisäksi varmastikin ostokäyttäytymistä, jotta voivat jatkossa markkinoida samantyyppisiä asioita oman kiinnostuksen mukaisesti. (H8)

Demografiatietoja ainakin ja sit muutenkin kaikki kiinnostuksen kohteet sen mukaan millä sivuilla on ja mitä siellä tekee. Kaiken käytännössä mitä netissä tekee. (H2)

Sijainti on tosi yleinen mitä ne pyrkivät selvittämään ja ikä. Vaikea spesifioida, mutta laajasti. (H5)

Haastateltavilta kysyttiin, mitä he ajattelevat, että kerätyillä tiedoilla tehdään. Haastateltavien mielestä tietojen keräämisen avulla pyrittiin tekemään rahaa ja arvaamaan käytösmaalleja ja erityisesti sitä, mikä kuluttajaa kiinnostaa, jotta osattaisiin mainostaa oikealla tavalla. Myös sillä, mitä kuluttuja klikkaa, ajateltiin olevan merkitystä. Osa vastaajista oli huomannut mainonnan lisäksi samanlaista

toimintaa sisällön suhteen esimerkiksi Instagramissa, joka tarjoaa vastaavanlaista sisältöä jatkossakin, jos käyttäjä jakaa tietynlaisia kuvia tai videoita eteenpäin.

Profiloi ainakin käyttäjiä, että ketkä palvelua käyttää ja muokkaa niitä palveluita käyttäjäystävällisemmäksi käyttäjäprofiileiden mukaisesti. Myy tietoja eteenpäin esimerkiksi, että saa oikeanlaista mainontaa sivustolle, josta saa tuottoa. Toki voi myydä varmaan muillekin toimialan tyypeille niitä tietoja, mitä musta on kerätty tai yhteistyökumppaneille. Kyllä veikkaan, että se profilointi on yksi isoimpia ja sitten se markkinointi. (H5)

Kun ne kerää sitä dataa, missä oon surffailut, niin ne pystyy lätkiin mainoksia niistä, mitä oon halunnut. Verkkokaupoilla on varmasti älykästä logiikkaa taustalla, joka hoitaa mulle mainoksia siitä mitä sillä hetkellä haluaisin ja mihin olisin altis tarttumaan. (H3)

Muutama haastateltava nosti esiin, että heidän mielestään kerätyillä tiedoilla tehdään varmasti paljon muutakin kuin edellä mainittuja asioita, mistä ei kuluttajalle kerrota kaikkea. Valvonnan ajateltiin myös olevan valtion keino, jota se voi hyödyntää turvallisuusliitännäisiin asioihin ja puuttua tarvittaessa, jos käyttäjät hakevat esimerkiksi hakukoneista paljon aseisiin liittyvää sisältöä.

### 6.1.2 Mainonnan ja sisällön kohdentaminen

Kun haastateltavilta kysyttiin heidän tietoisuuttaan kohdennetusta mainonnasta, kaikki vastaajat olivat tietoisia, että heille kohdennetaan mainontaa. Osa mainitsi lisäksi, että kun puhuu ääneen esimerkiksi puhelimen lähettyvillä jostain tietystä asiasta, siihen liittyviä mainoksia alkaa näkyä jonkun ajan kuluttua.

Oon tietoinen kohdennuksesta. Siitä on myös hyviä esimerkkejä. Tarpeeksi kauan, kun puhelimen vieressä hoet jotain, niin kyllä siitä alkaa mainoksia tulla. Esimerkiksi koiranleluja, vaikka et omistaisi koira. Mutta, jos sä oot antanu luvan kuunnella mikrofoonia tai vaikka et olis antanu lupaa, niin ne varmaan voi silti kuunnella ja sit alkaa tulla mainoksia. (H2)

Mainonnan ajankohtaan haastateltavat eivät olleet kiinnittäneet erityistä huomioita, mutta ainakin sesongin kuten joulun ja ystävänpäivän sanottiin vaikuttavan siihen, millaista mainontaa heille kohdennetaan.

Kävin Stockalla ja Googletin onko tiettyä hajuvettä. Niin koko eilinen päivä tuli näitä mainoksia. Sitten esimerkiksi ystävänpäivänä tulee generisiä mainoksia paljon, että ilahduta tyttöystävääsi tai poikaystävääsi. (H1)

Osa haastateltavista oli kuitenkin huomannut tietynlaisen sisällön kohdennusta tietyinä ajanjaksona esimerkiksi sen suhteen, että jos maailmalla tapahtuu jotain,

mikä yleisestikin kiinnostaa mediaa, on huomattu, että tällaista sisältöä alkaa tulla myös alustoilla vastaan paljon. Esimerkiksi Ukrainan sota kuului osan vastaajien puheessa. Toisaalta mainittiin myös se, että jos itse lähtee perehtymään näihin sisältöihin, niitä tarjotaan myös vastaisuudessa tästä syystä lisää.

Ennen kun käytti enemmän TikTokia, nii siellä tuli paljon kaikkea sotaan liittyvää sisältöä ja muihin vastaaviin liittyvää sisältöä. Instagramissa ja Facebookissa vähän vähemmän. (H5)

Jos maailmalla tapahtuu jotain mikä yleisestikin kiinnostaa mediaa, huomaan, että tällaista sisältöä alkaa tulla itsellenikin todella paljon. Toisaalta siihen voi vaikuttaa sekin, kun itse lähden perehtymään näihin sisältöihin, jonka vuoksi niitä tarjotaan minulle lisää. (H8)

### 6.1.3 Internetissä olevan tiedon luotettavuus

Haastateltavilta kysyttiin heidän käsitystään internetissä olevan tiedon luotettavuudesta. Haastateltavien mielestä internetistä löytyvään tietoon tulee lähtökohtaisesti suhtautua varauksella ja sieltä löytyy paljon niin luotettavaa kuin epäluotettavaakin tietoa. Luotettavaksi kuvailtiin vertaisarvioituja tekstejä ja yleensä sellaisia tutkimuksia, joiden lähdeaineistoon on mahdollisuus päästä myös itse käsiksi. Haastateltavista monet arvioivat tiedon luotettavuutta intuition sekä maalaisjärjen avulla ja eräs haastateltava mainitsi, että pitää enemmistön kantaa yleensä luotettavampana. Sen sijaan Iltapäivälehdet ja alustat, jonne kuka tahansa pääsee kirjoittamaan eivät herätä haastateltavien luottamusta.

Somessa oon aika kriittinen kaikkeen mitä siellä on. Iltapäivälehtien tyyliseen mediaan en usko. Arvioin luotettavuutta perus maalaisjärjenkin kautta, että mikä voisi olla realistisesti totta. Ja kyllä mä tykkään lukee artikkeleita ajankohtaisista asioista, mutta luotan silloin, jos ne on vertaisarvioitu. (H5)

Itse katson, onko sivusto sellainen, että kuka vaan siellä pystyy kirjoittaan. Esimerkiksi Reddit tai Wikipedia ei oo yhtä luotettavia, kuin joku minne ei voi kuka tahansa kirjoittaa. Pitää olla käynyt läpi jonkunlaisen screening processin. (H2)

Täytyy olla aika kriittinen kaikkeen mitä netistä löytyy, mutta on siellä myös paljon luotettavaa tietoa. Enimmäkseen käytän maalaisjärkeä sekä arvioin sen mukaan, kuinka monessa eri paikassa asia on kerrottu samalla tavalla. Eli yleensä luotan enemmistön ja vallitsevan kannan ilmoittamiin tietoihin, kuin vähemmistön tai ”yleisen” tiedon vastaiseen tietoon. Saatan

kiinnostuksesta lähteä selvittämään salaliittoteorioita, mutta aika kriittisesti suhtaudun niiden totuudenmukaisuuteen. (H8)

## 6.2 Valvontakapitalismin vaikutukset kulutuskäyttäytymiseen

Haastattelun toisessa osiossa selvitettiin valvontakapitalismin vaikutuksia haastateltavien kulutuskäyttäytymiseen. Tässä osiossa käsiteltiin ensin älylaitteiden ja internetalustojen koukuttavuutta ja tapoja manipuloida käyttäjiään. Lisäksi tässä osiossa selvitettiin, kuinka hyvin haastateltavat tuntevat internetalustojen käyttöehdot ja saavatko he mielestään tarpeeksi tietoa tietojenluovutus päätösten tueksi. Lisäksi selvitettiin haastateltavien käsityksiä mahdollisuuksista vaikuttaa tietojen käyttötarkoituksiin. Osion lopussa selvitettiin kohdennetun sisällön ja mainonnan vaikutuksia kuluttajien kulutuskäyttäytymiseen.

### 6.2.1 Kuluttajien riippuvuus älylaitteista ja internetalustoista

Haastateltavilta kysyttiin, ovatko he huomanneet olevansa riippuvaisia laitteista tai internetalustoista. Haastateltavat kertoivat, että eniten riippuvuutta aiheuttaa älypuhelin, koska sitä käytetään jatkuvasti kommunikoinnin välineenä ja siihen tulee tartuttua huomaamattakin tietyin väliajoin. Osa haastateltavista mainitsi, että kyllä ilman sosiaalista mediaa pystyy elämään, mutta kaikkien vastaajien mielestä sen sijaan Google tai joku vastaava hakukone on ehdoton apuväline arjessa.

Kyllä varmasti oon riippuvainen ainakin puhelimesta. Helposti jos on tylsää tai haluaa omaa rauhaa, tulee selattua puhelinta ja menee rullailemaan sovelluksia. Googlea tarvitsee päivittäin. (H6)

Pystyisin varmaan olemaan ilman someja, jos pakko olisi, mutta ei tulis yhtään mitään jos en pystyis Googlea käyttämään. Yleisesti hakukoneet on ihan must. (H2)

Tutkimuksessa selvitettiin, ovatko haastateltavat huomanneet, että sovellus koittaisi pitää heitä koukuttuneena. Osa haastateltavista kuvasi, että sovelluksien tarkoitus on lisätä käyttäjän sitoutuneisuutta ja saada käyttäjä pysymään alustalla mahdollisimman pitkään. Tällaisina koukuttamisen keinoina on havaittu esimerkiksi sovellusten push-ilmoitukset älypuhelimien tai muiden laitteiden näytöillä. Osa alustoista lähettää ilmoituksia sovelluksen sisäisen viestinnän lisäksi myös käyttäjien sähköpostiin, jotta henkilö aloittaisi laitteen tai sovelluksen selaamisen. Yhtenä keinona, erityisesti pelialustoilla havaittiin lahjonta, jonka avulla käyttäjä kosiskellaan takaisin pelaamisen pariin.

Vastaanotan paljon turhia push-ilmoituksia, joita sitten menen katsomaan ja jumiutan sitä kautta selaamaan kyseisen ilmoituksen sovellusta tai sitten muita sovelluksia. Myös tarjoamalla tietynlaista sisältöä, tulee helposti pysyttyä koukuttuneempana. (H8)

Esimerkiksi peli, Clash of clans tekee peliin koukuttuneisuuden sillain, että tulee pop up-ilmoituksia tietyin väliajoin, kun en oo hetkeen ollut siellä, niin sit se alkaa ilmoitteleen itestään. Ja jos on pelaamatta pidemmän aikaa, saa alennuksia, kun pitkästä aikaa tulee takaisin. Saa alkuun vauhtia, niin on "kiva" tulla takaisin. (H4)

LinkedInissä tulee ilmoituksia, jos joku julkaisee mielenkiintoista sisältöä. Näitä ilmoituksia tulee ihan sähköpostiin asti. (H5)

Myös sillä, mitä sisältöä käyttäjälle tarjotaan, nähtiin olevan merkitystä sovellukseen koukuttumisen kannalta. Spotifyn suositellut soittolistat, YouTuben shortit, eli lyhyet videot sekä TikTokissa ja Instagramissa olevat lyhyet videot, nähtiin vaikuttavina keinoina koukuttaa käyttäjää. Yksi haastateltava toikin esiin, että videoita jää vain selaamaan, kunnes havahtuu siihen, että on unohtanut tehdä sillä hetkellä omassa arjen elämässään tärkeitä askareita.

Esimerkiksi Instagram ja TikTok pyrii koukuttaan siten, että on lyhyttä sisältöä ja pääsee skrollaan, jos ei oo miellyttävää sisältöä. Sitten tulee ilmoituksia, jos vaikka kaveri tykkää jostain tai mitä ikinä. Spotifyssä tulee myös suosituksia. (H5)

Instagram on tosi paha, esimerkiksi Reelsit on pahoja samaan tapaan kuin TikTokissa, että niitä vaan jää selaamaan. Se homma vaan jatkuu ja unohtaa syödä ja mennä nukkumaan ja siitä on tosi vaikea irrottautua. Sama homma on nykyään YouTubessa. (H7)

Eihän noi sovellukset muuta nykyään teekään, shortit yms. Ne koittavat saada sitä engagement timea ihmisille. Aikasemmin Instagramissa oli kuvia varten ja YouTube oli videoita varten ja sit tuli TikTok, niin nyt ig:ssä ja YouTubessakin on nämä shortit. Sama toiminto on kopioitu muille alustoille. (H2)

## 6.2.2 Käyttöehtojen tuntemus

Kysyttäessä haastateltavilta internetalustojen käyttöehtojen tuntemuksesta ja niihin perehtymisestä vastaajajoukko jakautui selvästi. Osa haastateltavista sanoi suoraan, ettei oikeastaan tunne käyttöehtoja millään tavalla eikä ole paneutunut niihin lainkaan. Perehtymättömyys johtui ensisijaisesti halusta hoitaa asioita



sujuvasti ja päästä sivustolla eteenpäin ja syyksi mainittiin esimerkiksi se, että ajan tai kiinnostuksen puutteen vuoksi perehtyminen on jäänyt.

En oikeastaan tunne millään tavalla. Joskus olen jonkun sivuston käyttöehtoja silmäillyt, mutta yleensä on kiire päästä sivustolla eteenpäin enkä tästä syystä ole lainkaan perehtynyt niihin. (H8)

Toiset haastateltavista puolestaan käyttivät aikaa käyttöehtojen läpikäymiseen ja selvittelyyn. Nämä haastateltavat aina vähintään silmäilivät läpi, mihin laittavat suostumuksensa. Evästeistä valittiin näiden henkilöiden tapauksissa aina vain välttämättömät ja mainittiin, ettei haluta esimerkiksi kuvien leviävän kolmansille osapuolille.

Kyllä välillä selvittelen niitä, etenkin jenkkisivustojen kohdalla katson, että minne tietoja laitan ja jos pitää henkilötietoja sijoittaa, niin katson, minne sivustolle ne laitan. En myöskään evästeille myönnä kaikkia lupia, vaan otan lähes aina vaan tarpeelliset evästeet. Sen puitteissa olen tarkka. (H5)

Kyllä paneudun. Oon tehnyt siis tietoisien valinnan, että vain tietyt valitut kuvat mitä ne saa käyttää. Annan mahdollisimman vähän käyttöoikeuksia. En halua, että mun yksityisyys, esimerkiksi kuvat leviää kolmansille osapuolille. (H1)

Haastateltavilta kysyttiin saavatko he mielestään tarpeeksi tietoa tietojenluovutus päätöksensä tueksi. Vastaajat kokivat pääsääntöisesti, että eivät ole jaksaneet nähdä vaivaa selvittääksensä tietojenluovutus päätökseen vaikuttavia seikkoja tai sanoivat suoraan, että eivät koe saavansa tarpeeksi tietoa tietojenluovutus päätöstä tehdessään. Tämä johtui siitä, että vaikka tietoa olisi olemassa, se ei ole joko riittävän helposti saatavilla tai se on tehty kuluttajalle haastavaksi lukea.

En tiedä kun en oo niin hyvin perehtynyt. Kai niissä lukee jotain sinne päin ja yleensä klikkaan kyllä, enkä lue tarkemmin. Vaikeeksi on tehty ja menee heti hermo nii painaa vaan "Yes" tai lähtee sivulta pois. Ei jaksaa nähdä vaivaa. (H2)

Vaikea sanoa, koska en oo yrittänyt edes selvittää. Siellä on tarjolla sitä tietoa jossain, mutta toisaalta osa nettisivuista saattaa tehdä tiedon selvityksen vaikeaksi. (H4)

Vastaaan ei. Se on helposti saatavilla, mutta normaali ihminen ei kykene sitä lukemaan. En koe tästä syystä saavani tarpeeksi tietoa. (H7)

Eräs vastaaja nosti esiin, että Euroopan unionin jäsenmaiden sivustoilta löytyy kuitenkin yleensä enemmän tietoa, kuin esimerkiksi Yhdysvaltojen sivustoilla tietojen löytäminen on paljon hankalampaa.

Riippuu sivustosta. EU:ssa on tiukempaa, niin EU:n sivustoilla löytyy enemmän tietoa. Ei toki kaikissa. USA-pohjaisissa sivustoissa on paljon hankalampaa. Jos on tehty tosi hankalaksi, nousee tuntosarvet, enkä käytä palvelua. (H5)

Ainoastaan kaksi henkilöä kokivat saavansa tarpeeksi tietoa, eikä heillä ollut negatiivista sanottavaa nykyisistä käytännöistä.

Saan tarpeeksi tietoa. (H1)

Kyllä koen, että saan. Käytän myös paljon VPN:ää. kiitokset Euroopan unionille. (H3)

Kun kysyttiin, tekeekö vastaaja tietoisien valinnan luovuttaessaan tietojaan, osa vastaajista sanoi, että tekevät itse tietoisien päätöksen tietojensa luovuttamisesta.

Teen itse valinnan siinä kohtaa, kun luovutan jotain, mitä en välttämättä muuten haluaisi luovuttaa. (H3)

Kyllä teen, noissa kun en hyväksy evästeitä, niin vastaanotan sitten sellaisia geneeristen suomalaisten asioita. (H1)

Osa vastaajista puolestaan sanoi, ettei tavallaan tee tietoista päätöstä itse tietojen luovuttamisen suhteen, vaan hyväksyy evästeitä siitä syystä, että pääsee sujuvasti eteenpäin sen enempää miettimättä asiaa. Haasteltavat sanoivat, että luovuttavat tietoja pääasiassa pakon edessä, ja kokevat ettei ole muuta vaihtoehtoa. Päätöksen tietoisuutta siis kyseenalaistettiin.

En mieti, enkä tee tietoista päätöstä. Se on vaan, että painetaan väritettyjä nappuloita, että pääsee eteenpäin. (H4)

Pakko antaa, en haluaisi antaa, mutta pakko antaa, jos haluan käyttää. Annan yleensä mahdollisimman vähän ja aina pelkästään pakolliset, että pääse käyttämään sitä palvelua. (H2)

Tavallaan tiedostan, että tietojani saatetaan hyödyntää, mutta olen ehkä liiankin huoleton asian suhteen ja tavallaan, jos ei ole kaikkea tietoa saatavilla, onko valinta tietojen luovuttamisesta tietoinen. Mielestäni ei täysin, mutta kuitenkin itse ne tiedonkäyttöoikeudet heille luovutan. (H8)

Evästeistä haastateltavat hyväksyvät välttämättömät ja kaikkien evästeiden hyväksymistä kartetaan, mutta sovelluksille annetaan suostumuksia hieman helpommin kuin pelkille nettisivuille.

Meen aina matalimmalla mahdollisella tiedolla, enkä koskaan luovuta kaikkia tietoja. (H5)

Appeissa teen tietoisin valinnan, että hyväksyn, mutta nettisivuilla aina estän ja kiellän kaikki mahdolliset mitä tulee vastaan. (H7)

Haastateltavilta kysyttiin, onko heillä kokemuksia siitä, että olisivat jääneet ilman palvelua, jos he eivät ole antaneet lupaa tietojen keräämiseen. Haastateltavista osa kertoi jääneensä joissain tapauksissa kokonaan ilman palvelua, jos ei ole antanut lupaa tietojen keräämiseen. Osa kertoi myös evästeiden hyväksymättä jättämisen vaikuttaneen palvelukokemukseen ja esimerkiksi Instagramin pysäyttävän selaamisen melko nopeasti, jos ei ole rekisteröitynyt käyttäjä.

Kerättävien tietojen käyttötarkoituksesta kysyttäessä, jotkut vastaajista sanoivat suoraan, etteivät koe pystyvänsä hallitsemaan, mihin heidän henkilötietojansa käytetään, mutta toiset uskovat, että pystyvät evästeiden avulla vaikuttamaan siihen, mitä tietoja heistä kerätään.

En pysty hallitsemaan, jos haluaa liittyä, niin pitää vaan luottaa siihen, että niitä käsitellään niin kuin pitää käsitellä. (H3)

En pysty hallitsemaan. Se on muiden käsissä. Esimerkiksi Facebookissa olen ollut niin pitkään jo ennen kun oli mitään tietosuojavaatimuksia, niin mun tiedot on myyty jo monta kertaa eteenpäin. (H1)

En pysty vaikuttamaan mitä ne tekee multa kerätyillä tiedoilla, mutta pystyn vaikuttamaan siihen, mitä tietoja kerätään. (H5)

Seuraavaksi haastateltavia pyydettiin kuvittelemaan tilanne, jossa he ovat lukemassa jotain haluamaansa uutista tai artikkelia ja uutisen päälle tulee banneri, jonka mukaisesti he voivat valita hyväksyä kaikki evästeet tai maksaa palvelusta pienen kuukausimaksun. Mikäli haastateltava maksaa kuukausimaksun, yritys ei seuraa häntä evästeiden avulla tai esimerkiksi kohdenna mainontaa. Jotkut vastaajista sanoivat ensisijaisesti tässä vaiheessa poistuvansa sivustolta, mutta toissijaisesti hyväksyvänsä evästeet, jos uutisen tai artikkelin pariin on pakko päästä. Osa sanoi myös suoraan hyväksyvänsä evästeet.

En käyttäisi palvelua ollenkaan. Varmaan antaisin luvan tietojen käyttöön, jos ois ihan pakko. Enemmän annan luvan, mutta en ala maksaa siitä ja joskus lähden kokonaan pois. (H2)

Sen enempää tietämättä mitä tietoja kerätään, hyväksyisin. Koen vaivanloiseksi sen, että maksaisin siitä niin antaisin vaan tiedot. (H3)

Suurin osa vastaajista ei olisi valmiita maksamaan yritykselle lainkaan seuraamisen tai valvonnan lopettamisesta. Vaikka tietosuojasta maksaminen ei herättänyt vastaajissa juurikaan kannatusta, osa vastaajista kertoi kuitenkin maksavansa VPN:stä kuukausittain. He myös mainitsivat, että tässä mielessä tavallaan ovat valinneet maksaa siitä, että VPN estää heidän seuraamisensa. Tässä yhteydessä haastateltavat toivat myös esiin, että kaikille sivustoille ei ole mahdollista mennä, mikäli VPN on käytössä.

En maksa, koska ei tarvii maksaa. En maksais mitään ja saisi mun puolesta seurata. Ajattelen, että ei vaikuta muhun, nii ottaisin sen ilmaisen vaihtoehdon. (H4)

Oon jättänyt käyttämättä sivustoja, jos vaaditaan liikoja. En oo menossa niille sivuille, missä mun pitää ottaa VPN pois. (H7)

### 6.2.3 Kulutusvalinnat

Haastateltavilta kysyttiin, vaikuttaako kohdennettu sisältö tai mainonta heidän mielialaansa ja sitä kautta kulutuskäyttäytymiseen. Osa haastateltavista oli huomannut kohdistetulla sisällöllä olevan vaikutusta omaan mielialaan sekä kulutuskäyttäytymiseen. Myös mainonnan sanottiin muun sisällön ohella näissä tapauksissa monesti vaikuttavan.

Kyllä allekirjoitan täysin. En mä ihan kaikkea osta, mutta kyllä käyn ne selaamassa läpi. Vaikuttaa sekä sisältö että kohdennettu mainonta. (H7)

Joo vaikuttaa, jos näkee siistin videon, jossa joku juoksee ja sit meen ostaan samat lenkkarit, enkä näe sitä välttämättä pahana asiana. (H3)

Jos koen olevani surullinen tai väsynyt, teen helpommin harkitsemattomia kulutusvalintoja. Eli mikäli tällaisena hetkenä vastaanotan tiettyä sisältöä, olen herkempi toimimaan sen mukaan mitä niillä tavoitellaankin. Tämän vuoksi tulee helposti myös ostettua asioita sen mukaan mitä mainoksia tulee vastaan. (H8)

Joukossa oli kuitenkin myös vastaajia, joiden mielestä sisällön tai mainonnan kohdentamisella ei ollut vaikutusta heidän kulutusvalintoihinsa.

Seuraavaksi haastateltavilta kysyttiin, ovatko he huomanneet esimerkiksi verkkokaupoissa alennuskuponkeja vastineeksi siitä, että he rekisteröityvät kyseisen verkkokaupan jäseneksi. Lisäksi heiltä kysyttiin, miten he kokevat tämäntyyppisen toiminnan ja vaikuttaako se heidän tietoihinsa.

kulutusvalintoihinsa. Verkkokauppojen alennuskupongeilla rekisteröintiä vastaan sanottiin olevan vaikutusta siinä tapauksessa, jos on jo valmiiksi tarve ostaa joku tietty tuote tai palvelu. Rekisteröintiä tehtiin herkemmin myös siinä tapauksessa, jos sivusto oli sellainen, mistä haastateltava tietää ostavansa jatkossakin.

En tartu koskaan tohon, mutta jos tarviin kyseisestä kaupasta jotain niin sit tarpeeseen voin rekisteröityä. (H3)

On vaikutusta. Kyllä huomaan, että kun kilahtaa jossain sivustolla, että nyt saat tuotteet -10 %, kun rekisteröidyt, niin kyllä menen niihin. Mutta pyrin kuitenkin tarpeeseen hankkimaan. (H7)

Alennusprosentin suuruudella ei kuitenkaan nähty juurikaan itsearvoisesti olevan merkitystä, vaan valtaosalla tarve määrittää ostoksia ja rekisteröinti voidaan alennuksen toivossa tehdä tarpeen täyttämiseksi.

Ostin juuri viime viikolla isälle 60-vuotislahjan Keskisen Kellosta. Sain 20 % lisäalennusta, kun tilasin uutiskirjeen. Kyllä alennusprosentin pitää olla vähintään 15-20%. Voi olla myös pienempi prosentti, jos summa on suurempi. Eurot vaikuttaa. (H1)

Tuotteet, joita hankkii tarpeeseen, niin niissä riittää pienempikin alennus. Heräteostoksissa, oon pitänyt sellaista n. -20 %. (H7)

### **6.3 Kuluttajien kokemat valvontakapitalismin vaikutukset**

Haastattelun viimeisessä osiossa haastateltavilta selvitettiin heidän käsityksiään valvontakapitalismin hyödyistä ja haitoista. Lisäksi keskustelua käytiin valvontakapitalismin seurauksista ja niiden aiheuttamista tulevaisuuden näkymistä. Tässä viimeisessä osiossa haastateltavat toivat esiin myös ratkaisuja, joilla haitallisia seurauksia voitaisiin ehkäistä.

#### **6.3.1 Valvontakapitalismin hyödyt ja haitat**

Verkostoitumisen ja yhteydenpidon helpottaminen eri internetalustojen avulla oli kaikkien haastateltavien mielestä hyvä asia. Eräs haastateltava toi myös esiin, että internetin alustojen kautta on myös lisätty työpaikkoja ja monilla ihmisillä on merkityksellisiä ihmissuhteita, joita ilman alustoja ei välttämättä olisi muodostunut. Lisäksi mainittiin, että palveluiden monipuolistuminen on hyvä asia, ja että tällaisen teknologian avulla on kehitetty uusia palveluita. Haastateltavat pitivät myös kohdennettua mainontaa ja mahdollisia alennuksia

pääasiassa hyvänä asiana. He sanoivat lisäksi mieluummin katsovansa kohdennettua mainontaa kuin kohdentamatonta geneeristä mainontaa.

Verkostoituminen ja yhteydenpidon helpottaminen on parantunut ja se on hyvä myös työllisyyden lisäämisen kannalta ja monilla ihmisillä on kavereita, joita ilman näitä alustoja ei välttämättä olisi. On myös hyvä asia, että ihmisillä on töitä. (H2)

Mielestäni palveluiden monipuolistuminen on hyvä asia ja esimerkiksi se, että tällaisen teknologian avulla on kehitetty uusia palveluita, joilla saa esimerkiksi ruuan kotiovelle. Pidän myös kohdennettua mainontaa ja mahdollisia alennuksia hyvänä asiana. Mieluummin kohdennettua mainontaa kuin kaikkea sekaisin. (H8)

Eräät vastaajat nostivat esiin, että, jos jotain henkilöä epäillään rikoksesta, niin sijaintitietojen seuraamisen avulla on mahdollista päästä epäillyn jäljille ja näki tämän hyvänä asiana.

Jos joku on tehnyt rikoksen tai epäillään, niin pystytään seuraamaan lokaatiota. Se on ainoa, miten siitä mun mielestä on hyötyä. (H1)

Jos tällä tyyllillä saataisiin rikollisia kiinni, kun valvotaan sijaintia tarkemmin. (H3)

Jos vois hyötykäyttää ja tällä tavalla ehkästä rikollisuutta, niin se on mun mielestä hyvä asia. (H6)

Useiden haastateltavien mielestä se, ettei kuluttajalla ole tarpeeksi tietoa mihin tietoja kerätään ja yleinen tietojen keräämisen läpinäkymättömyys koettiin valvontakapitalismin haitaksi. Esiin myös nostettiin, että mitä aiemmin kuluttaja on liittynyt esimerkiksi sosiaaliseen mediaan, sitä todennäköisempää on, että tiedot ovat levinneet hyvin laajalle, eikä käyttäjä voi enää millään tavalla kontrolloida tällaisia tietoja.

On huono asia, kun ei tiedä mihin tietoja kerätään. Se myös, kun se ei ole näkyvää. Meidän ikäisemme tiedot on kaikkialla sosiaalisessa mediassa. Meitä nuoremmilla on parempi tilanne, kun nykyään on säästöksiä, joilla tätä rajoitetaan. (H1)

Valta-aseman keskittyminen isoille toimijoille nähtiin kilpailun näkökulmasta huonona asiana, mutta puolestaan tietoturvan näkökulmasta osa toi esiin, että luottavat itseään koskevat tiedot enemmän muutamalle isolle toimijalle. Tämä mielipide kuitenkin vaihteli ja osa haastateltavista sanoikin, että haluaisi myös tietoturvan näkökulmasta jakaa isot yhtiöt pienempiin toimijoihin, jolloin luottaisivat tietonsa enemmän niiden haltuun.

Vois luulla, että kun on isompi toimija niin niillä vois olla hyvät suojaukset sillain, ettei tiedot mene ihan mihin vaan, mutta ei se monopolikaan ole hyvä, jos se tieto keskittyy vaan tietylle. Mieluummin kuitenkin silleen, että yks iso toimija. Tämä on hankala kysymys. (H2)

Kyllä se kuulostaa pahalta, että jollain on monopoliasema enkä katso hyvällä sitä. Sillä on tilanteessa sitten vielä enemmän valtaa. Jos pitää valita, niin mieluummin kuitenkin hajautetusti pienillä toimijoilla. Tietoturvan kannalta myös pienemmällä toimijoilla. (H4)

Väärän tiedon leviäminen ja valeuutiset oli miltei kaikkien vastaajien mielestä suuri haitta. Mainittiin myös, että somessa ja alustoissa liikkuu paljon väärää tietoa, joka aiheuttaa pahimmillaan joukkohysteriaa ja tekoäly tekee jatkuvasti entistä vaikeammaksi erottaa, mikä on totta ja mikä ei.

Disinformaatio on todella huono asia. Somessa ja internetalustoilla liikkuu väärää tietoa ja toi AI-teknologia tekee vaikeammaksi erottaa, mikä on oikeasti totta ja mikä ei. (H5)

Keskusteluissa nousi myös esiin ajatus siitä, että ehkä koronavirus olisi mennyt ohi nopeammin, jos eläisimme edelleen aikaa ennen sosiaalista mediaa, sillä ihmisten sanottiin uskovan herkästi, mitä esimerkiksi somessa luki pandemian aikaan ja kaikki väitetty ei ollut totta.

Ylipäänsä fakenews ja disinformaatio voi olla tosi haitallista. Ihmiset uskoo kaiken niin ei voi laittaa mitä tahansa. Luulisin että korona olisi mennyt helpommin ohi, jos se olisi tullut ennen someaikaa koska ihmiset usko kaiken mutta kaikki ei ollut totta. (H2)

Eräs vastaaja nosti kuitenkin esiin, että häntä häiritsee tiedon sensurointi ja hän mainitsi, että ihmisillä pitää olla mielipide- ja sananvapaus, eikä yksi taho, esimerkiksi tietty yritys tai viranomainen saisi poistaa tietoa tai määritellä, mikä on oikeaa tietoa.

Itseäni enemmän häiritsee sensurointi ja se ettei saa muodostaa vapaata mielipidettä. Ihmisillä pitää olla sananvapautta ja mielipidevapautta kertoa mielipiteitä, eikä yksi taho saa poistaa tietoa ja määritellä, mikä on oikeaa. Kyllä somen käyttäjällä pitää olla itsellä valittavissa mihin uskoo. Jos aina joku poistaa sieltä heidän mielestensä väärät tiedot, niin silloin, tulee vaan yhdenlaista tietoa tietyltä taholta. (H7)

Demokratian heikentyminen nähtiin yksimielisesti haittana ja eräs vastaaja jopa mainitsi, että kohdeyleisön manipulointi tämän hyödyn toivossa pitäisi kriminalisoida. Nostettiin myös esiin, että ihmisten mielipiteisiin vaikuttamisen

sanottiin pahimmillaan johtavan henkilöiden radikalisoitumiseen. Haastateltavat nostivat myös paljon huolia esiin sen suhteen, miten alustat ja laitteet vaikuttavat lapsiin ja nuoriin ja erityisesti siihen, kuinka jo alakouluikäiset ovat usein riippuvaisia laitteistaan.

Haittana on se, että tänään kun istuttiin ravintolassa, niin sinne tuli pari poikaa nii ne tuli syömään ja he olivat vaan koko ajan omalla puhelimella. Pakko siinä on jäädä jotain pois, kun on koko ajan ruudulla. (H3)

Kysyttäessä haastateltavat kertoivat, että eivät luota heidän henkilötietojensa olevan turvassa Internet-alustoilla. Osan mielestä tämä ei kuitenkaan huoleta heitä, tai he eivät olleet juuri pohtineet asiaa. Toisten mielestä puolestaan identiteettivarkaudet tai henkilötunnuksien ja pankkitietojen leviäminen oli keskeinen huolenaihe.

Kyllä huolettaa siinä määrin, jos somen kautta, joku tekeytyy minuksi ja aiheuttaa henkilökohtaista hallaa. Niitä on tapahtunut myös ihan normaaleille ihmisille eikä pelkästään julkkiksille. (H5)

Kyllä tietojen väärinkäyttö huolettaa. Hetut ja pankkitiedot leviävät tuolla. (H7)

### 6.3.2 Valvontakapitalismin seuraukset

Valvontakapitalismin aiheuttamista tulevaisuuden seurauksista puhuttaessa vastaajien mielipiteet vaihtelivat. Jotkut haastateltavista sanoivat, että ajattelevat etenkin Euroopan unionin alueella tilanteen paranevan, kun EU-lakeja muokataan siihen suuntaan, että tietojenkalastelu olisi haastavampaa. He myös suhtautuivat toiveikkaasti, että pian valvontaa ei ehkä olisi nykyiseen tapaan.

EU:n alueella veikkaan, että tilanne ehkä paranee. EU-lakeja muokataan siihen suuntaan, että tietojenkalastelu olisi haastavampaa. (H5)

Osa haastateltavista ei kuitenkaan suhtautunut tulevaisuuden näkymiin yhtä positiivisesti ja käytti jopa dystopia-termiä. Tässä yhteydessä tuotiin muun muassa esiin, että pahimmassa tapauksessa tulevaisuudessa siirrytään mikrosirutettuun social credit systemiin, jossa valtio tietää kansalaisista kaiken sekä pisteyttää ja jakaa ihmisiä sen perusteella.

Toivon että ei mennä tähän, mutta dystopisia mielikuvia on, esimerkiksi Kiinasta, jossa on social credit system ja valtio tietää kaiken, pisteyttää ja alkaa jakaa porukkaa sen perusteella. Jos kaikille tulee mikrosirut, niin sitten voidaan tietää kaikesta kaikki vielä helpommin. Pahimmissa tapauksissa uskon tähän ja jos se on jossain jo käytössä ihan vaan sen takia että pystytään kontrolloimaan ihmisiä. (H2)



Dystopinen skenaario voi olla mahdollinen, jos valta on yhdellä kanavalla ja sieltä toivotetaan vaan yhdentyypistä sisältöä, joka muokkaa ihmisten käyttäytymistä ja mieltä. Se on paha skenaario. (H7)

Tulevaisuudessa valvontakapitalismin haitalliset seuraukset nähtiin myös nuorten keskittymiskyvyn heikkenemisenä ja mainittiin, että esimerkiksi mielenterveysongelmat kasvavat sosiaalisen median sekä laitteiden ja alustapalveluiden riippuvuuden takia.

Näkisin seuraukset enemmän siinä, että nuorten keskittymiskyky ei ole enää yhtä hyvällä tasolla kuin ennen sekä ylipäätään esimerkiksi mielenterveysongelmat tulevat kasvamaan somen takia. Eli enemmänkin siinä, kun kaikki ovat nykyään niin riippuvaisia laitteista ja alustapalveluista. (H8)

### 6.3.3 Kuluttajien ratkaisuehdotukset

Haastatteluissa ratkaisusta keskusteltaessa, ensisijaisesti esille nousivat yritysten tiukemmat vastuut ja lainsäädännölliset keinot puuttua valvontakapitalismin haittoihin. Mainittiin myös, että olisi hyvä, jos ihmisillä olisi rehellisesti oikeus tulla unohdetuksi siten, että kaikki ihmisestä kerätty data poistettaisiin pyydettyäessä.

Ratkaisuksi sanoisin, että lainsäädäntö, jota kaikkien valtioiden ja henkilöiden pitäisi noudattaa. Yrityksille lisäksi jotain sanktioita. Pitäisi luoda yhtenäinen kulttuuri tähän. (H5)

Olisi hyvä, jos ihmisillä olisi rehellisesti oikeus tulla unohdetuksi siten, että kaikki ihmisestä kerätty data pyydettyäessä poistettaisiin, mutta en tiedä onko se mahdollista. (H8)

Eräs vastaaja nosti myös esiin, että hänen mielestään kaikki data tulisi pitää pelkästään Euroopan sisällä. Yhtenä ratkaisuna henkilötiedoista kerättävälle datalle esitettiin myös vanhentumisaikaa, jonka mukaisesti henkilöistä kerättävä data tulisi vanhentua tietyn ajan kuluessa.

En haluaisi, että dataa lähtisi Euroopan ulkopuolelle. Tämä tehtäisiin laajatenantaisesti, sillain, että olisi paljon pieniä konesaleja ympäriinsä valtion ja EU:n toimesta. Muilla mailla on niin paljon enemmän mahdollisuuksia vaikuttaa poliittisesti ja muutenkin meidän mielipiteisiimme. Data on myös sellaista, että sen pitäisi vanhentua, kun jos se ei vanhene ja sitä voidaan rajattomasti säilyttää. Henkilödatalla pitäisi olla esimerkiksi kahden vuoden vanhentumisaika. (H1)

Vastaajat pohtivat myös sitä, että tulisiko valvontaoikeus olla ylipäänsä valtiolla, viranomaisilla vai yrityksillä, ja saako esimerkiksi rikoksesta tuomittua valvoa kevyemmin perustein, kuin henkilöä, joka ei ole syyllistynyt rikokseen.

Jos kaikkea valvotaan, niin katooko yksityisyys. Sitten on myös kysymys siitä, että kenellä on oikeus valvoa, onko se valtio, viranomaiset vai joku yritys ja määritelläänkö se laissa vai miten se menee. Jos mut esimerkiksi tuomitaan jostain, niin pitäisikö mua voida valvoa kevyemmin perustein, kun jotain, joka ei ole syyllistynyt rikokseen? (H3)

Lopuksi haastateltavia pyydettiin valitsemaan, haluisivatko he palata sen kaltaiseen maailmaan, jossa näitä valvontakapitalismin mahdollistamia palveluita ei ollut, vai elää nykymaailmassa, jossa nämä palvelut toimivat nykyisen tapaan. Haastateltavista suurin osa valitsisi nykymallin, mutta muutama vastaajista palaisi mieluummin lapsuutensa aikaiseen maailmaan, jossa valvontakapitalismin mahdollistamaa liiketoimintalogiikkaa ei vielä ollut käytössä.

Uudessakin systeemissä näen paljon hyvää. Ottaisin tän uuden mallin kyllä. Tilanne ei vielä mun mielestä ole vielä niin huolestuttava. (H3)

Kyllä hyviä vanhoja aikoja kaipaen ja valitsisin sen. Tykkään digitalisaatiosta, mutta jos pakko valita, niin sitten ottaisin sen mitä ennen oli. Jos ei olisi niin valvottua, olisi kiva hyödyntää somea ja kun asiat on sen kautta helpottuneet. Mutta tietojen eteenpäin myyminen ilman suostumusta ei ole hyvä. (H7)

## 7 JOHTOPÄÄTÖKSET

Tämän Pro gradu -tutkielman tarkoituksena oli selvittää kuluttajien tietoisuutta valvontakapitalismista ja sen toimintatavoista sekä sen vaikutuksista kuluttajan kulutuskäyttäytymiseen. Tämän lisäksi selvitettiin valvontakapitalismin vaikutuksia ja sitä mitkä asiat kuluttaja kokee hyödylliseksi ja minkä haitalliseksi.

Tutkimukseen sisältyvään kirjallisuuskatsausosuuteen kuului laaja tutustuminen aiheen kannalta keskeiseen kirjallisuuteen sekä aikaisempaan tutkimukseen. Tämän teoriaosuuden jälkeen toteutettiin laadullisen tutkimuksen haastatteluiden avulla, joiden vastauksista kävi ennen kaikkea ilmi se, että haastateltavat ovat havainneet valvontakapitalismin ilmiöitä päivittäisessä toiminnassaan, mutta heidän tietoisuutensa sen syvemmästä toimintalogiikasta on vielä hämäränpeitossa. Tämä Pro gradu -tutkielman tavoite on lisätä kuluttajien tietoisuutta valvontakapitalismista.

Empiirisen aineiston perusteella termi valvontakapitalismi ei ollut kaikille haastateltaville entuudestaan tuttu, mutta kaikki haastateltavat tunnistivat selvästi valvontakapitalismin liiketoiminnalle ominaisia ilmiöitä ja etenkin kohdennettu mainonta oli haastateltaville tuttua. Kirjallisuudessa termin määritelmästä ei ole riitaa, mutta eroavaisuuksia on sen suhteen, mihin sävyyn liiketoiminnasta, etenkin tietojen keräämisen suhteen puhutaan. Esimerkiksi Zuboff puhuu valvontakapitalismista erityisen raflaavasti ja korostaen sitä, kuinka rosvoten ja häikäilemättömästi yritykset keräävät tietoja käyttäjistään. Zuboffin mukaan tätä varjo-operaatiota toteutetaan ilman käyttäjien etukäteen antamaa suostumusta ja jopa laittomasti. Venkatesh puolestaan tuo esiin, että hänen näkemyksensä mukaan valvontakapitalistit maksavat käyttäjilleen palkkaa rahan sijaan tarjoamalla palvelun, jonka avulla käyttäjä pystyy täyttämään sosiaaliset tarpeensa. Näin ollen kirjallisuudessa on kahta koulukuntaa sen puolesta, onko kyseessä molemminpuolinen kauppa kuluttajan ja yrityksen välillä vai ottaako yritys liiketoimintansa raaka-aineet kuluttajasta vastikkeetta.

Aiheeseen liittyvän kirjallisuuden perusteella on selvää, että valvontakapitalismia toteutetaan rajattomassa laajuudessa ja kaikki tieto on arvokasta sen totuudenmukaisuudesta ja laadusta huolimatta.

Valvontakapitalismin tapauksessa tiedon määrä korvaa laadun. Mielenkiintoisena tuloksena haastatteluista nousi esiin, että kuluttajat ovat perillä siitä, että heistä kerätään heidän käyttäytymistään koskevaa dataa, joita ovat muun muassa Facebook-tykkäykset, klikkaukset ja sivustot, joilla he vierailevat, hakuhistoria, ostokäyttäytyminen sekä sijaintitiedot. Metatietojen keräämisestä haastateltavat eivät ole yhtä valveutuneita tai tietoisia, että tällaisillakin tiedoilla voi olla jopa enemmän merkitystä kuin niillä tiedoilla, jota he tietoisesti luovuttavat. Kuten Willis on edellä teoriaosuudessa kuvatulla tavalla tuonut esiin, valokuvien värisävy, kirkkaus ja värikylläisyys kertovat käyttäjän persoonallisuudesta yhtä paljon kuin varsinainen kuvan sisältö. Myös nämä metatiedot voivat olla yhtä ennustettavia tietoja, kuin tiedot siitä, mitä käyttäjät katsovat tai tekevät internetissä. Erityisen mielenkiintoinen havainto oli se, että osa haastateltavista ajatteli, että he pystyvät itse vaikuttamaan siihen, mitä tietoja heistä kerätään, vaikkakaan eivät pysty tietojen käyttötarkoitusta määrittämään. Teoriaosuudessa esiin tuodun mukaisesti valvontakapitalismille on kuitenkin ominaista tiedon epäsymmetrinen ja epätäydellinen jakautuminen kuluttajan ja yrityksen välillä. Tämän perusteella on mahdollista olettaa, että mikäli kuluttajat eivät ylipäättään tiedä mitä tietoja heistä kerätään tai mitä tiedolla tehdään, eivät he silloin voi myöskään tietoisesti vaikuttaa siihen.

Aikaisemmassa tutkimuksessa ja kirjallisuudessa käyttäjien manipuloinnin keinot ovat laajalti tunnettuja. Myös tämän tutkimuksen haastatteluissa kävi ilmi, että kuluttajat ovat havainneet valvontakapitalismin liittyvää manipulointia jokapäiväisessä elämässään, mutta ovat siitä huolimatta kohtalaisen piittaamattomia siitä. On mielenkiintoista, että kuluttaja tietää ne keinot, miten häntä manipuloidaan. Siitä huolimatta hän saattaa esimerkiksi iltaisin päättää tarttua älypuhelimien ja katsoa, löytyykö sieltä jotain katsottavaa. Kuluttaja tiedostaa, että jos hän nyt menisi nukkumaan, hän olisi aamulla virkeämpi ja hänen yleisvointinsa olisi parempi. Tämän perusteella vaikuttaa siltä, että kuluttaja ei malta odottaa ”palkintoa” eli pidempien yöunien tuomaa vireystilaa huomiseen, vaan maksimoi mieluummin lyhyen hetken viihdykkeen yöunien kustannuksella. Kuten teoriaosuudessa on tuotu esiin, ihminen ei toimi rationaalisesti ja tästä syystä nudging toimii.

Laadullisen tutkimuksen avulla selvitettiin, vaikuttaako valvontakapitalismi kuluttajan tietoisiin kulutusvalintoihin ja kulutuskäyttäytymiseen. Kaikki haastateltavat havaitsivat vastaanottavansa kohdennettua mainontaa ja sisältöä, eivätkä nähneet sitä negatiivisena asiana. Osalla haastateltavista kohdennettu mainonta vaikutti merkittävästi kulutuskäyttäytymiseen ja he toivat esiin, kuinka saattavat tehdä myös ostoksia, joita eivät olisi ilman tällaista mainosta tehneet. Monet haastateltavat toivat myös esiin, että tietynlainen sisältö vaikuttaa ajoittain heidän tietoisiin kulutus päätöksiinsä. Tästä voi tehdä johtopäätöksen, että valvontakapitalismilla on vaikutusta monien kuluttajien kulutuskäyttäytymiseen ja tietoisiin kulutusvalintoihin.

Yksi huomionarvoinen havainto oli niin ikään se, että haastattelujen perusteella valtaosa kuluttajista ei ole halukkaita maksamaan omasta

tietosuojastaan tai yksityisyydestään verkossa. Kyse ei ole siitä, etteivät kuluttajat olisi huolissaan omasta tietoturvastaan tai välittäisi siitä, vaan kyse on ennemmin siitä, että heillä ei oman käsityksensä mukaan ole mitään salattavaa. Toinen esiin noussut syy oli se, että asiaan perehtyminen ja yksityisyydestä maksaminen on liian vaivalloista. Yksi mielenkiintoinen havainto oli myös se, että haastateltavat jakautuivat täysin sen mukaisesti, että perehtyvätkö he käyttöehtoihin ja evästeasetuksiin vai hyväksyvätkö he ne täysin piittaamattomina. Osa kuluttajista perehtyy käyttöehtoihin ja hyväksyy ainoastaan välttämättömät evästeet. Osa haastateltavista toi kuitenkin esiin, että ei perehdy käyttöehtoihin lainkaan, koska kokee, että ne on lähtökohtaisesti tehty niin vaikeasti ymmärrettäviksi ja pitkiksi, että kuluttaja ei halua käyttää aikaa niihin perehtymiseen. Haastatteluista nousikin esiin yhteneväinen kanta, että kuluttajat toivoisivat, että käyttöehdot olisivat helppolukuisemmat ja kauttaaltaan selkeämmät. Näistä voidaan tehdä johtopäätös, että kirjallisuudessa esiin tuodut näkökohdat siitä, että kuluttajalla ei todellisuudessa ole aitoa valinnanvapautta, pitävät paikkaansa. Monet kuluttajat ovat huolettomampia omaan tietoturvaansa liittyen myös siitä syystä, että heillä ei ole mitään salattavaa tai he kokevat, että eivät kuitenkaan voi vaikuttaa tietojen keräämiseen.

Aikaisemmassa tutkimuksessa ja kirjallisuudessa ei juurikaan kuvata valvontakapitalismiin liittyviä hyötyjä. Useassa lähteessä todetaan, että sovellukset mahdollistavat paljon ja älylaitteiden avulla on saavutettu paljon hyvää, mutta valvontakapitalismi itsessään nähdään negatiivissävytteisenä ilmiönä. Haastateltavat puolestaan ovat kokeneet valvontakapitalismissa hyödylliseksi verkostoitumisen helpottumisen. Kuluttajat pitivät myös kohdennettua mainontaa ja verkon kautta tulevia alennuksia hyödyllisinä. Mielenkiintoinen huomio oli se, että haastateltavien käsitykset valvontakapitalismin haitallisista vaikutuksista, olivat pääosin yhteneväiset kirjallisuudessa esiin tuotuihin näkemyksiin. Merkityksellistä oli kuitenkin se, että vallan keskittyminen vain muutamalle suurelle toimialle, ei koettu haastateltavien keskuudessa yhtä ongelmallisena kuin aiheeseen liittyvässä kirjallisuudessa. Toisaalta haastateltavat ovat ajatelleet asiaa enimmäkseen yksilön näkökulmasta ja vastanneet haastattelussa sen mukaisesti, luottavatko ennemmin tietonsa muutamalle suurelle toimijalle kuin kymmenille pienille. Haastateltavat kuitenkin puolsivat kirjallisuudessa esiin tuotua näkökohtaa, jonka mukaan vallan keskittyminen vain muutamille tahoille on kilpailun ja demokratian kannalta varsin ongelmallista, koska tällöin tieto antaa suhteettoman paljon valtaa näille toimijoille. Näin ollen haastateltavien ajatukset yhteiskunnallisella tasolla valvontakapitalismin vaikutuksista olivat yhteneväisiä kirjallisuuskatsauksessa esiin tuotujen seikkojen kanssa. Myös haastateltavat ovat tunnistaneet ja havainneet disinformaatioon liittyviä vaikutuksia ja pitivät niitä lähtökohtaisesti valvontakapitalismin haittana.

Haastateltavat ratkaisivat valvontakapitalismiin liittyviä ongelmia samaan tapaan kuin aikaisemmassa tutkimuksessa ja aihetta koskevassa kirjallisuudessa on esitetty. Sekä kirjallisuudessa että haastatteluissa on nostettu tärkeimmiksi ratkaisuksi se, että valvontakapitalismin epäkohtiin ja kuluttajien oikeuksiin

puututaan ennen kaikkea lainsäädännöllisillä ja poliittisilla toimilla. Valvontakapitalismiin liittyvien haittojen ratkaiseminen on kuitenkin haastavaa, koska valtioiden lainsäädännöt ja kulttuurit eroavat merkittävästi toisistaan.

Valvontakapitalismia on aikaisemmin tutkittu enimmäkseen yritysten ja liiketoiminnan kehittämisen näkökulmasta, eli miten saadaan kuluttajat koukuttamaan palveluihin vielä entistä paremmin ja siten, että se palvelee nimenomaan näiden suurien yritysten etua. Tässä tutkimuksessa paneuduttiin kuluttajan näkökulmaan ja tietoisuuteen, joka palvelee itse kuluttajaa. Tulevaisuudessa valvontakapitalismiin liittyvää tutkimusta on aiheellista tehdä vielä enemmän kuluttajaa ja yhteiskuntaa palvelevista näkökulmista.

## LÄHTEET

- Acquisti, A., Brandimarte, L., & Loewenstein, G. (2015). Privacy and human behavior in the age of information. *Science*, 347(6221), 509-514. <https://doi.org/10.1126/science.aaa1465>
- Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., ... & Wilson, S. (2017). Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR)*, 50(3), 1-41. <https://doi.org/10.1145/3054926>
- Aho, B., & Duffield, R. (2020). Beyond surveillance capitalism: Privacy, regulation and big data in Europe and China. *Economy and Society*, 49(2), 187-212. [doi.org/10.1080/03085147.2019.1690275](https://doi.org/10.1080/03085147.2019.1690275)
- Andrew, J. & Baker, M. (2021). The General Data Protection in the Age of Surveillance Capitalism. *Journal of Business Ethics*, 168, 565-578. <https://doi.org/10.1007/s10551-019-04239-z>
- Banerjee, S. B. (2008). Corporate social responsibility: The good, the bad and the ugly. *Critical sociology*, 34(1), 51-79. <https://doi.org/10.1177/0896920507084623>
- Bhattacharjee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. Textbooks Collection, 3.
- Blank, G., Dutton, W. H., & Lefkowitz, J. (2019). Perceived threats to privacy online: The internet in Britain, *the Oxford Internet Survey*, 2019. <http://dx.doi.org/10.2139/ssrn.3522106>
- Bleakley, P. (2023). Panic, pizza and mainstreaming the alt-right: A social media analysis of Pizzagate and the rise of the QAnon conspiracy. *Current Sociology*, 71(3), 509-525. <https://doi.org/10.1177/00113921211034896>
- Bovet, A., & Makse, H. A. (2019). Influence of fake news in Twitter during the 2016 US presidential election. *Nature communications*, 10(1), 7. <https://doi.org/10.1038/s41467-018-07761-2>
- Butcher, P. (2019). Disinformation and democracy: The home front in the information war. *EPC Discussion Paper*, 30 January 2019. [https://www.epc.eu/content/PDF/2019/190130\\_Disinformationdemocracy\\_PB.pdf](https://www.epc.eu/content/PDF/2019/190130_Disinformationdemocracy_PB.pdf)
- Chandler, D., & Fuchs, C. (2019). *Digital objects, digital subjects: Interdisciplinary perspectives on capitalism, labour and politics in the age of big data*. University of Westminster Press. <https://doi.org/10.16997/book29>
- Cinnamon, J. (2017). Social injustice in surveillance capitalism. *Surveillance & Society*, 15(5), 609-625. <https://doi.org/10.24908/ss.v15i5.6433>
- Dentith, M. R. X. (2016). The Problem of Fake News. *Public Reason* 8 (1-2):65-79.

- Elias, J. (2019). *Google contractor reportedly tricked homeless people into face scans*. CNBC News. Haettu 3.3.2024  
<https://www.cnn.com/2019/10/03/google-contractor-reportedly-tricked-homeless-people-into-face-scans.html#close>
- Eskola, J., & Suoranta, J. (1998). *Johdatus laadulliseen tutkimukseen*. Vastapaino.
- Fallis, D. (2015). What is disinformation?. *Library trends*, 63(3), 401-426.  
<https://doi.org/10.1353/lib.2015.0014>.
- Fetzer, J. H. (2004). Disinformation: The use of false information. *Minds and machines*, 14, 231-240.  
<https://doi.org/10.1023/B:MIND.0000021683.28604.5b>
- Fisher, M., Cox, J. W., & Hermann, P. (2016). *Pizzagate: From rumor, to hashtag, to gunfire in DC*. Washington Post, 6, 8410-8415. Haettu 5.3.2024  
[https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c\\_story.html](https://www.washingtonpost.com/local/pizzagate-from-rumor-to-hashtag-to-gunfire-in-dc/2016/12/06/4c7def50-bbd4-11e6-94ac-3d324840106c_story.html)
- Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, 58(1), 3-19.  
<https://doi.org/10.1177/0007650317727540>
- Foster, J. B., & McChesney, R. W. (2014). Surveillance capitalism: Monopoly-finance capital, the military-industrial complex, and the digital age. *Monthly Review*, 66(3), 1-31. [https://doi.org/10.14452/MR-066-03-2014-07\\_1](https://doi.org/10.14452/MR-066-03-2014-07_1)
- Gelfert, A. (2018). Fake news: A definition. *Informal logic*, 38(1), 84-117.  
<https://doi.org/10.22329/il.v38i1.5068>
- Gidaris, C. (2019). Surveillance capitalism, datafication, and unwaged labour: the rise of wearable fitness devices and interactive life insurance. *Surveillance & Society*, 17(1/2), 132-138.  
<https://doi.org/10.24908/ss.v17i1/2.12913>
- Gritsenko, D., & Silvan, K. (2018). Aluetutkimus big data-aikakaudesta. *Idäntutkimus*, 25(3-4), 47-52.  
<https://journal.fi/idantutkimus/article/view/77562>.
- Guess, A. M., & Lyons, B. A. (2020). Misinformation, Disinformation, and Online Propaganda. In N. Persily & J. A. Tucker (Eds.), *Social Media and Democracy* (pp. 10-33). chapter, Cambridge: Cambridge University Press.  
<https://doi.org/10.1017/9781108890960>
- Harris, T. (2017). *How a handful of tech companies control billions of minds every day*. Los Angeles, California, Katsottavissa:  
<https://www.youtube.com/watch?v=C74amJRp730>
- Hernández-Ramírez, R. (2019). On false augmented agency and what surveillance capitalism and user-centered design have to do with it.



*Journal of Science and Technology of the Arts*, 11(2), 18-27.  
<https://doi.org/10.7559/citarj.v11i2.667>

- Hirsjärvi, S. & Hurme, H. (2008). *Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö*. Helsinki: Gaudeamus Helsinki University Press
- Hirsjärvi, S., & Hurme, H. (2015). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Helsinki: Gaudeamus Helsinki University Press.
- Hirsjärvi, S., & Hurme, H. (2017). *Tutkimushaastattelu: Teemahaastattelun teoria ja käytäntö*. Gaudeamus.
- Hirsjärvi, S., Remes, P., Sajavaara, P., & Sinivuori, E. (2009). *Tutki ja kirjoita* (15. uud. p.). Tammi.
- Hirsjärvi, S., Remes, P., & Sajavaara, P. (1997). *Tutki ja kirjoita*. Tammi.
- Jørgensen, R. F., (2019). *Human rights in the age of platforms*. The MIT Press.
- Kallio, H., Pietilä, A. M., Johnson, M., & Kangasniemi, M. (2016). *Systematic methodological review: developing a framework for a qualitative semi-structured interview guide*. 72(12), 2954-2965. <https://doi.org/10.1111/jan.13031>
- Keller, M., (2023). *Mitä on tietosuoja?* Alma Talent. Helsinki.
- Lazer, D. M., Baum, M. A., Benkler, Y., Berinsky, A. J., Greenhill, K. M., Menczer, F., ... & Zittrain, J. L. (2018). The science of fake news. *Science*, 359(6380), 1094-1096. <https://doi.org/10.1126/science.aao2998>
- Li, J., & Su, M. H. (2020). Real talk about fake news: Identity language and disconnected networks of the US public's "fake news" discourse on Twitter. *Social Media+ Society*, 6(2).  
<https://doi.org/10.1177/2056305120916841>
- Macnish, K. N. (2019). Introduction to Privacy. *Data, Privacy and the Individual*. /IE University Press.
- Marwick, A. E., & Lewis, R. (2017). *Media manipulation and disinformation online*. Data & Society Research Institute.
- McCordle, M. (2003). Understanding generation Y. *Principal Matters*, (55), 28-31. <https://search.informit.org/doi/10.3316/ielapa.200305936>
- Meyer, R. (2018). The grim conclusions of the largest-ever study of fake news. *The Atlantic*, 8, 2018. Haettu 5.4.2024  
<https://www.theatlantic.com/technology/archive/2018/03/largest-study-ever-fake-news-mit-twitter/555104/>
- Mirsch, T., Lehrer, C., & Jung, R. (2017). Digital Nudging: Altering User Behavior in Digital Environments. In Proceedings of the 13th International Conference on Wirtschaftsinformatik (WI) 2017 (pp. 634-648). *Association for Information Systems*. AIS Electronic Library (AISeL).  
<http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1076&context=wi2017>

- Mirsch, T., Lehrer, C., & Jung, R. (2018). Making Digital Nudging Applicable: The Digital Nudge Design Method. In Proceedings of the 39th International Conference on Information Systems (ICIS) *Association for Information Systems*. AIS Electronic Library (AISeL).  
<http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1072&context=icis2018>
- Morozov, Evgeny. 2019. "Capitalism's New Clothes". *The Baffler* 4.2.2019. Haettu 1.5.2024. <https://thebaffler.com/latest/capitalisms-new-clothes-morozov>
- Murphy, M. H. (2017). Algorithmic surveillance: the collection conundrum. *International Review of Law, Computers & Technology*, 31(2), 225-242.  
<https://doi.org/10.1080/13600869.2017.1298497>
- Neuvonen, R. (2023). Mahdoton kilpajuoksu? Oikeus viestinnän kehityksen mahdollistajana. *Lakimies*, 121(7-8), 1109-1130. Haettu 1.4.2024  
<https://journal.fi/lakimies/article/view/136151>
- Nield, D., (2019). All the Ways Google Tracks You - and How To Stop It. *Wired*. Haettu 5.1.2024 <https://www.wired.com/story/google-tracks-you-privacy/>
- Nield, D., (2020). All the Ways Facebook Tracks You - and How to Limit It. *Wired*. Haettu 5.1.2024 <https://www.wired.com/story/ways-facebook-tracks-you-limit-it/>
- Orlowski, J. (ohjaaja) & Orlowski, J., Coombe D., Curtis, V. (käsikirjoittajat). (26.1.2020). Dokumenttielokuva. *The Social Dilemma*. Netflix
- Pennycook, G., & Rand, D. G. (2021). The psychology of fake news. *Trends in cognitive sciences*, 25(5), 388-402. <https://doi.org/10.1016/j.tics.2021.02.007>
- Puusa, J. & Juuti, P. (2020). *Laadullisen tutkimuksen näkökulmat ja menetelmät*. Gaudeamus.
- Rigatelli, S., (2021). Facebook-jättikanteelle tyrmäys Yhdysvalloissa – oikeuden päätös siivitti yhtiön arvon historialliseen biljoonaan dollariin. Yle Uutiset. Haettu 2.3.2024 <https://yle.fi/a/3-12000455>
- Ruckenstein, M., & Granroth, J. (2020). Algorithms, advertising and the intimacy of surveillance. *Journal of Cultural Economy*, 13(1), 12-24.  
<https://doi.org/10.1080/17530350.2019.1574866>
- Nikander, P., Hyvärinen, M., Ruusuvuori, J., Pöysä, J., Jolanki, O., Nikander, P., & Karhunen, S. (2010). *Haastattelun analyysi*. Vastapaino.
- Saaranen-Kauppinen, A. & Puusniekka, A. (2006). *KvaliMOTV – Menetelmäopetuksen tietovaranto*. Tampere: Yhteiskuntatieteellinen tietoaarkisto. Haettu 27.3.2024 <http://www.fsd.uta.fi/menetelmaopetus/>
- Shahin, S., & Zheng, P. (2020). Big data and the illusion of choice: Comparing the evolution of India's aadhaar and China's social credit system as

- technosocial discourses. *Social Science Computer Review*, 38(1), 25-41.  
<https://doi.org/10.1177/0894439318789343>
- Sirkkunen, E. (2016). Yksityisyys valvonnan verkoissa. *Media & viestintä*, 39(2), 117-136. <https://doi.org/10.23983/mv.61429>
- Sirkkunen, E., & Haara, P. (2017). *Yksityisyys ja notkea valvonta: Yksityisyys ja anonyymiteetti verkkoviestinnässä-projektin loppuraportti*.  
<https://urn.fi/URN:ISBN:978-952-03-0331-0>
- Suoranta, E. (2021). Shoshana Zuboffin Valvontakapitalismin aika ja friktion mahdollisuudet. *Kirjallisuudentutkimuksen Aikakauslehti Avain*, 18(2), 120-125. <https://doi.org/10.30665/av.103410>
- STT-Yle (2020). *Facebookia syytetään kilpailulain rikkomisesta ja valta-aseman väärinkäytöksestä Yhdysvalloissa – Instagram ja WhatsApp halutaan irrottaa emoyhtiöstä*. Yle Uutiset. Haettu 2.3.2024 <https://yle.fi/a/3-11690040>
- Trittin-Ulbrich, H., Scherer, A. G., Munro, I., & Whelan, G. (2021). Exploring the dark and unexpected sides of digitalization: Toward a critical agenda. *Organization*, 28(1), 8-25. <https://doi.org/10.1177/1350508420968184>
- Trochim, W. (10.11.2021). *Qualitative measures*. Conjointly.com. Haettu 1.1.2024 <https://conjointly.com/kb/qualitative-measures/>
- Tuomi, J., & Sarajärvi, A. (2018). *Laadullinen tutkimus ja sisällönanalyysi (Uudistettu laitos)*. Kustannusosakeyhtiö Tammi.
- Turow, J. (2011). *The Daily You: How the New Advertising Industry Is Defining Your Identity and Your Worth*. London. Yale University Press.  
<https://doi.org/10.1177/1461444814535723>
- Varghese, S. (2019). Pokémon Go was a warning about the rise of surveillance capitalism. *Wired*. Haettu 2.3.2024 <https://www.wired.com/story/the-age-of-surveillance-capitalism-facebook-shoshana-zuboff/>
- Venkatesh, N. (2021). Surveillance Capitalism: a Marx-inspired account. *Philosophy*, 96(3), 359-385. <https://doi.org/10.1017/S0031819121000164>
- Waldo, J., Lin, H. S., & Millett, L. I. (2010). Engaging privacy and information technology in a digital age: Executive summary. *Journal of Privacy and Confidentiality*, 2(1). <https://doi.org/10.29012/jpc.v2i1.580>
- Weinmann, M., Schneider, C., & Brocke, J. V. (2016). Digital nudging. *Business & Information Systems Engineering*, 58, 433-436.  
<https://doi.org/10.1007/s12599-016-0453-1>
- West, S. M. (2019). Data capitalism: Redefining the logics of surveillance and privacy. *Business & society*, 58(1), 20-41.  
<https://doi.org/10.1177/00076503177181>
- Westin, A. F. (2003). Social and political dimensions of privacy. *Journal of social issues*, 59(2), 431-453. <https://doi.org/10.1111/1540-4560.00072>

- Willis, L. E. (2020). Deception by Design. *Harvard Journal of Law & Technology* 34, 115. <https://ssrn.com/abstract=3694575>
- World Health Organization (WHO), 2024. *Infodemic*. Haettu 24.2.2024: [https://www.who.int/health-topics/infodemic#tab=tab\\_1](https://www.who.int/health-topics/infodemic#tab=tab_1)
- Yeung, K. (2019). 'Hypernudge': Big Data as a mode of regulation by design. In *The social power of algorithms* (pp. 118-136). *Routledge*. <https://doi.org/10.1080/1369118X.2016.1186713>
- Zwitter, A. (2014). Big data ethics. *Big data & society*, 1(2), 2053951714559253. <https://doi.org/10.1177/2053951714559253>
- Zuboff, S. (2015). Big other: Surveillance Capitalism and the Prospects of an Information Civilization. *Journal of Information Technology*, 30(1), 75-89. <https://doi.org/10.1057/jit.2015.5>
- Zuboff, S., (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books
- Zuboff, S. (2020). You Are Now Remotely Controlled. *The New York Times*. 24. Haettu 26.1.2024 <https://www.nytimes.com/2020/01/24/opinion/sunday/surveillance-capitalism.html>
- Zuboff, S. (2021a). You are the object of a secret extraction operation. *The New York Times*, 12. Haettu 26.1.2024 <https://www.nytimes.com/2021/11/12/opinion/facebook-privacy.html>
- Zuboff, S. (2021b). The coup we are not talking about. *The New York Times*, 29, 2021. Haettu 27.1.2024 <https://www.nytimes.com/2021/01/29/opinion/sunday/facebook-surveillance-society-technology.html>
- Zuboff, S. (2022). Surveillance capitalism or democracy? The death match of institutional orders and the politics of knowledge in our information civilization. *Organization Theory*, 3(3). <https://doi.org/10.1177/26317877221129290>

## LIITE 1 HAASTATTELUKYSYMYKSET

### Haastateltavan taustatiedot

- Kertoisitko nimesi ja ikäsi?
- Mitä älylaitteita käytät arjessasi?
- Mitä internet-pohjaisia alustapalveluita käytät päivittäin?

### Haastateltaville luettu alustus aiheesta:

”Valvontakapitalismi tarkoittaa liiketoimintaa, joka tekee rahaa ihmisistä jäävillä digitaalisilla jäljillä. Esimerkiksi suosittu internetalustat kuten Facebook, Google, Amazon, Instagram, WhatsApp, Snapchat ja Tiktok perustavat liiketoimintansa tähän malliin. Valvontakapitalismin liiketoimintaa hyödyntää näiden lisäksi myös arkisemmat toimijat, kuten puhelinoperaattorit ja kauppojen kanta-asiakasohjelmat.

Eli edellä mainitun tyyliiset yritykset keräävät näiden internetalustojen kautta dataa ihmisten arjen valinnoista ja käyttäytymisestä, ja tekevät tästä käyttäjistä kerätystä datasta ennusteita eli käyttäytymismalleja. Sen jälkeen yritykset myyvät näitä ennusteita ja kerätyn datan avulla tehtyjä analyyseja eteenpäin kolmansille osapuolille (esimerkiksi mainostajille), josta nämä yritykset saavat merkittäviä tuloja.”

### Kuluttajan tietoisuus valvontakapitalismista:

1. Oletko törmännyt termiin valvontakapitalismi aikaisemmin ja/tai onko edellä kuvattu liiketoimintalogiikka tuttu?
2. Onko sinulla tietoa tai käsitystä missä laajuudessa valvontakapitalismia toteutetaan?
3. Mitä tietoja ajattelet, että sinusta kerätään internetalustojen kautta?
4. Mitä ajattelet, että kerätyillä tiedoilla tehdään?
5. Oletko tietoinen siitä, että sinulle kohdennetaan mainontaa?
6. Oletko huomannut vastaanottavasi kohdennettua mainontaa erityisesti jonain tietynä ajankohtana/ajanjaksona?
7. Oletko huomannut vastaanottavasi tietynlaista sisältöä tiettyinä ajanjaksoina?
8. Onko mielestäsi internetistä löytyvä tieto luotettavaa?
9. Millä tavalla arvioit, onko joku tieto internetissä luotettavaa vai ei?

### Valvontakapitalismin vaikutukset kulutuskäyttäytymiseen:

10. Huomaatko olevasi riippuvainen älylaitteista tai internetalustoista?
11. Oletko huomannut, että sovellukset koittaisivat pitää sinua koukuttuneena?
12. Kuinka hyvin tunnet internetalustojen käyttöehdot, joihin annat suostumuksesi ja millä tavalla paneudut alustojen käyttöehtoihin?
13. Saatko mielestäsi tarpeeksi tietoa tietojenluovutus päätöksen tekemisen tueksi ja mistä syystä luovutat tietojasi internetalustoilla?
14. Teetkö mielestäsi tietoisien valinnan omien tietojasi luovuttamisesta?
15. Onko sinulla kokemusta siitä, että jäisit ilman jotakin palvelua, jos et anna lupaa tietojen keräämiseen?
16. Koetko voitavasi itse määrittellä, mihin tarkoitukseen henkilötietojasi käytetään?
17. Kuvitellaan tilanne, että olet lukemassa jotain haluamaasi uutista tai artikkelia ja sisällön päälle tulee banneri, jonka mukaisesti voit valita hyväksyä kaikki evästeet tai maksaa palvelusta pienen kuukausimaksun. Mikäli valitset maksaa kuukausimaksun, yritys ei seuraa sinua evästeiden avulla, kerää tietojasi tai esimerkiksi kohdenna mainontaa onlinekäyttäytymisesi mukaisesti. Kumman vaihtoehdon valitset ja miksi?
18. Kuinka paljon olisit valmis maksamaan yritykselle siitä, että se ei seuraa sinua?
19. Huomaatko, että sinulle kohdistettu sisältö vaikuttaa mielialaasi ja sitä kautta kulutuskäyttäytymiseesi? Millä tavalla?
20. Huomaatko kohdennetun mainonnan vaikuttavan kulutuskäyttäytymiseesi? Millä tavalla?
21. Oletko huomannut verkkokaupoissa alennuskuponkeja, joilla saat esimerkiksi 10 tai 15 prosentin alennuksen, jos rekisteröidyt jäseneksi? Mitä mieltä olet näistä? Kuinka usein tartut tällaisiin tarjouksiin?
22. Kuinka suuri tarjotun alennuksen pitäisi olla, että tartut siihen?

### Kuluttajien kokemat valvontakapitalismin vaikutukset:

23. Mitkä asiat koet valvontakapitalismissa hyödylliseksi?
24. Mitkä asiat koet valvontakapitalismissa haitalliseksi?
25. Koetko, että henkilötietosi ovat turvassa internetalustoilla, esimerkiksi tietojenkalasteluilta tai tietovuodoilta?
26. Oletko huolestunut siitä, että alustoilta kerätään yhä enemmän tietoa eri tarkoituksia varten? Mitä huolia aiheesta herää?
27. Ajatteletko, että tietojen keräämisestä ja valvontakapitalismista voisi olla seurauksia tulevaisuudessa? Millaisia seurauksia?
28. Millä tavalla ratkaisit valvontakapitalismista aiheutuvia ongelmia?

29. Kumman vaihtoehdon valitsisit; nykymallin, jossa omilla henkilötiedoilla rahoitetaan internetalustoilla toimivia palveluita eli hyödynnetään tätä valvontakapitalismin liiketoimintalogiikkaa, vai haluaisitko elää ennemmin samaan tapaan kuin ennen vanhaan, että tällaisia palveluita ei ollut lainkaan? Perustele miksi.