

Artikkeli



Yksityisyys valvonnan verkoissa

Tässä artikkelissa tarkastelen yksityisyyden rakentumista verkkovalvonnan kontekstissa. Tarkastelen kehitystä neljästä näkökulmasta: selvennän verkkovalvonnan käsitettä, erittelen taloudellisen verkkovalvonnan toimintatapoja ja niiden vaikutusta yksityisyyteen, tutkin verkon alustojen käyttöehtoja yksityisyyden kannalta sekä esittelen verkon käyttäjien yksityisyyskäsitteitä. Edellisten perusteella esitän johtopäätöksissä ehdotuksia mediatutkimuksen tehtäviksi verkkovalvonnan ja sen seurausten tutkimuksessa.

AVAINSANAT: verkkovalvonta, taloudellinen verkkovalvonta, verkkomainonta, yksityisyys, yksityisyyden suoja, verkkojulkisuus, Google, Facebook

Internetin ja mobiilin median käytöstä kertyvästä digitaalisesta jalanjäljestä eli henkilödatasta on tullut verkkotalouden keskeisin arvon luoja ja vaihdon väline. Jos me käyttäjät olimme 2000-luvun puolivälin internet -retoriikassa kuninkaantekijöitä, kymmenen vuotta myöhemmin meidät on mediapalvelinten uumenissa tiivistetty kuluttajaprofileiksi, joista käydään kauppaa.

Viimeistään 2010-luvulla internetin palveluiden ilmaisuus on osoittautunut myy-tiksi. Me maksamme verkon ”ilmaiset” palvelut henkilökohtaisella tiedolla, jota meistä usein huomaamattamme kerätään ja jonka perusteella kulutuskäyttäytymis-tämme seurataan, profiloidaan ja segmentoidaan. Asetelman voi tiivistää Ian Carria (2013) mukaillen: käytät ilmaista verkkotyökälua, mutta alusta (esimerkiksi Google tai Facebook) käyttää sinua.

Yritysten palvelimille kertyvä data sisältää yksityiskohtaisia ja yksityisyyden suo-jaan kuuluvia tietoa. Käyttäjätietoa keräävät yritykset vakuuttavat käyttävänsä tietoja vain parantaakseen palveluita ja toimivansa vastuullisesti henkilökohtaisen tiedon suhteen. Käyttäjätietoa kokoavat yritykset korostavat mielellään, että kyseessä on vaihtokauppa, jossa molemmat osapuolet voittavat yritykset tehokkaampia palveluita ja enemmän mainostuloja ja käyttäjät puolestaan parempia palveluita ja kiinnosta-

vampia mainoksia. Siten ei ole ihme, että käyttäjistä kerätyn tiedon hyväksikäyttöön liiketoimintansa rakentaneen Facebookin perustaja Mark Zuckerberg julisti jo 2010, että internetissä yksityisyys on ”jo katoamassa oleva normi” (Johnson 2010).

Yksityisyyden merkitystä ihmisen arjessa mittaavat kyselytutkimukset kertovat kuitenkin hieman toisenlaista tarinaa. Niiden valossa on selvää, että verkon käyttäjät ovat huolissaan yksityisyyden menetyksestä ja henkilötietojen keräämisestä (Madden 2014, Turow et. al. 2015, Sirkkunen 2015). Yksityisyyden menetys ja valvonnan kohteeksi joutuminen huolettavat verkon käyttäjiä ainakin yleisellä tasolla, joten yksityisyyden ei voi sanoa normina tyystin kadonneen. Yksityisyyden piiriin kuuluvalla tiedolla on paitsi kaupallista arvoa myös edelleen merkitystä ihmisten mielissä.

2000-luvulla verkon ja sosiaalisen median yksityisyyttä koskevassa tutkimuksessa kiinnitettiin paljon huomiota siihen, julkaisevatko esimerkiksi nuoret itsestään yksityisyyden kannalta herkkää aineistoa, jonka julkitulo voisi haitata heidän elämäänsä myöhemmin (ks. esim. Barnes 2006). Vähemmän huomiota on saanut se, miten henkilötietoihin, profilointiin ja segmentointiin perustuva liiketoiminta suuntaa teknologioiden kehitystä ja muokkaa osaltaan yksityisyyden rajoja, medioiden toimintatapoja, mediasisältöjä ja mediamaisemaa. Kyseessä on niin perusteellinen muutos internetin taloudessa ja liiketoimintamalleissa, että sen merkitystä ja vaikutuksia on syytä pohtia erityisesti mediatutkimuksen näkökulmasta. Tässä artikkelissa tarkoituksena on selvittää, mitä yksityisyydelle on tapahtumassa käyttäjätiedon keräämiseen perustuvan verkkotalouden aikakaudella. Tavoitteena on kytkeä yksityisyys ja sen muutokset teknologiavälitteiseen vallankäyttöön (Gillespie 2010, van Dijck 2013, Langlois & Elmer 2013). Tämän teen selventämällä valvonnan ja verkkovalvonnan käsitteitä, tutkimalla millaisia rakenteellis-teknologisia ulottuvuuksia taloudellisella verkkovalvonnalla on ja miten rakenteet muokkaavat verkkoalustojen toimintatapoja ja kehystävät käyttäjille tarjoutuvia toimintamahdollisuuksia.

Tutkimuskysymykset ovat seuraavat:

- Mitkä ovat taloudellisen verkkovalvonnan menetelmät?
- Miten yksityisyyttä koskeva lainsäädäntö toteutuu tällä hetkellä internetin palveluissa?
- Miten suomalaiset verkon käyttäjät näkevät yksityisyydensuojan ja omat vaikutusmahdollisuutensa verkossa?
- Mitkä ovat verkkovalvonnan ja yksityisyyden muutosten haasteet mediatutkimukselle?

Artikkelin aluksi teen eron taloudellisen ja valtiollisen verkkovalvonnan välillä. Sen jälkeen osoitan esimerkkien avulla, miten taloudellinen valvonta on rakentunut verkkomainontaan ja sen teknologioihin. Tämän jälkeen siirryn tarkastelemaan yksityisyyden suojaa sekä analysoin internetin suosituimpien alustojen yksityisyyskäytäntöjä yksityisyyden näkökulmasta. Seuraavaksi siirryn käyttäjiin ja esittelen, miten suomalaiset verkon alustojen käyttäjät ovat vastanneet yksityisyyttä ja verkkovalvontaa koskevassa mielipidetutkimuksessa. Artikkelin lopussa osoitan, miten rakenteelliset muu-

tokset ovat johtaneet paitsi vähenevään yksityisyydensuojaan myös uudenlaisten valvontakoneistojen muodostumiseen sekä viittoilen samalla tietä kriittiselle media-tutkimukselle.

Valvontaa verkon aikakaudella

Monet yhteiskuntateoreetikot katsovat, että valvonta eri muodoissaan kietoutuu yhteen modernin kansallisvaltion ja kapitalismin syntymisen kanssa (esim. Giddens 1984). Yksityisyyden, yksityisomistuksen ja valvonnan välistä dialektiikkaa voinee pitää kapitalismin rakenteellisena piirteenä (Fuchs 2011a, 144). Klassinen esimerkki valvonnan ja teknologian yhdistymisestä on Jeremy Benthamin 1700-luvun lopussa vankiloita varten kehittänyt keskusvalvontajärjestelmä, panoptikon, joka Foucaultin tulkitsemana on kehittynyt metaforaksi valvonnan läpitunkemasta, sisäistettyyn kuriin perustuvasta yhteiskunnasta (Foucault 1980, Brunila 2014, 77).

Valvonnan muodot ovat teknologisoituneet edelleen Benthamin ajoista. Yksityisyyttä ja valvonnan teknologioita käsitelleet tutkijat ovat jo vuosikymmeniä korostaneet tietojenkäsittelyn ja tietokoneen merkitystä. Tätä vaihetta on kutsuttu muun muassa uudeksi valvonnaksi, datavalvonnaksi, elektroniseksi panoptikoniksi, elektroniseksi valvonnaksi tai digitaaliseksi valvonnaksi (Fuchs 2012 b, 1). Gary T. Marxin mukaan uutta on se, että teknologian avulla on mahdollista entistä tehokkaammin koota yksityisyyden piiriin kuuluvaa tietoa. Hänen mukaansa ”vanhan” valvonnan aikaan valvova taho tiesi suurin piirtein samat asiat kuin valvonnan kohdekin, sillä tietoja ei voitu poimia eri lähteistä ja yhdistellä kattaviksi ja yksityiskohtaisia henkilöprofileja luoviksi tietokannoiksi. ”Uuden” eli digitalisoituneen datavalvonnan tunnuspiirteitä on erityisesti se, että ”valvoja tietää asioita, joita valvottava ei tiedä” (Fuchs ym. 2012b, 1, myös Bauman & Lyon 2013).

Sosiologit Zygmunt Bauman ja David Lyon katsovat, että valvonta kuuluu jälkimodernin yhteiskunnan ytimeen. Jo Baumanin ja Lyonin keskustelukirjan nimi, *Liquid Surveillance* (2013) kertoo, miten valvonta osana baumanilaista notkeaa modernia ulottuu kaikkialle – matkustukseen, pakolaisvirtojen kontrollointiin, kaupunkien tilalliseen järjestykseen, kulutukseen ja ostamiseen, internetin käyttöön ja sosiaalisen median alustoihin saakka. Baumanin mukaan elämme, paitsi notkean modernin aikakautta, myös jälkipanoptisessa yhteiskunnassa. Kun modernin aikakauden luoman keskeisen valvontakoneiston eli Benthamin panoptikonin kohteet epäilivät, että joku jossain juuri nyt ehkä valvoo heitä, niin jälkipanoptisen yhteiskunnan tunnuspiirteitä on, että yhtä valvovaa tahoja tai katsetta on mahdotonta osoittaa, valvontaa on kaikkialla ja ei missään. Ajatus valvonnasta on arkipäiväistynyt ja valvonnan kohteet valvovat vapaaehtoisesti itse itseään käyttämällä älypuhelimia, internetiä ja asiakas- ja luottokortteja (Bauman & Lyon 2013). Brunila kutsuu tilannetta filosofi Daniel DeLandaan lainaten panspektriseksi valvonnaksi, jossa yhden valvovan sensorin sijasta lukemattomat sensorit keräävät meistä tietoa koko ajan ja kaikkialla (Brunila 2014, 80).

Verkko on tuonut valvonnan yhä uusille alueille. Tiivistetysti muotoiltuna verkkovalvonta on systemaattista ihmisten toimintojen tai viestinnän seuranta internetin ja mobiiliviestinnän mahdollistaman teknologian avulla. Sosiaalisen median alustojen yleistymisen on tuonut lisää mahdollisuuksia ja elämäalueita valvonnan piiriin. Trottierin ja Lyonin (2012) mukaan esimerkiksi Facebookilla on ainakin neljä piirrettä, jotka mahdollistavat uudenlaisia verkkovalvonnan muotoja. Ensinnäkin Facebookin käyttäjät rakentavat omia ja ystäviensä identiteettejä, joista on helppo tehdä johtopäätöksiä elämäntavoista ja kulutustottumuksista. Toiseksi Facebookissa tapahtuva vuorovaikutus tuottaa sinällään ainutlaatuista tietoa käyttäjien sosiaalisuuden muodoista ja dynamiikasta. Kolmanneksi Facebookissa henkilökohtaiset sosiaaliset verkostot tulevat näkyviksi, mitattaviksi ja prosessoitaviksi. Neljänneksi sosiaalisen median sisältö on helposti kontekstualisoitavissa ja sisällön tekijät jäljitettävissä. (Trottier & Lyon 2012, 89.)

Verkon käyttäjien jälkeensä jättämistä jäljistä ovat kiinnostuneita monenlaiset tahot ja toimijat. Yhtäältä kaupalliset yritykset keräävät tietoja verkon käyttäjistä sekä profiloivat ja lajittelevat yleisöään. Näiden yritysten voi sanoa harjoittavan *taloudellista verkkovalvontaa* (Bauman & Lyon 2013, 54). Toisaalta tietoverkoissa toimivat Yhdysvaltojen NSA:n, Britannian GCHQ:n, Ruotsin FRA:n ja Venäjän FSB:n kaltaisen turvallisuuspalvelut, jotka harjoittavat verkon käyttäjien *valtiollista verkkovalvontaa* etupäässä kansallisen turvallisuuden nimissä.¹

Joissakin tapauksissa valtiollinen ja taloudellinen valvonta voivat yhdistyä. Edward Snowdenin paljastama PRISM-ohjelma osoitti, että sellaiset verkkomaailman jätit kuin Microsoft, Yahoo, Google, Facebook, Paltalk, YouTube, Skype, AOL ja Apple ovat luovuttaneet tietoja niin ulkomaisista kuin yhdysvaltalaisista käyttäjistään NSA:lle. Voidaankin perustellusti sanoa, että digitaalinen arkielämämme on jatkuvan valvonnan ympäröimää, ja että hallinnon ja talouden intressit synnyttävät vaihtelevia valvontateknologisia verkostoja ja koosteita (Haggerty & Ericson 2000; Cohen 2012).

On syytä myös muistaa, että internet ja digitaalinen mediateknologia erilaisine verkko- ja mobiilisovelluksineen mahdollistaa niin sanotun vastavalvonnan, jossa kohteet kääntävät valvonnan suunnan valvojiin tai viranomaisiin (esim. Mann ym. 2003, 332). Tärkeä valvonnan välttämisen muoto on myös Tor-verkon kaltaisten salausteknologioiden käyttö, joka on yleistynyt muun muassa Snowden -paljastusten seurauksena. Internetissä on edelleen mahdollista luoda ”puolivarjoisia tiloja”, joissa käyttäjät voivat toimia halutessaan anonymisti tai rajoittaa viestintää vain saman mielisten pariin. Salausteknologiat mahdollistavat ainakin jossain määrin käyttäjien suojautumisen esimerkiksi valtiolliselta valvonnalta (Nikkanen 2014, 143). On selvää, että valvonnan välttämällä on erityistä merkitystä sananvapauden toteutumisen kannalta esimerkiksi valtiollisen kontrollin oloissa.

Näkyvissä on paradoksaalinen tilanne, jossa valtiollisen valvonnan varsinaiset kohteet eli kansainväliset terroristisolut ja rikollisryhmät ovat jo siirtyneet käyttämään tehokkaita salausten menetelmiä, ja turvallisuusviranomaisten massavalvonnan kohteeksi jäävätkin etupäässä tavalliset verkon käyttäjät, jotka eivät salaa viestintäänsä. Taloudellinen tai valtiollinen verkkovalvonta edellyttää toimiakseen luottavaisia verkon käyttäjiä (esim. Sloop & Gunn 2010).

Verkkoviestinnän ja teknologian kehitys on siis luonut uusia mahdollisuuksia valvonnalle, joka on sinänsä muodossa tai toisessa leimannut moderneja yhteiskuntia jo vuosisatoja. Valvontaa verkossa on hyödyllistä tarkastella ainakin kahdesta hahmottelemastani näkökulmasta, sillä valtiollisella ja taloudellisella valvonnalla on erilaiset toimintalogiikkansa ja teknologiansa.

Taloudellisen valvonnan menetelmiä

Seuraavaksi siirryn käsittelemään tarkemmin taloudellisen verkkovalvonnan kehitystä ja valvonnan menetelmiä, koska ne ovat toistaiseksi jääneet vähälle huomiolle mediatutkimuksessa. Käytän esimerkkeinä Googlen ja Facebookin käyttämiä keinoja käyttäjätietojen keräämisessä. Nostamalla esiin datan keräämisessä käytettävät keinot, kuten klikkausten mittaus, evästeet, tykkäysnappulat ja kirjautumisprotokollat selvennän konkreettisesti, miten valvonta on lomittunut osaksi verkon alustojen arkista käyttöä.

On syytä muistaa, että meitä herkeämättä seuraava valvontakoneisto ei ole yhden tietoisin suunnitelman tulosta, vaan että seurannan keinot ovat muodostuneet keskeiseksi osaksi verkkomainonnan prosesseja vähitellen. Turow (2011) kuvaa osuvasti mainonnan muotoutumista internetissä. Turowin mukaan vielä 1990-luvulla mainostajat eivät luottaneet internetiin mainosvälineenä juuri lainkaan. Ongelmana oli tuolloin se, että eri sivustojen kävijämääriä ei osattu luotettavasti mitata ja mainostajille annettiin epätarkkaa tietoa verkkomainonnan tehokkuudesta.

Vähitellen internetin vahvuudet mainosalustana kuitenkin paljastuivat. Kehitettiin uusia seurannan teknologioita, kuten klikkauksien mittaaminen sekä evästeet, joiden avulla saatiin kvantifioitua tietoa mainonnan seuraamisesta ja kyettiin identifioimaan ja jäljittämään käyttäjiä. Klikkauksien avulla markkinoijat näkivät, kuinka paljon mainoksia tai muuta sisältöä on todella käyty katsomassa. Muun muassa evästeiden ja JavaScript-komentokielen avulla julkaisijat ja mainostajat kykenevät tunnistamaan ja tallentamaan mainossivulla vierailleen tietokoneen ja vähitellen myös yhdistämään käyttäjästä kertyneen datan tiettyyn henkilöön.

Mainonnan tarpeet sanelivat siis osaltaan seurantateknologian kehitystä. Tärkeä edelläkävijä oli Google, joka alkoi laskuttaa mainostajia vain, jos käyttäjä todella klikkasi mainosta. Tämä oli merkittävä kehitysaskel, sillä aiemmin joukkoviestinnän aikakaudella mainostajat joutuivat lähinnä arvailemaan viestinsä tehokkuutta. Valvontateknologioiden vähittäinen kehitys on johtanut lopulta lähes saumattomaan valvontaan, jossa esimerkiksi Google voi seurata, mitä käyttäjä tekee internetissä tai mobiiliverkossa ja mitä mainoksia hän avaa tietokoneilla, tableteilla tai älypuhelimella. Samalla yhtiö voi paikantaa henkilön liikkeitä maantieteellisesti mobiililaitteiden seurannan avulla.

Googlen tavoitteena on saada kaikki internetin käyttäjät rekisteröitymään yhtiön alustoille ja sen jälkeen seurata heidän toimintaansa ja liikkeitään verkossa ja lopulta myös ostopäätöksiään supermarkettien, kahviloiden ja muiden liikkeiden kassoilla

(Turow 2011, 157). Eri alustoille levittäytyvän valvonnan seurauksena Google tietää jokaisesta palveluitaan käyttävästä kuka hän on, mistä hän pitää ja millainen on hänen ystäväpiirinsä. Kasautuvan tiedon ja tarkkojen käyttäjäprofiilien avulla Google pyrkii ennakoimaan, mitä tuotteita tietty henkilö tarvitsee eri vuorokaudenaikoina ja milloin hänelle ylipäätään kannattaa kohdistaa mainontaa. Mainostajan kannalta kulutuksen ennustettavuus on tärkeä tavoite ja käyttäytymisen ennakointi onkin käyttäjien valvonnan ja tiedon keräämisen keskeinen motiivi (emt. 159).

Google kuuluisa hakualgoritmi, Pagerank, joka asettaa verkkosivut järjestykseen niihin johtavien linkkien määrän perusteella, on saanut tuekseen muita Googlen algoritmeja, jotka kiihdyttävät verkon mainoskäyttöä (Brunila 2014). Esimerkiksi AdSense-ohjelman avulla bloggaajat ja muut yksittäiset sisällöntuottajat voivat sijoittaa Googlen välittämiä ja hinnoittelemaa mainoksia sivuilleen saaden pienen osuuden mainostuotosta itselleen. AdWord suodattaa Googlen hakujen perusteella sopivia mainoksia tuotteesta mahdollisesti kiinnostuneelle Googlen käyttäjälle. AdRank puolestaan arvioi mainosten suosiota ja klikkausten määrän ja niiden klikkailuun käytetyn ajan perusteella.

Algoritmien ohjaamaa on myös huutokauppa, jossa mainostajat kilpailevat tarjoksillaan käyttäjistä, jotka ovat tehneet äskettäin hakuja mainostettaviin tuotteisiin liittyvistä aihealueista. Tällaiset käyttäjien selaushistorioiden reaaliaikaiset huutokaupat ovat levinneet myös suomalaisen verkkomedian mainosmyyntiin (Virranta 2015). Facebook on kehittänyt seuranta erityisesti tarkemman käyttäjäprofiloinnin suuntaan. Perusta luodaan sillä, että Facebook kerää tietoa kaikesta, mitä käyttäjät tekevät Facebookissa ja muilla yhtiön omistamilla alustoilla, jotta yhtiö voi myydä käyttäjiensä tarkat kuluttajaprofiilit mainostajille. Erityisen hyödyllisiä profiilien muodostamisessa ovat tykkäämistä (ja nyttemmin myös muita tunteita) osoittavat reaktionappulat sekä Facebookin tunnuksilla kirjautuminen eri verkkopalveluihin. Rektionappulat osoittavat yrityksille selkeästi, miten verkkomarkkinointi on onnistunut ja mistä tuotemerkeistä pidetään ja milloin käyttäjä on sopivassa mielentilassa vastaanottamaan mainontaa (Griffin 2016). Samalla käyttäjien sosiaaliset profiilit täydentyvät jatkuvasti makutottumusten osalta. Tykkäämistä ja muita tunteita osoittavat rektionappulat ovat siis käyttäjäprofiilien rakentamisen kannalta olennaisia (Gerlitz & Helmond 2013). Facebookin tunnuksilla kirjautuminen eri verkkopalveluihin puolestaan laajentaa Facebookin valvontamahdollisuuksia edelleen myös muille kuin omille verkkoalustoille.

Facebook toimii myös alustana muiden yritysten tekemälle käyttäjätiedon keräämiselle. Facebookissa mainostavat voivat esimerkiksi koota mainostensa klikkaajista ja heidän ystävistään koostuvia mikroverkostoja evästeiden avulla. Ystävien kautta päästään käsiksi yhä uusiin verkostoihin, joiden jäsenille voidaan kohdistaa mainontaa niin Facebookissa mutta myös sen ulkopuolella (Turow 2011, 147). Mainostajat luovat myös ilmaisia pelejä ja muita liitännäisiä, joita Facebookin käyttäjät voivat lisätä sivuilleen ja joiden kautta yrityksille siirtyy tietoa käyttäjistä ja heidän reaktioistaan. Vuonna 2016 Facebook ilmoitti alkavansa kerätä tietoja kaikista internetin käyttäjistä asentamalla tykkää -nappuloita ja muita koodinpalasia myös Facebook-alustojen ulko-

puolelle. Näin yhtiö voi kilpailla paremmin Googlen kanssa käyttäjien seurannan ja mainosten välittämisen ja myymisen alueilla (Marshall 2016).

Profiloitun mainonnan tavoitteena on paikallistaa halutun tyyppiset kuluttajat mistä tahansa internet- tai mobiiliverkon kolkasta ja tarjota mainos sopivaan aikaan juuri sinne missä kohteet sattuvat olemaan (Turow 2011, 85). Kun käyttäjätieto yhdistetään reaaliaikaiseen hinnoitteluun, tarkasta käyttäjäprofiilista saadaan mahdollisimman paljon hyötyä. Myös hinnoittelu on muuttumassa henkilökohtaiseksi, esimerkiksi niin, että tietyille asiakasryhmille annetaan tietoa alennuksista, toisille taas ei. Profilointi ei rajoitu pelkästään kohteille suunnattuun mainontaan ja erikoistarjouksiin. Se ulottuu myös median sisältöihin, kuten journalismiin, muokaten niitä erilaisille kohderyhmille.

Liikomme siis verkossa algoritmien seuraamina. Turow kutsuu yritysten harjoittamaa verkkovalvontaa pitkäksi klikkaukseksi (emt. 11–12). Pitkällä klikkauksella tarkoitetaan saumatonta prosessia, jossa seurataan henkilön reaktioita ensimmäisestä verkkomainoksesta eteenpäin tuotteen ostamiseen tähtäävällä polulla. Päämääränä on paikantaa sopivan profiilin omaava kuluttaja, päättää millaisilla tuotetarjouksilla hänet ympäröidään ja jäljittää mainonnan seuraukset mahdollisimman tarkasti. Prosessi voi sisältää monenlaista markkinointiponnistuksia. Se voi koostua tuotetta markkinoivasta, kevyesti journalismia muistuttavasta jutusta, tuotteen kauppaamisesta profiloituilla mainoksilla sekä alennustarjouksilla, jotka voidaan suunnata paikallisesti esimerkiksi älypuhelimien sijainnin perusteella. Kun tuote vielä ostetaan etukortilla, luottokortilla tai käteiskortilla, syntyy ketju, jossa kuluttaja tuottaa koko ajan tietoja häntä seuraaville tahoille, jotka puolestaan tarkentavat henkilön profiilia ja rakentavat edelleen markkinointiin käytettävää verkkomainetta.

Näin on luotu markkinoijille mittauksiin perustuvia tapoja profiloida käyttäjiä, kohdistaa mainontaa vain halutuille, yksittäisille henkilöille haluttuihin ympäristöihin. Samalla voidaan seurata mainonnan tehokkuutta ostopäätöksiin saakka. Verkkomainonnan kehityksen seurauksena perinteisten, toimitettuja sisältöjä tarjoavien mediatalojen merkitys on vähenemässä mainonnan ja yleisön yhdistäjänä. Paine luoda mainostettaville tuotteille sopivaa ympäristöä on synnyttänyt esimerkiksi Demand Median kaltaisia sisältöfarmeja (Vehkoo 2011, 89). Ne tekevät freelancevoimin keveitä ja viihdyttäviä uutisia juuri niistä kysymyksistä, joita käyttäjät ovat tehneet hakukoneilleen. Suurin uhka perinteisellä tavalla journalistista sisältöä tuottaville mediaryityksille on, että mainoksen esiintymisympäristöllä – esimerkiksi journalismilla – ei ole enää entisenlaista merkitystä. Suuret mediatalot ovat menettäneet vaikutusvaltaansa, ja nykyään mainostajat painostavat myös perinteisiä julkaisijoita toimimaan verkkoyritysten tapaan eli antamaan lisää tietoa sivujensa käyttäjistä ja tekemään tarkempia mittauksia mainosten vaikuttavuudesta. (Turow 2011, 83)

Yhteenvetona voi sanoa, että sen jälkeen kun mainonnasta on tullut internet-talouden keskeisin ansaintalähde, käyttäjistä kerättävä tieto on muuntunut yhä arvokkaammaksi. Tietoja käyttäjistä keräävät niin klikkaukset, tykkäykset ja muut seurannan keinot ovat muovautuneet Turown mainitsemäksi pitkäksi klikkaukseksi eli saumattomaksi seurannaksi, joka ulottuu tuotteiden ostovaiheeseen saakka. Taloudellisen

valvonnan myötä kerätyn käyttäjätiedon keskittyminen muutamille, lähinnä Yhdysvalloista käsin toimiville yrityksille on muuttamassa internetin taloudellista rakennetta entistä keskittyneempään suuntaan. On myös selvää, että suuret toimijat ohjaavat käyttäjille tarjoutuvia palveluita ja niiden teknisiä ominaisuuksia haluamaansa suuntaan. Keskittymiskehityksen seurauksena on ollut se, että eurooppalainen yksityisydensuojaa turvaava lainsäädäntö on joutunut törmäyskurssille yhdysvaltalaisen lainsäädännön ja suuryritysten taloudellisten intressien kanssa. Seuraavaksi siirrynkään tutkimaan sitä, millainen merkitys taloudellisella verkkovalvonnalla on erityisesti yksityisydensuojalle lainsäädännön tasolla.

Kamppailua verkon yksityisyyden rajoista

Kamppailua eurooppalaisen ja yhdysvaltalaisen yksityisyyskäsitteen välillä käydään paraikaa muun muassa EU:n tuomioistuimessa. Vaikka EU on kyennyt saamaan aikaan yksittäisiä muutoksia käyttöehtoihin, kuten esimerkiksi Googlen myöntymisen vanhentuneiden ja virheellisten henkilötietojen poistamiseen Euroopassa (ns. Oikeus tulla unohdetuksi -periaate), paljon ristiriitoja on vielä jäljellä. Uusia ongelmia ratkottavaksi on luonut muun muassa EU-tuomioistuimen vuoden 2015 lokakuussa antama ns. Schrems-tuomio, jossa purettiin EU:n ja USA:n välinen ns. safe harbour -järjestely, jonka perusteella yhdysvaltalaisyrietykset olivat aikaisemmin saaneet siirtää eurooppalaisten henkilötietoja Yhdysvaltoihin. Tuomiossaan EU-tuomioistuin katsoi, että sopimus rikkoi EU-kansalaisten perusoikeuksia ja että yhdysvaltalaisyrietysten tulee muuttaa käytäntöjään EU-lainsäädännön mukaisiksi (Koistinen 2016). Jonkinlainen periaatteellinen yhteisymmärrys yhdysvaltalaisyrietysten käytäntöjen muuttamisesta EU-lainsäädännön mukaisiksi syntyi EU:n ja yhdysvaltalaisyrietysten välillä keväällä 2016, mutta tätä kirjoitettaessa on vielä epäselvää, pääsevätkö lainsäätäjät sittenkään kaikista yksityiskohdista yksimielisyyteen.

Yksityisyyden rajat ovat siis muuttamassa. Seuraavaksi tutkin sitä, mille keskeisille periaatteille yksityisyyden suoja on länsimaisessa lainsäädännössä rakennettu ja miten suurten verkkoalustojen käyttöehdot ovat mukautuneet lainsäädännön suuriin linjoihin.² Vertailen Googlen ja Facebookin yksityisyyskäytäntöjä Soloven (2008) esittämään yksityisyyden taksonomiaan. Esittelen myös belgialaisen, EU-lainsäädäntöä ja Facebookin käytäntöjä koskevan raportin löydöksiä. (Van Alsenoy et. al. 2015).

Solove (2008) on rakentanut yksityisyyden taksonomian empiirisesti ”alhaalta ylöspäin” kooten ja luokitellen yksityisyyttä koskevaa säännöstöä pääosin länsimaiden lainsäädännöstä. Taksonomian avulla on mahdollista tarkastella sitä, miten lainsäätäjät ovat ymmärtäneet ja operationalisoineet yksityisyyden käsitteen lainsäädännössä.

Soloven taksonomia (emt. 104–105) lähtee liikkeelle tiedon tai datan kokoamiseen liittyvistä ongelmista, jatkaen tiedon prosessoinnilla ja levittämällä ja päättyä yksityisyyttä kohtaan tehtyihin avoimiin hyökkäyksiin. Soloven mukaan länsimaisten yksityisyyden määritelmien ydintä ovat muun muassa oikeus yksinäisyyteen, oikeus

rajoittaa muiden ihmisten puuttumista omiin tekemisiin tai asioihin, oikeus kontrolloida ja salata henkilökohtaisia tietoja, oikeus suojata omaa yksilöllisyyttään sekä oikeus jakaa intiimin piiriin kuuluvia asioitaan vain haluamiensa ihmisten kanssa (Solove 2008).

Soloven taksonomian kannalta Googlen toiminta näyttää ongelmalliselta ainakin kolmessa mielessä. Ensinnäkin Googlen tapa yhdistellä tietoa eri lähteistä ja koota tarkkoja käyttäjäprofileja on lähellä aggregointia, eli tietokokonaisuuksien yhdistelemistä yksityisyyttä loukkaavalla tavalla. Myös se, että käyttäjät eivät ole antaneet eksplisiittisesti lupaa kaikkeen siihen, mitä heistä kerätyllä datalla tehdään, on lähellä Soloven taksonomian mukaista toissijaista käyttöä, eli datan käyttöä muihin tarkoituksiin kuin mitä varten se oli alun perin koottu. Koska Googlen käyttäjiä ei myöskään päästetä päättämään heitä koskevan tiedon käsittely- ja käyttötavoista, ollaan myös lähellä Soloven mainitsemaa ulkopuolelle sulkemista.

Arvioin myös Facebookin käyttöehtoja³ Soloven taksonomian kannalta. Facebookin käytännöt vaikuttavat ainakin yhtä ongelmallisilta kuin Googlenkin. Tietoja kerätään, yhdistellään ja käytetään yksityisyydensuojaa mahdollisesti loukkaavalla tavalla. Kaikkeen datan prosessointiin ei ole pyydetty eksplisiittisesti lupaa tai datan käsittelytavat on ilmaistu epäselvästi käyttäjille. Facebookin käyttäjät eivät todennäköisesti tiedä, mitä ja miten Facebookin kumppaniyritykset keräävät tietoa käyttäjistä. Käyttäjät eivät myöskään pääse mukaan omia tietojaan koskevien päätösten tekemiseen.

Facebookin käyttäjilleen tarjoama puutteellinen yksityisyyden suoja on herättänyt arvostelua eri puolilla Eurooppaa. Esimerkiksi Leuvenin ja Brysselin yliopistojen raportissa (Van Alsenoy et.al. 2015) käydään läpi Facebookin vuonna 2015 uudistamat käyttöehdot käyttäjien oikeuksien kannalta. Raportissa todetaan, että Facebook kerää ja yhdistelee käyttäjiltä lupaa kysymättä entistä enemmän henkilötietoja omistamiensa yritysten, yhteistyösivustojen ja mobiiliapplikaatioiden avulla.⁴ Facebookin omistamista yrityksistä esimerkiksi Instagram ja WhatsApp keräävät paljon nuoria käyttäjikseen, jotka tulevat näin tiedonkokoamisen ja seurannan kohteiksi, vaikka eivät ole lainkaan käyttäneet Facebookia tai ovat luopuneet sen käytöstä.

Raportti myöntää Facebookin antavan uudistetuissa ehtoissaan entistä enemmän tietoa siitä, miten yhtiö käyttää käyttäjistä kerättyä tietoa ja miten käyttäjä voi paremmin hallita tietojaan, mutta lähinnä vain suhteessa muihin Facebookin käyttäjiin. Uudetkin ehdot ja käytäntöjen kuvaukset sisältävät entisen perusongelman, joka on se, että yhtiön oman toiminnan kuvaaminen yksityisyyttä koskevan tiedon keräämisessä ja käytössä jää niukaksi. Belgialaisraportin mukaan ainakin vuoden 2015 käyttöehdot sisälsivät edelleen epäoikeudenmukaisia ja eurooppalaista yksityisyyden – ja kuluttajansuojan henkeä rikkovia sopimusmuotoiluja. Raportin kirjoittajien mukaan Facebook asettaa käyttäjät ota tai jätä -tyyppiseen tilanteeseen, jossa ei ole muuta vaihtoehtoa kuin hyväksyä ehdot, jos haluaa palvelun käyttöönsä. Raportti katsookin, että Facebook käyttää hyväksi määräävää asemaansa sosiaalisen median palveluiden joukossa EU-lainsäädännön vastaisesti (Van Alsenoy et.al. 2015).

Suomalaisittain ymmärretty korkea yksityisyydensuoja on siis kokenut kovia viime aikoina erityisesti verkkoympäristössä. Vertailuni osoitti, että sekä Soloven taksono-

mian että EU-lainsäädännön näkökulmasta yhdysvaltalaisen verkkojättien yksityisyyskäytännöissä on kosolti toivomisen varaa.

Yksityisyyden suojaa Suomessa kaventavat taloudellisen valvonnan lisäksi myös muut hankkeet. Erityisesti valtiollisen verkkovalvonnan aloittaminen lähivuosina on johtamassa yksityisyydensuojan muutoksiin, sillä valmisteltavana oleva verkkovalvontalaki tulee todennäköisesti vahvistamaan viranomaisten seurantakeinoja verkossa. Lain laatimisen perusongelma on se, miten yksityisyyttä suojaavat kansalaisten perusoikeudet ja verkkovalvonnan lisääminen sovitetaan yhteen (Sajari 2015).

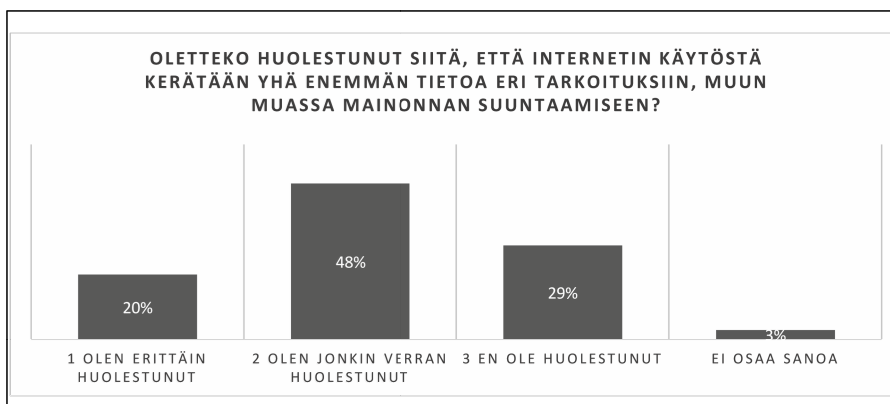
Seuraavaksi siirrän näkökulmani verkkomaailman rakenteista eli taloudesta ja lainsäädännöstä valvonnan varsinaisiin kohteisiin eli verkon alustojen käyttäjiin ja selvittelen sitä, miten he mielipidetutkimuksen valossa ymmärtävät yksityisyytensä ehdot ja käyttäjistä kerättävän tiedon merkityksen.

Suomalaiset ja verkon yksityisyys

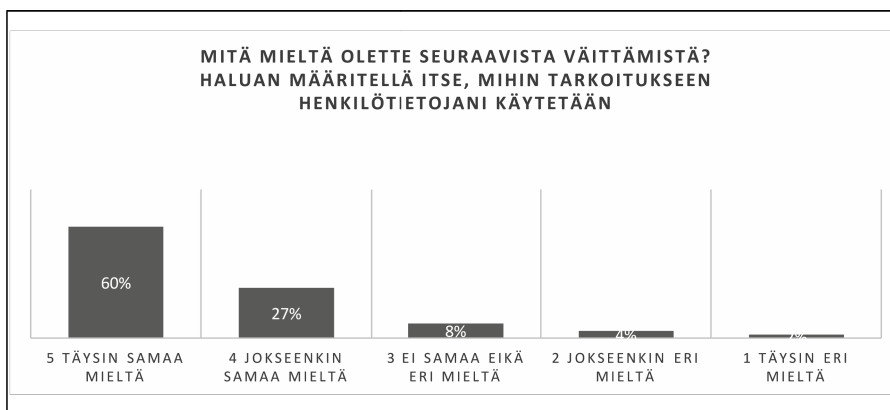
Tavallisten suomalaisten verkon käyttäjien suhtautumista yksityisyydensuojan toteutumiseen ei ole tutkittu kovinkaan kattavasti. Julkista keskustelua esimerkiksi verkkovalvontalasta ja valtiollisesta verkkovalvonnasta on käyty lähinnä ministeriöiden virkamiesten, liike-elämän ja poliitikkojen kesken. Poikkeuksena on Helsingin Sanomien Säätiön rahoittama ja COMET-tutkimuskeskuksen keväällä 2015 toteuttama tutkimus, jonka tarkoitus oli selvittää suomalaisten mielipiteitä yksityisyyden toteutumisesta verkkomaailmassa. Tutkimus toteutettiin henkilökohtaisina haastatteluina osana Taloustutkimuksen Omnibus-kuluttajatutkimusta. Otos on muodostettu kiintiöpoiminnalla, kiintiöinä kohderyhmän valtakunnallinen ikä-, sukupuoli-, lääni- ja kuntatyyppijakauma. Vastaajina oli tuhat 15–19-vuotiaista suomalaista.⁵ Seuraavaksi hyödynnän tutkimusraportin (Sirkkunen 2015) keskeisiä tuloksia ja sekä hankkeen loppuraportin (Sirkkunen & Haara 2016) johtopäätöksiä, jotka olen tiivistänyt kuudeksi keskeiseksi löydökseksi.

1. Yksityisyyttä pidetään edelleen arvossa. Yksityisyyden säilymisestä kannetaan edelleen huolta myös verkkoympäristössä. 68 prosenttia kyselyn vastaajista ilmoitti olevansa erittäin tai jonkin verran huolestunut siitä, että internetin käyttäjistä kerätään yhä enemmän tietoa eri tarkoituksiin. Vastaajat haluavat myös tietää lisää siitä, miten ja mitä tietoa kerätään. Peräti 76 prosenttia vastaajista haluaa tietää tarkemmin, mitä tietoja heistä kerätään ja mihin näin koottuja tietoja käytetään. Vastaukset osoittavat selvästi, että suomalaisia huolestaa määräysvallan menettäminen sen suhteen, miten heitä koskevaa tietoa oikein käytetään. Jopa 87 prosenttia vastaajista oli täysin tai jokseenkin samaa mieltä seuraavan väittämän kanssa: *Haluan määritellä itse, mihin tarkoitukseen henkilötietojani käytetään.*

Kuvio 1: Vastausjakauma kysymykseen: Oletteko huolestunut siitä, että internetin käytöstä kerätään yhä enemmän tietoa eri tarkoituksiin, muun muassa mainonnan suuntaamiseen?



Kuvio 2: Vastausjakauma kysymykseen: Mitä mieltä olette seuraavasta väittämästä? Haluan määritellä itse, mihin tarkoitukseen henkilötietojani käytetään.

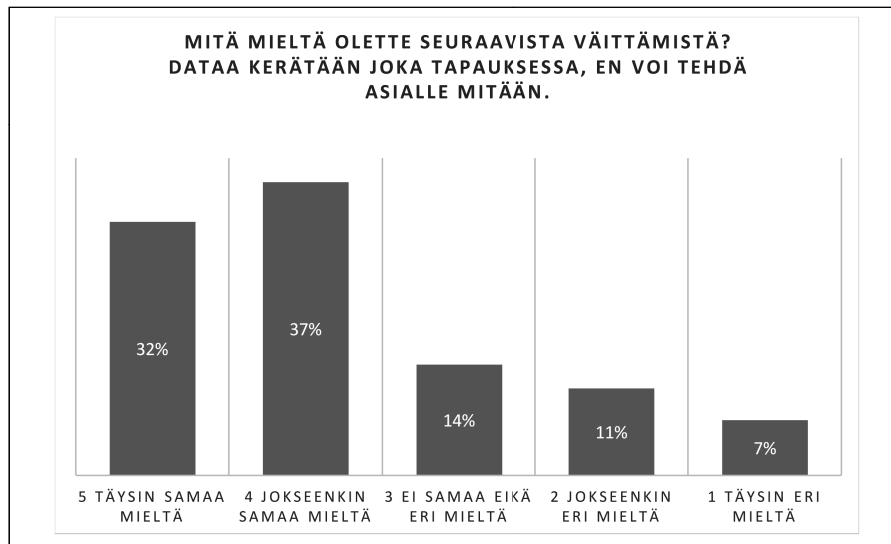


Puolet vastaajista (50 %) ilmoitti olevansa melko huonosti tai erittäin huonosti perillä siitä, millaista tietoa sosiaalisen median palvelut, verkon selainohjelmat tai verkko-operaattorit keräävät heistä internetissä. 44 prosenttia katsoi puolestaan olevansa melko hyvin ja tai erittäin hyvin perillä siitä, minkälaista tietoa heistä kerätään.

2. *Palveluiden käyttöehtoja tunnetaan huonosti, mutta ne hyväksytään silti.* Palveluiden käyttöehtoihin on tutustuttu vaihtelevasti. Facebookin käyttäjistä 63 prosenttia, Googlen käyttäjistä 40 prosenttia, Instagramin käyttäjistä 38 prosenttia ja WhatsAppin käyttäjistä ilmoittaa tutustuneensa palvelun käyttöehtoihin jollain tavoin. Tässä törmätään muissakin tutkimuksissa esiin nousseeseen internetin yksityisyyskäsitteisiin ja käytäntöjä koskevaan ristiriitaan. Yhtäältä ihmiset ovat huolissaan yksityisyyden toteutumisesta, mutta toisaalta eivät kuitenkaan lue läpi uusien palve-

luiden käyttöehtoja. Suurin osa kyselyyn vastanneista katsoi, että palveluiden ehdoille ja tietojen keräämiselle ei ole vaihtoehtoa. 69 prosenttia vastanneista on täysin tai jokseenkin samaa mieltä seuraavan väittämän kanssa: *Dataa kerätään joka tapauksessa, en voi tehdä asialle mitään*. Tämän luvun lopussa keskustellaan tarkemmin siitä, miten nämä tulokset oikein pitäisi tulkita.

Kuvio 3. Vastausjakauma kysymykseen: Mitä mieltä olet seuraavasta väittämästä? Dataa kerätään joka tapauksessa, en voi tehdä asialle mitään.



Väite, jonka mukaan henkilötietojen suoja ei ole tärkeätä, koska minulla ei ole mitään salattavaa, ei saanut kovin suurta kannatusta. 49 prosenttia oli väitteen kanssa jokseenkin tai täysin eri mieltä, kun puolestaan 36 prosenttia oli täysin tai jokseenkin samaa mieltä.

3. *Viranomaisten verkkovalvonta herättää ristiriitoja.* Viranomaisiin kohdistuvan luottamuksen kannalta kiinnostavia tuloksia saatiin kysymykseen, pitäisikö Suomen turvallisuusviranomaisille antaa oikeus seurata ilman lupaa kansalaisten internetin käyttöä ja viestinnän sisältöä. Niukasti yli puolet vastaajista (53 %) katsoi, että tällaista oikeutta verkkovalvontaan ei pitäisi antaa, kun 36 prosenttia puolestaan hyväksyisi seurannan. Nuoret vastaajat suhtautuivat kriittisemmin valvontaan kuin keski-ikäiset ja ikääntyneet.

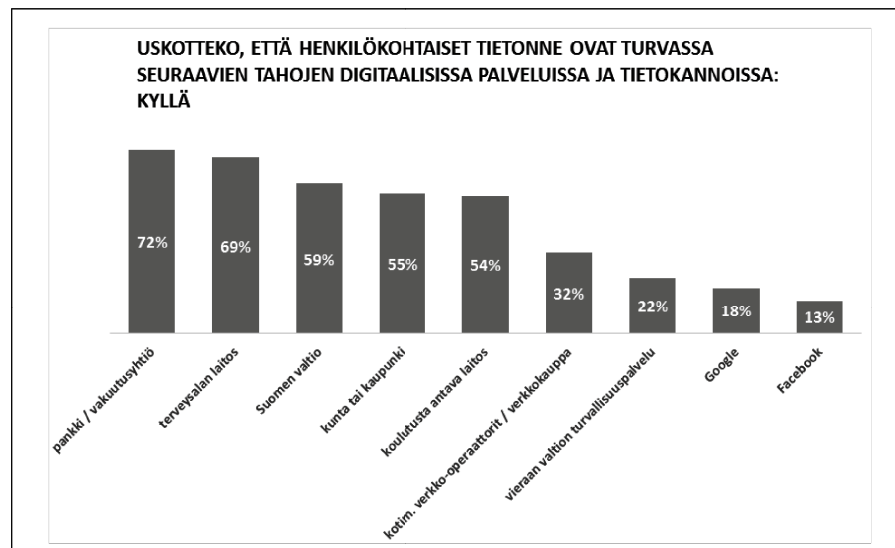
4. *Nuoret ovat tarkkoja yksityisyydestään.* Usein väitetään niin sanotun verkkonatiivin sukupolven suhtautuvan leväperäisesti siihen, mitä tietoja he itsestään verkossa julkaisevat. Tämä käsitys ei saanut vahvistusta vastauksista, itse asiassa kävikin päinvastoin. Nuoremmilla vastaajilla näyttää olevan enemmän halua yksityisyyden suojaan kuin vanhemmilla vastaajilla. Esimerkiksi vain 29 prosenttia 15–24-vuotiaista katsoi,

että heillä ei ole mitään salattavaa, kun vastaava luku 65–79-vuotiailla oli 53 prosenttia. Nuoret halusivat myös vanhempia ikäluokkia tarkemmin määritellä, mihin heitä koskevia henkilötietoja käytetään.

5. *Pankkeihin ja vakuutusyhtiöihin luotetaan, Googleen ja Facebookiin ei niinkään.* Suomalaisten käsitykset ja mielikuvat siitä, missä henkilökohtaisia tietoja säilytetään turvallisesti, vaihtelivat kovasti. Kysymys *uskotteko, että henkilökohtaiset tietonne ovat turvassa seuraavien tahojen digitaalisissa palveluissa tai tietokannoissa* tuotti monensuuntaisia tuloksia.

Parhaiten henkilökohtaista tietoa digitaalisissa palveluissa ja tietokannoissa turvaavat vastaajien mielestä pankit ja vakuutusyhtiöt (72 %), sairaalat, terveyskeskukset ja lääkärriasemat (69 %), Suomen valtio (59 %), kunnat ja kaupungit (55 %) ja koulutusta antavat laitokset (54 %). Huomattavasti vähemmän luottoa vastaajilta löytyy kotimaisille verkko-operaattoreille tai verkkokaupoille (32 %). Erityisen vähän luotetaan Googlen (18 %) ja Facebookin (13 %) kykyyn pitää käyttäjien henkilökohtaisia tietoja turvassa. Tässä on yksi verkon yksityisyyteen liittyvä paradoksi - kaikkein käytetyimpiin alustoihin luotetaan kaikkein vähiten.

Kuvio 4. Vastausjakauma kysymykseen: *Uskotteko, että henkilökohtaiset tietonne ovat turvassa seuraavien tahojen digitaalisissa palveluissa tai tietokannoissa?* (Lähde Sirkkunen & Haara 2016)



6. *Selainhistoriaa tuhotaan, kuvien julkaisemista harkitaan.* Vastaajat ovat omaksuneet erilaisia käytäntöjä, joilla he koettavat suojella yksityisyyttään internetissä. 75 prosenttia vastasi käyttävänsä eri salasanoja eri verkkopalveluissa, 65 prosenttia tuhonneensa selainhistoriaa tai evästeitä, 58 prosenttia jättäneensä julkaisematta kuvia tai videoita, joista voisi tunnistaa yksityisiä ihmisiä. 56 prosenttia vastasi jättäneensä

ottamatta käyttöön joitakin verkkopalveluita niiden puutteellisen yksityisyyden suojan vuoksi ja 51 prosenttia vastasi välttävänsä julkisten ja avoimien wi-fi-verkkojen käyttöä. Muita yksityisyyttä suojaavia käytäntöjä vastattiin olevan selaimen käyttäminen anonyymisti (46 %), palveluiden käytön lopettaminen puutteellisen yksityisyyden suojan vuoksi (36 %) ja salausohjelmien, esimerkiksi Tor-verkon käyttö (16 % vastanneista).

Mielipidetutkimuksen tulokset osoittavat kohtuullisen selvästi, että suomalaiset ovat huolissaan yksityisyyden menettämisestä tiedonkeruun seurauksena. Samalla tunnetaan epävarmuutta ja huolta siitä, mihin käyttäjistä kerätyt tiedot kertyvät ja miten niitä käytetään. Sangen selkeä ja yksiselitteinen oli toive saada lisää päätösvaltaa henkilötietojensa käytössä. Varsin selkeästi nousi esiin myös Googlea ja Facebookia kohtaan tunnettu epäluottamus henkilökohtaisten tietojen turvassa pitämisessä. Hienoinen yllätys oli, että nuoret eivät vastauksien perusteella osoittautuneet huolettomiksi yksityisyydensuojansa suhteen ja muutkin vastaajat ilmoittivat pyrkivän suojelemaan yksityisyyttään internetissä. Tässä lienee kuitenkin syytä muistaa se, että mielipidetutkimukset saavat vastaajat usein vastaamaan niin kuin he olettavat kunnan kansalaisen vastaavan eikä välttämättä mietitä omia arjen ratkaisuja ja käytäntöjä. Mutta vaikka tuloksiin liittyisikin hivenen kaunistelua, huolestumista osoittava yleissuunta saa vahvistusta. Ristiriitaisempia jakaumia liittyi muun muassa vastauksiin viranomaisten verkkovalvonnasta. Iso periaatteellinen tulkintaongelma liittyy väitteeseen, jonka mukaan dataa kerätään joka tapauksessa, enkä voi asialle mitään. Epäselväksi jää se, hyväksyvätkö ihmiset tietoisesti henkilötietojen keräämisen palveluiden käytön ehtona niin kuin mainostajat ja verkkopalveluja tarjoavat yritykset väittävät vai ovatko kyseessä pikemminkin alistuminen vaihtoehtojen puuttuessa ja sosiaalinen paine, joka pakottaa mukaan verkostoitumaan esimerkiksi Facebookiin.⁶

Käyttäjille tosiasiallisesti tarjoutuvista mahdollisuuksista on käyty myös akateemista keskustelua. Annenbergin yliopiston julkaisemassa raportissa (Turow ym. 2015) lähdetään siitä, että käyttöehtojen hyväksyminen ei merkitse vapaaehtoista yksityisyydensuojasta luopumista, vaan pikemminkin alistumista palveluiden ehtoihin. Raportin mukaan pikemminkin kuin kykenevänsä tekemään valintoja, yhdysvaltalaiset uskovat olevan turhaa yrittää vaikuttaa siihen, mitä yritykset voivat saada tietoonsa heistä.

”Tämä alistuminen on virheellisesti tulkittu siten, että käyttäjät ovat suostuneet vaihtokauppaan ja samalla annettu kuva lainsäätäjille ja poliitikoille että käyttäjät hyväksyvät laajan henkilötietojen keräämisen vaikka mielipidetutkimukset toistuvasti ovat osoittaneet, että he vastustavat näitä toimia.” (Turow ym. 2015)

Tässä esitellystä suomalaisesta aineistosta on mahdollista tehdä vastaavan suuntaisia tulkintoja. Ihmisten suostumista käyttöehtoihin ei ole syytä suoraviivaisesti ymmärtää periaatteellisena hyväksymisenä kaikelle henkilötiedon keräämiselle.

Joka tapauksessa tarvitaan lisää tutkimusta juuri verkon käyttäjien asenteista ja toiveista yksityisyyden suojan suhteen verkon eri alustoilla. Kyselytutkimuksen tuloksista käy myös ilmi, että käyttäjien luottamus kaikkein suosituimpiin palvelualustoihin kuten Googleen ja Facebookiin on vähäistä, vaikka näitä palveluita käytetään eniten maailmassa. Tällainen ristiriitainen tilanne vertautuu batesonilaisesta sosiiaalipsykologiasta tuttuun kaksoissidokseen, jossa samasta tilanteesta on samaan aikaan voimassa vastakkaiset näkemykset (me emme kerro, mihin tietojasi käytetään mutta sinun on hyväksyttävä se päästäksesi käyttämään palveluja). On selvää, että näin moniulotteista kysymystä ei voida selvittää yksinomaan mielipidetutkimuksilla, vaan on käytettävä muita tutkimusmenetelmiä. Seuraavassa esitän joitain johtopäätöksiä artikkelistani sekä lisääntyvän valvonnan mediatutkimukselle asettamista haasteista.

Johtopäätöksiä – kriittisen mediatutkimuksen haasteet

Tässä artikkelissa olen pyrkinyt osoittamaan, miten verkkovalvonta toimii ja miten saumattomasti taloudellinen valvonta on lomittunut suurten internet-yritysten liiketoimintaan ja teknologisiin ratkaisuihin. Nähtävillä on myös laajempi muutos internetin talouden rakenteissa ja toimintadynamiikassa. Noin kymmenen vuotta sitten toivottiin internetin käyttäjälähtöisyyden ja amatöörietoksen purkavan valtahierarkioita ja Wikipedian kaltaisten, yhteiskäyttöisyyteen perustuvien palveluiden haastavan ainakin jollain tasolla yksityisomisteisia palvelualustoja (esim. Benkler 2006). Sittenmin on kuitenkin käynyt selväksi, että yhteiskäyttöisyyden sijasta kasvoivatkin Facebookin ja Googlen kaltaiset suuryhtiöt, jotka tarjoamalla maksuttomia, helppokäyttöisiä alustoja kykenivät hyödyntämään käyttäjien luovuuden ja aktiivisuuden, sitomaan heidät valvonnan kohteiksi omille alustoilleen ja käyttämään syntyvää tietoa erityisesti mainonnan suuntaamisessa (Pasquinelli 2009).

Olen hahmotellut rakenteellisia valta-asetelmia erityisesti yksityisyyden näkökulmasta. Olen tarkastellut vaihe vaiheelta, miten kaupallinen verkkovalvonta asemoi verkon käyttäjät lähinnä kulutuspotentiaaliksi ja -profiiliksi perusteella ja miten palveluiden käyttöehdoissa kulminoituu ristiriita korkeaa yksityisyyden suojaa toivovien käyttäjien ja alustojen omistajien taloudellisten intressien välillä. Tarkoitukseni on ollut myös problematisoida alan yritysten esittämiä näkemyksiä, joiden mukaan käyttäjätietojen kokoaminen ja profiloitunut palvelut ovat osa ”luonnollista” kehitystä ja merkitsevät vain lisää tehokkuutta ja käyttömukavuutta. Kyse on myös valtasuhteesta, jossa esimerkiksi kyselytutkimuksessa selkeästi esiin nousut käyttäjien halu tietää, mitä tietoa heistä kerätään ja miten tuota tietoa käytetään, on pitkälti sivuutettu.

Esiin tuomani kehityskulut nostavat esiin monia kysymyksiä valvonnan yhteiskunnallisesta vaikutuksesta, joihin mediatutkimuksen olisi syytä tarttua. Keskeisiä kysymyksiä ovat 1) voidaanko valvontaa ylipäätään välttää tilanteessa, jossa lähes kaikkea toiminnasta digimaailmassa jää jälkiä 2) mitä seurauksia taloudellisella

verkkovalvonnalla on julkisuudelle ja sen rakentumiselle 3) millaisia seurauksia alustojen omistuksen keskittymisellä on käyttäjien asemalle ja yksityisyydelle sekä 4) miten voitaisiin tarjota käyttäjille oikeus määritellä tarkemmin itseään koskevan datan keräämistä ja käyttöä.

Ensinnäkin valvonnan yleistymisestä ja arkipäiväistymisestä avautuu kriittiselle mediatutkimukselle olennainen haaste - miten tehdä valvontateknologioita ja -käytäntöjä näkyväksi ja herättää keskustelua siitä, voimmeko luovuttaa henkilötamme muutamien toimijoiden käyttöön. Keskeinen viestintäpoliittinen kysymys on esimerkiksi se, miten verkkovalvonnan valvonta tulisi järjestää globaalien internetin aikakaudella.

Toiseksi olen nostanut esiin käyttäjätiedon keräämiseen perustuvan liiketoimintamallin vaikutukset mediamaisemaan ja julkisuuteen. Käyttäjätiedosta on tullut vaihdon väline ja sitä kerätään yhä enemmän. Turow (2011, 3) katsoo, että räätälöityjen mediasisältöjen ja mainonnan takana oleva logiikka muuttaa tulevana vuosikymmenenä paitsi median taloutta myös paljolti sitä, miten näemme itsemme, muut ympärillämme sekä maailman ylipäättään. Turowin mielestä taloudellista valvontaa tulee rajoittaa, sillä sen seuraukset saattavat olla tuhoisia paitsi yksityisyyden suojalle myös avoimeen kansalaiskeskusteluun pyrkivälle julkisuudelle ja demokratialle. Couldry ja Turow (2014) varoittavat myös, että jos yhteisiä faktoja, ideoita, lähtökoh- tia ja keskustelunaiheita eri yhteiskunnallisten ryhmien (ja luokkien) välille rakentava media putoaa alaspäin mediatalouden ravintoketjussa, seuraukset voivat olla vakavat. Tällainen kehitys lisäisi ihmisten välistä etäisyyttä, loisi epäluottamusta ja sosiaalista diskriminaatiota edistävää yhteiskunnallista ilmapiiriä. Tässäkin asettuu kohtalaisen kokoinen haaste mediatutkimukselle, jonka tulisi kiinnittää entistä tarkemmin huomiota verkkojulkisuuden rakenteellisiin muutoksiin ja pyrkiä arvioida julkisuuden toimintaa erityisesti demokratian ja kansalaiskeskustelun näkökulmista.

Kolmanneksi olen halunnut tarkastella sosiaalista mediaa vallan jakautumisen sekä käytäntöjen ja rakenteiden välisen dynamiikan näkökulmista (ks. myös Sirkkunen 2009) ja nostaa esiin verkkovalvonnan olennaisia piirteitä. Aidatusta internetistä kirjoittava Andrejevic (2007) vertaa verkkovalvonnan aikakautta siihen yhteiskuntahistorian vaiheeseen, jossa maanomistuksessa tapahtuneet muutokset, kuten yhteiskäyttöisten maiden muuttuminen yksityisomaisuudeksi johtivat feodalismista kapitalismiin. Andrejevicin mukaan olemme nyt vastaavanlaisessa tilanteessa, jossa on syntynyt jako niihin, jotka kontrolloivat yksityistettyjä interaktiivisia tiloja (virtuaalisia tai muunlaisia) ja niihin, jotka hyväksyvät valvonnan päästäkseen käsiksi näihin tiloihin, tavaroihin, tuotteisiin, palveluihin ja mukavuuksiin (Andrejevic 2007, 3). Kriittisen mediatutkimuksen tulisi myös tarkastella sitä, minkälaisia valtasuhteita ja toimintojen dynamiikkaa käyttäjien ja alustojen välillä syntyy, miten tuotanto- ja omistussuhteet järjestyvät ja mitä seurauksia näillä kehityskuluilla on esimerkiksi yksityisyydelle.

Viimeisenä jäljellä on kysymys siitä, onko tavallisella internetin käyttäjällä mahdollista ylläpitää yksityisyyden suojaa ja kontrolloida sitä, miten häntä koskevaa tietoa käytetään. Ekskursioni osoitti, että eurooppalaiset lainsäätäjät koettavat

osaltaan puolustaa käyttäjien oikeuksia. Mutta myös uudenlaisia merkkejä vaihtoehtojen etsimisestä on olemassa. Esimerkiksi henkilötiedon omaehtoiseen hyödyntämiseen pohjaava Oma data -aloite (Poikola ym. 2014) on askel verkon käyttäjien kontrollimahdollisuuksien lisäämiseksi. Aloitteessa lähdetään liikkeelle ajatuksesta, jonka mukaan verkon käyttäjällä on oikeus hallita itsestään kerättyä tietoa sekä jakaa, vaihtaa tai myydä sitä edelleen muihin palveluihin. Toteutuessaan Oma data -malli purkaisi edellä esitetyn kaksoissidoksen ja palauttaisi henkilökohtaisen tiedon hallinnan käyttäjille mahdollistaen myös ”oman datavaluutan” vaihdolle perustuvien uudenlaisten palveluiden ja liiketoimintamallien kehityksen.

Jotkut kriittiset tutkijat hahmottelevat vielä pidemmälle meneviä verkon valta-asetelmien muutoksia. Esimerkiksi marxilaista käsitteistöä sosiaaliseen mediaan, verkkovalvontaan ja yksityisyyteen monissa artikkeleissaan soveltanut Fuchs (2011a, 2011b, 2012) näkee Facebookin ja Googlen pääomaa keräävinä koneistoina sekä pitää taloudellista verkkovalvontaa inhimillisen luovuuden tuotteistamisena ja riistona. Fuchs uskoo, että kriittisillä voimilla on vielä mahdollisuuksia horjuttaa suuryritysten valta-asemaa verkossa muun muassa mediakasvatuksen avulla ja rakentamalla verkon keskeiset palvelut ja alustat yhteiskäyttöisyyden periaatteen varaan. Oli tavoite kuinka utopistiselta vaikuttava tahansa, kriittisen mediatutkimuksen tulisi etsiä ja pitää esillä vaihtoehtoja nykyisille käyttäjätiedon keräämiselle perustuville liiketoimintamalleille.

Ekskursioni verkkovalvontaan ja yksityisyyteen osoittaa, että tarvitaan lisää internetiin kohdistuvaa mediatutkimusta, jonka avulla on mahdollista käsitellä ja käsitteellistää talouden, politiikan ja teknologian kaltaisten tekijöiden suhdetta valtaan ja sosiaaliseen oikeudenmukaisuuteen (ks. esim. Wasco ym. 2011). Valtasuhteiden analysoimiseksi tulee myös verkkoalustojen tasolla tutkia sitä, minkälaisia taloudellisia, teknisiä kulttuurisia ja sosiaalisia intressejä palveluiden algoritmeihin koodautuu (Bucher 2012; Langois & Elmer 2013). Lisäksi tarvitaan myös arjen viestintäkäytäntöjen tutkimusta. Käyttäjät suhtautuvat palveluihin eri tavoin ja heillä on omat, rajalliset, mutta silti olemassa olevat resurssit koodata palveluja eri tavoin kuin mitä yritykset itse tarjoavat niin kuin Saariketo (2015) hyvin osoittaa. Yksityisyyttä ei tule ymmärtää yksinomaan taloudellisten tai juridisten määrittelyjen valossa vaan myös toimintana, jossa ihmiset erilaisissa arjen käytännöissään ratkaisevat ongelmia ja rakentavat yksityisyytensä rajoja. Se, minkälaiset edellytykset heillä tähän kulloinkin on, ei ole kuitenkaan yksin heidän määrättävissään. Internet alustoinen muodostaa mediatutkimukselle niin moniulotteisen tutkimuskohteen, että se vaatii rakenteita, teknologiaa ja käytäntöjä yhdessä tarkastelevaa tutkimusotetta. Muuten rakenteiden ja toiminnan välinen monisyinen dynamiikka jää tavoittamatta.

Viitteet

- 1 Myös Suomessa on viime aikoina keskusteltu verkkovalvonnan toteutumisesta. Elokuussa 2015 hallitus ilmoitti aloittavansa verkkotiedustelulain valmistelun ja sen arvioidaan tulevan eduskunnan käsittelyyn joskus vuoden 2017 aikana. Hankkeella on mittavia eettisiä ja juridisia seurauksia, sillä verkkotiedustelun salliminen vaatii muutoksia nykyiseen viestinnän luottamuksellisuutta koskevaan lainsäädäntöön sekä perustuslakiin. (Sajari 2015, Niilola 2015.)
- 2 Alan kirjallisuudessa tutkija toisensa jälkeen toteaa, että yksityisyyttä on mahdotonta määrittellä universaalisti ja yksiselitteisesti. Yksityisyyden merkitys on kontekstuaalista ja se vaihtelee maasta tai kulttuurista toiseen (Solove 2008,2, Zureik 2010,358). Vaikka yksityisyyden tarkassa määrittelyssä on ongelmansa, yksityisyyden arvo tunnustetaan silti jollain tavoin suurimmassa osassa valtioiden perustuslakeja tai lainsäädäntöä. Yksityisyys on liitetty myös YK:n määrittelemiin perusoikeuksiin Suomessa viestinnän yksityisyyttä säädellään lainsäädännössä monella tasolla perustuslain yksityiselämän suojasta lähtien. Muita yksityisyyden suojaan vaikuttavia lakeja ovat muun muassa henkilötietolaki, laki viranomaisten toiminnan julkisuudesta, laki yksityisyyden suojasta työelämässä, laki yksityiselämää loukkaavan tiedon levittämisestä, sähköisen viestinnän tietosuojalaki sekä muutamat EU:n direktiivit.
- 3 Linkki nykyisiin käyttöehtoihin: <https://www.facebook.com/legal/terms>
- 4 Vuoden 2015 alkupuolella Facebook omisti seuraavat yhtiöt: Facebook Payments Inc., Atlas, Instagram LLC, Mobile Technologies Inc. Onavo, Parse, Moves, Oculus, Liverail ja WhatsApp Inc.
- 5 Tietoja vastaajista:

1) Vastaajien sukupuoli

Sukupuoli	
Nainen	Mies
533	467

2) Vastaajien ikäryhmät

Ikäryhmä				
15-24 v.	25-34 v.	35-49 v.	50-64 v.	65-79 v.
176	159	210	239	216

3) Vastaajien ammatti/asema

Vastaajan ammatti/asema						
Maanviljelijä/ työntekijä	Toimihenkilö	Ylempi toimihenkilö/ asiantuntija	Yrittäjä/ johtava asema	Opiskelija, koululainen	Eläkeläinen	Kotiäiti/- isiä/ työtön
223	82	82	53	159	288	113

4) Vastaajien koulutus

Mikä on koulutuksenne					
Perus-/keski-/ kansa-/ kansalaiskoulu	Ammatti-/ tekninen-/ kauppakoulu	Ylioppilas/ lukio	Opistotaso	Ammattikorkeakoulu	Yliopisto, korkeakoulu
217	300	92	127	94	161

- 6 Käyttäjien huolestuneisuudesta kertovien tulosten kanssa ristiriidassa ovat muutamat Facebookin käyttäjien asenteita laadullisin menetelmin kuvanneet tutkimukset (mm. Ridell 2011, Taddicken 2012, Saariketo 2015). Näissä Facebookin käyttäjien haastatteluissa ja ryhmäkeskusteluissa käyttäjätiedon kerääminen ei ole herättänyt kovinkaan jyrkkää kritiikkiä. Vastaajat tuntuivat hyväksyvän henkilötietojen keräämistä välttämättömänä ehtona päästä käyttämään palvelua.

Kirjallisuus

- Andrejevic, Mark (2007). *iSpy. Surveillance and Power in the Interactive Era*. Lawrence, Kansas: University Press of Kansas.
- Barnes, Susan B. (2006). A privacy paradox: Social networking in the United States. *First Monday* 11:9. September 2006. Saatavilla: <http://firstmonday.org/ojs/index.php/fm/article/view/1394/1312> (luettu 06.06.2016).
- Bauman, Zygmunt & Lyon, David (2013). *Liquid Surveillance. A Conversation*. Cambridge, UK: Polity Press.
- Benkler, Yochai (2006). *The Wealth of Networks. How Social Production Transforms Markets and Freedoms*. New Haven and London: Yale University Press.
- Brunila, Mikael (2014). Runsauden räjähdys – internet hakutalouden jälkeen. Teoksessa Brunila, Mikael & Kallio, Kimmo (2014). *Verkko suljettu. Internet ja avoimuuden rajat*. Helsinki: Into.
- Bucher, Taina (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *New Media & Society* 0(0) 1-17.
- Carr, Ian (2013). Tools, platforms, and Google Reader. Blogimerkintä 14.03.2013. Saatavilla: <http://www.rougthtype.com/?p=3077> (luettu 06.06.2015).
- Cohen, Julie E. (2012/2013). What privacy is for. *Harvard Law Review*, Vol. 126, 2013. Saatavilla: <http://ssrn.com/abstract=2175406> (luettu 06.06.2016).
- Couldry, Nick & Turow, Joseph (2014). Big data, big questions. Advertising, big data, and the clearance of the public realm: Marketers' new approaches to the content subsidy. *International Journal of Communication* 8 (2014) 1710-1726. Saatavilla: <http://ijoc.org/index.php/ijoc/article/view/2166>. (luettu 06.06.2016).
- Dijck, José van (2013). *The Culture of Connectivity. A Critical History of Social Media*. Oxford: University Press.
- Gerlitz, Carolin & Helmond, Anne (2013). The Like economy: Social buttons and the data-intensive web. *New Media & Society*. First published on February 4, 2013. Saatavilla: doi:10.1177/1461444812472322 (luettu 06.06.2016).
- Giddens, Anthony (1984). *The Constitution of Society*. Cambridge: Polity Press.
- Griffin, Andrew (2016) Facebook reactions: Belgian police warn citizens not to react to posts on social media. Independent 13.05.2016. <http://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-reactions-belgian-police-warn-citizens-not-to-react-to-posts-on-social-media-a7027786.html> (luettu 06.06.2016)
- Gillespie, Tarleton (2010). The politics of 'Platforms'. *New Media & Society* 12:3, 347-364.
- Foucault, Michel (1980). *Tarkkailla ja rangaista*. Keuruu: Otava.
- Fuchs, Christian (2011a). An alternative view of privacy on Facebook. *Information*, 2, 140-165.
- Fuchs, Christian (2011b). New media, Web 2.0 and surveillance. *Sociology Compass* 5:2; 134-147.
- Fuchs, Christian (2012a). The political economy of privacy on Facebook. *Television & New Media* 13.2, 139-159.
- Fuchs, Christian ym. (2012b). Introduction. Internet and surveillance. Teoksessa Fuchs et al. (toim.) *Internet and Surveillance. The Challenges of Web 2.0 and Social Media*. New York: Routledge.
- Haggerty, Kevin & Ericson, Richard (2000). The surveillant assemblage. *British Journal of Sociology* 5: 4, 605-622.
- Johnson, Bobbie (2010) Privacy no longer a social norm, says Facebook founder. The Guardian. <https://www.theguardian.com/technology/2010/jan/11/facebook-privacy> (luettu 06.06.2016)
- Koistinen, Olavi (2016) Tämä itävaltalainen opiskelija pani Facebookin seinää vasten, kaatoi suurvaltojen sopimuksen oikeudessa ja veti rajat Yhdysvaltojen vakoilulle. Helsingin Sanomat 23.01.2016.
- Langlois, Ganaele & Elmer, Greg (2013). The research politics of social media platforms. *Culture Machine* 14. 1-17.
- Madden, Mary (2014). Public perceptions of privacy and security in the post-Snowden era. Saatavilla: <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/> (luettu 06.06.2016).
- Mann, Steve; Nolan, Jason & Wellman, Barry (2003). Sousveillance: Inventing and using wearable computing devices for data collection in surveillance environments. *Surveillance & Society* 1:3, 331-355.
- Marshall, Jack (2016) Facebook wants to help sell every ad on the web. The Wall Street Journal 27.05.2016. <http://www.wsj.com/articles/facebook-wants-to-help-sell-every-ad-on-the-web-1464321603> (luettu 06.06.2016)

- Niilola, Merja (2015). Professori: Tiedustelu- ja vakoilulaista pahimmillaan NSA-massaurkintaa. Yle Uutiset, kotimaa, 21.08.2015. Saatavilla: http://yle.fi/uutiset/professori_tiedustelu_ ja_vakoilulaista_pahimmillaan_nsa-massaurkintaa/8235130 (luettu 06.06.2016)
- Nikkanen, Hanna (2014). Massavalvonta ja puolivarjoiset tilat. Teoksessa Brunila, Mikael & Kallio, Kimmo (toim.) *Verkko suljettu. Internet ja avoimuuden rajat*. Helsinki: Into Kustannus.
- Pasquinelli, Matteo (2009). Google's PageRank algorithm: A diagram of cognitive capitalism and the rentier of the common intellect. Teoksessa Becker Konrad & Stalder, Felix (toim.). *Deep Search*. London: Transaction Publishers.
- Poikola, Antti; Kuikkaniemi, Kai & Kuittinen, Ossi (2014). My Data -johdatus ihmiskeskeisen henkilötiedon hyödyntämiseen. Liikenne- ja viestintäministeriö. Saatavilla: <http://www.lvm.fi/-/my-data-johdatus- ihmiskeskeiseen-henkilötiedon-hyodyntamiseen-842175> (luettu 06.06.2016)
- Ridell, Seija (2011). *Elämää Facebookin ihmemaassa*. Tampere: Tampereen yliopisto, Viestinnän, median ja teatterin yksikkö CMT.
- Saariketo, Minna (2015). Neuvotteluja kytkösmedian arkkitehtuurisesta vallasta. *Media ja Viestintä* 3.
- Sajari, Petri (2015). Oikeustieteilijät torjuvat verkkovalvonnan. Verkkovalvonta olisi todennäköisesti vastoin EU-tuomioistuimen ratkaisua. Helsingin Sanomat 12.01.2015. Saatavilla: <http://www.hs.fi/kotimaa/a1420951852080> (luettu 06.06.2016).
- Sirkkunen, Esa (2009). Aidattu vai avoin verkko? Omaehtoisen toiminnan muodot ja rajat sosiaalisen median tiloissa. Teoksessa Ridell (ym. toim.) *Julkisen tilan poetiikkaa ja politiikkaa*. Tampere: Tampere University Press.
- Sirkkunen, Esa (2015). Raportti yksityisyys -kyselytutkimuksen tuloksista. Tutkimuskeskus COMET, Tampereen yliopisto, kesäkuu 2015. Saatavilla: <http://www.uta.fi/cmt/tutkimus/comet/tutkimus/ Yksityisyys- ja-anonymiteetti-verkkoviestinnassa/index/prianokyselyraportti.pdf> (luettu 06.06.2016)
- Sirkkunen, Esa & Haara Paula (2016) Yksityisyys verkkoviestinnässä -hankkeen loppuraportti. Tutkimuskeskus COMET, Tampereen yliopisto (julkaistaan myöhemmin)
- Sloop, John M. & Gunn, Joshua (2010). Status control: An admonition concerning the publicized privacy of social networking. *The Communication Review*, 13:4, 289-308.
- Solove, Daniel J. (2008). *Understanding Privacy*. Cambridge: Harvard University Press.
- Taddicken, Monika (2012). Privacy, surveillance, and self-disclosure in the social web: Exploring the user's perspective via focus groups. Teoksessa Fuchs et al. (toim.) *Internet and Surveillance. The Challenges of Web 2.0 and Social Media*. New York: Routledge.
- Trottier, Daniel & Lyon, David (2012). Key features of social media surveillance. Teoksessa Fuchs et al. (toim.) (2012) *Internet and Surveillance. The Challenges of Web 2.0 and Social Media*. New York: Routledge
- Turow, Joseph (2011). *The Daily You. How the New Advertising Industry Is Defining Your Identity and Your Worth*. New Haven & London: Yale University Press.
- Turow, Joseph, Hennessy, Michael & Draper, Nora (2015) *The Tradeoff Fallacy. How Marketers Are Misrepresenting American Consumers And Opening Them Up to Exploitation*. A Report from the Annenberg School of Communication, University of Pennsylvania. Saatavilla: https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf (luettu 06.06.2016)
- Van Alsenoy, Brendan (2015.) From social media service to advertising network. A critical analysis of Facebook's Revised Policies and Terms. Draft, 23 February 2015. Saatavilla: <http://www.law.kuleuven.be/citip/en/news/item/facebooks-revised-policies-and-terms-v1-1.pdf> (luettu 06.06.2016)
- Wasko, Janet; Murdock, Graham & Sousa, Helena (toim.) (2011). *The Handbook of Political Economy of Communications*. Sussex, UK: Wiley-Blackwell.
- Vehkoo, Johanna (2011). *Painokoneet seis! Kertomuksia uuden journalismin ajasta*. Helsinki: Kustannusosakeyhtiö Teos.
- Virrantaa, Riikka (2015). Huutokauppa ilman ihmisiä. *Suomen Lehdistö* 1/2015.
- Zureik, Elia (2010). Cross-cultural study of surveillance and privacy: Theoretical and empirical observations. Teoksessa: Zureik, Elia ym. (toim.) (2010) *Surveillance, Privacy and the Globalization of Personal Information*. Montreal: McGill-Queen's University Press.